# Business Edition Product Guide

## Product Overview

Syncplicity Business Edition provides easy-to-use online file management for businesses, combining intuitive native support of both PCs and Macs for users, and unique centralized management for IT.   Syncplicity automatically syncs files across all designated computers, backs up data automatically in real time, and makes sharing files and collaborating easier than ever before.

End users enjoy automated file sync, back-up, file sharing, and collaboration in one easy to use cloud solution. Files are always where users need them with Business Edition's anywhere access, full versioning and change management.  Users seamlessly move from their laptop to desktop, mobile device to Google Docs -- files are synced in real-time across all the places they work.   Our solution lets users work with their files and folders wherever they keep them today, in native environments like the Mac, PC, online services like Google Apps, servers like File Servers and SharePoint Servers, and mobile devices like iPhones, iPads and Android devices, while gaining all the benefits of cloud computing.  Users collaborate with one-click file sharing, can access deleted file versions anytime, and data is never lost with automatic back-up and instant restore.

Businesses get the tools they need to easily secure and manage files company-wide. The IT management console offers unique reporting and administration, giving companies the ability to protect users from data loss, to ensure users have anywhere access to their files, set file management policies to secure corporate data, and easily add, configure and support multiple users.  Beyond Macs and PCs, Business Edition supports file servers, Google Docs, other online file stores and mobile devices.  The solution scales to any number of users, files, file sizes and storage. We place the utmost importance on security through military-grade encryption and SAS70 Type II/SSAE-16 certification of our data hosting centers.   Customers can be deployed within an hour of signing up, and report IT cost savings as they deploy Syncplicity across their organizations.

## Top Customer Features

- Instant Sync between any data source with inclusion and exclusion
- Real-Time Back-Up with Full File Versioning and Audit Trail
- Native integration with Windows and Mac means unprecedented ease of use
- Secure mobile apps with remote wipe, policy controls, and at-rest encryption for iPhone, iPad, Android, and Kindle Fire
- Instant restore of any previous file or file version can be done by a user or remotely by an IT Admin
- Google Apps Integration with Single Sign-On and comprehensive Google Docs support
- Policy-Controlled Multi-User Sharing and Collaboration
- News Feed
- Anywhere Access to files via website, cloud applications, and mobile device
- Central User Creation and Management with Pre-Configuration, and Reporting
- Integration with Existing Infrastructure
- Remote Help Desk
- Enterprise Level Security

### Instant Sync between any data source with inclusion and exclusion

Administrators and users can set up any folder and file to synchronize between computers. Any file, file type, or folder, including sub-folders, can be included or excluded from sync. Synced folders can be stored in any location. Client sync speed can be modified, synced folders managed, and status displayed.

### Real Time Back-Up with Full File Versioning and Audit Trail

Every file is continuously versioned in real-time to ensure every file is fully protected, so users don't need to be on the corporate network for their data to be protected. Every time a file is created, changed, or deleted, the file is immediately versioned. Each version is tracked to indicate what modification took place, when the change occurred, and, for collaboration scenarios, who performed the action. An unlimited number of previous versions and deleted files can be retained with the Business Edition account.

### Secure mobile apps with remote wipe, policy controls, and at-rest encryption for iPhone, iPad, Android, and Kindle Fire

Provide secure file access, sync, backup, sharing and collaboration everywhere your employees work. They'll have the latest version of files where they need them, offline or online. Behind the scenes, Syncplicity keeps it all secure with end-to-end transfer and unique at-rest encryption, remote wipe capabilities, and policy and permission controls.

### Native integration with Windows and Mac means unprecedented ease of use

Unlike many other solutions that require users to change their behavior or move their files to a new place, Business Edition is a drop-in solution which allows users to work with their existing file hierarchies. Users work in the same environments they have now to access, share, collaborate and backup effortlessly, using the same files, programs and file hierarchy they use today.

### Instant restore of any previous file or file version by a user or remotely by an IT Admin

Any deleted file or previous file version is downloadable or can be instantly retrieved or reverted in-place by either the end-user or helpdesk IT. If a computer is lost or crashes, instant recovery is simple: after the client is installed on a new computer, it can instantly begin to restore all backed up files to their original locations. This instant restore capability is a key benefit over other backup solutions that move customer data to cheap offline or near-line storage, making instant data restoration impossible.

## Google Apps Integration with Single Sign-On and comprehensive Google Docs support

With Business Edition's Google Apps and Google Docs integration, businesses have a way to integrate Google's cloud applications with their existing rich desktop applications such as Microsoft Office. Users are able to open and edit files without having to manually manage files between Google Docs or in a desktop application. With Single Sign-On with Google Apps, business customers logged into their Google Apps account can seamlessly access their Syncplicity account through a Google Apps UI widget and without needing to reauthenticate. Business Edition also eliminates many of the limitations around Google Apps such as providing offline access to Google Docs files and supporting files and storage in excess of the Google Apps file and storage limits.

## Policy-Controlled Multi-User Sharing and Collaboration

Business Edition's sharing and collaboration makes easy for users to easily share and collaborate with others, both inside and outside of the firewall, while Business Edition's policy controls ensure IT can manage the flow of files to ensure compliance with corporate policy.

For basic sharing, shared files allow anonymous, read-only sharing secured by a URL that can be easily sent to others. For more advanced sharing and collaboration, any folder can be instantly created and shared across multiple users with per-user permissions. Administrators can set policies on sharing to enforce corporate data policies and can monitor sharing within the company to ensure compliance.

## News Feed

The News Feed enables users to view all file activity that has occurred within their account and filter the information so they are presented with only the events they are interested in.

## Anywhere Access to files via website, cloud applications, and mobile device

Business Edition ensures users always have access to their files, even if they don't have access to their computer. Files can be accessed through a web file browser from any browser, a mobile optimized site, and a 3rd party iPhone app. Business Edition also allows users to view and edit their files online with just a web browser through integration with cloud applications such as Zoho, Scribd, Picnik, and Google Docs.

## Central User Creation and Management with Pre-Configuration, and Reporting

Business Edition's Central User Administration enables IT Administrators to streamline management of multiple user accounts and to ensure these accounts conform to IT policy. User accounts can be bulk provisioned and pre-configured to establish default folders to be backed up and folders they have access to. Through policy controls, pre-configuration options can be set to take effect without user intervention. IT Admins can gain insight into user activity, utilization, and data flows to find out files are being protected what and where data is being shared.

## Integration with Existing Infrastructure

Business Edition can either work with existing on-premise infrastructure such as File Servers and SharePoint servers or can replace them. Companies have the choice to keep what works and replace what doesn't. Business Edition also features Federated Authentication through both the industry standard SAML and OpenID protocols, allowing it to use existing user credentials and policies stored in common user directories such as Active Directory, LDAP, and Google Apps.

## Remote Help Desk

Remote Help Desk ensures that an IT help desk is able to fully support their users. All major actions which a user can perform, IT helpdesk can also perform on their behalf. Designed to enable quick and easy resolution for cases, even in cases where support personnel don't have direct access to a user's machine or screen, administrators can perform actions such as viewing user configuration and performing actions such as remote restore, setting account specific configuration, or helping a user manage their shares. Help desk can also train a user to self-help by using the website impersonation to view the online user account the user sees, enabling support to remotely walk users through actions over the phone.

## Enterprise Level Security

Business Edition provides a highly secure, available, and dependable file management system. Secure from the ground-up, the highest levels of military grade AES-256 and 256bit SSL encryption are used to protect all customer data during transmission and at rest along with strong defense-in-depth such as maintaining encryption keys in a separate data center from encrypted data to keep the digital keys away from the vault. In addition, all data centers used by Syncplicity are SAS70 Type II/SSAE-16 certified and are DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 compliant. All data within stored within Syncplicity Business Edition are stored in quadruplicate across multiple geographically separate data centers to ensure the highest levels of robustness and dependability.

## How to Access and Use Top Features

This document will describe the top features of the Syncplicity along with setup and access for Users and Admins. These features are listed below:

**Real Time Back-Up with Full File Versioning and Audit Trail**

**Instant Sync between any data source with inclusion and exclusion**

**Instant restore of any previous file or file version by a user or remotely by an IT Admin**

**Google Apps Integration with Single Sign-On and comprehensive Google Docs support**

**Policy-Controlled Multi-User Sharing and Collaboration**

**News Feed**

**Anywhere Access to files via website, cloud applications, and mobile device**

**Central User Creation and Management with Pre-Configuration, and Reporting**

**Remote Help Desk**

## GETTING STARTED FOR ADMINS

You will need a Company Account in order to use Business Edition and perform any of the how-to's within this guide. You can sign up on-line to create a trial Business Edition account.

### Creating a Business Edition Company Account

Signing up for Syncplicity is a fast and easy process. To sign up for a Syncplicity account, just follow the steps below:

1. Go to http://www.syncplicity.com/products/ and select the Syncplicity Business Edition
2. Enter your email address, name, password and number of user accounts you would like in your trial. Agree to the Terms of Service, and then click **Sign Up.**

## GETTING STARTED FOR END-USERS

You will need a user account set up with a client installed on Windows or Mac OS to perform some of the how-to's within this guide. The Admin Console section later on in this document describes how to provision an account for a new user. Once the new user account is provisioned, you will need the follow the steps below to set up a user account for the first time.

When a user account is first created, the user will receive an email invite to set up Syncplicity with a URL link. This link provides will walk them through the fast and easy steps to get the Syncplicity client installed on their machine.

Sample invite:

syncplicity

Effortless synchronization, backup & sharing.

## Welcome to Syncplicity

Your company's administrator just created a new Syncplicity account for you. Click the Login Now button to activate the account, set your password, and get started.

Syncplicity makes working with files and folders a breeze by:

- Keeping every version of every file backed up
- Ensuring files are always in sync across all your computers
- Giving you instant, anytime access to any file online
- Letting you share folders with others on your team

To find out more about what Syncplicity can do, visit our short Product Tour.

Welcome!

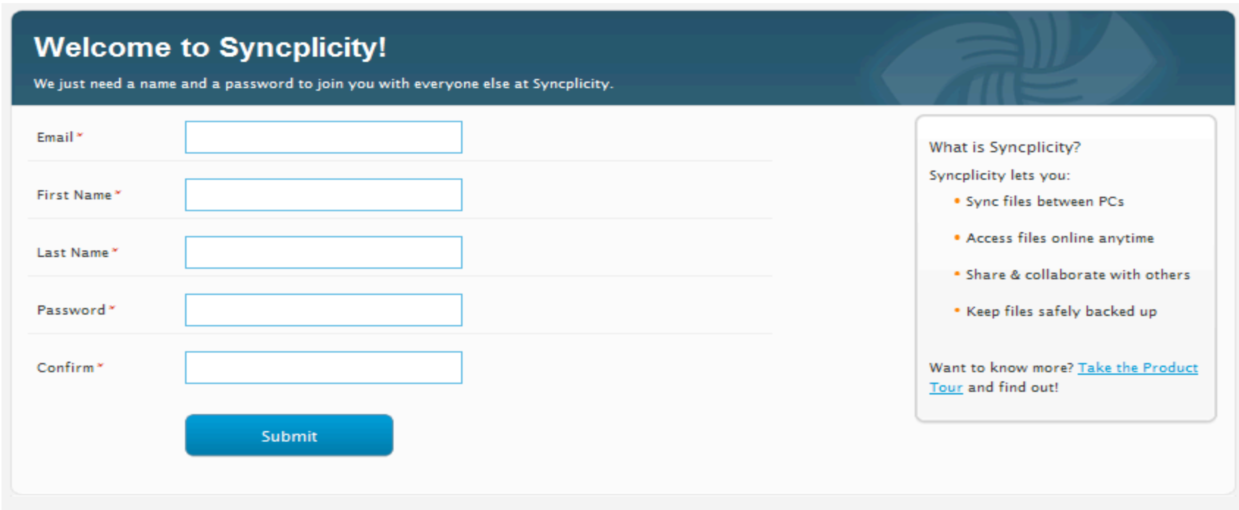
**The Syncplicity Team**
**support@syncplicity.com**

Note: if clicking on links in this email doesn't work, just copy and paste the following address into your browser's address bar:
https://my.syncplicity.com/Login.aspx?InviteToken=XXXXXXX

Login Now

**Synchronization**
Edit a document at work and when you arrive at home you'll find the latest version waiting for you.
**Backup**
Your files are important, so we never stop backing them up. Make a change and Syncplicity will securely store it right away.
**Sharing**
Share documents and files with others easily. When your colleague adds or updates a file, you'll get it immediately.

**Step 1**: Upon clicking the invite link in the email invite, the user is asked to enter their information and click **Submit**.




**Step 2:** The user then downloads the Syncplicity client and follows the prompts.


After the client is successfully installed, you will see the Syncplicity logo in the taskbar icon tray on the bottom right of the screen on Windows or a black and white Syncplicity icon logo on the menu bar on Mac OS.

## REAL TIME BACK-UP WITH FULL FILE VERSIONING AND AUDIT TRAIL

Users can add or exclude any folder to be managed by Business Edition by following these steps. Once a folder is added, it will be automatically synced and backed up in real time with full versioning and an audit trail. This process also happens automatically for any folders which are added for sharing purposes. Here's what occurs in the syncing process:

1. Syncplicity scans your computer to see what has been added (or in the case of subsequent synchronizations, what has changed)
2. The content will be uploaded online in real-time
3. Click on the Syncplicity tray icon to see the status of the sync. Once the status shows "Fully synced," you may navigate to my.syncplicity.com/files to view your files online.

### Action: Add Folder

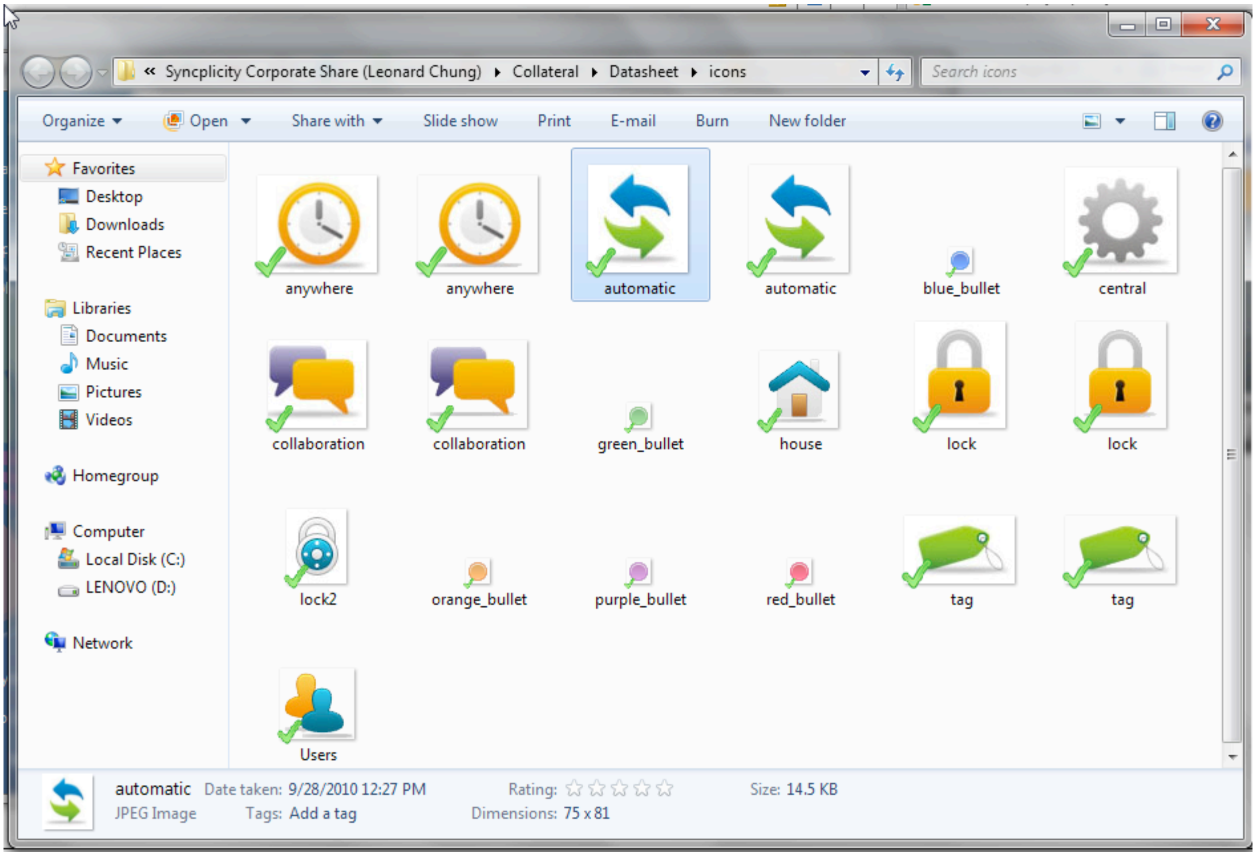
**Note:** Adding a folder will add all sub-folders and files unless they are otherwise excluded

Adding a folder to your Syncplicity account is the first step to sync folders between account users. To add a folder to your sync:

1. Right-click on the folder you wish to add, and select **Syncplicity**
2. Click **Add to Syncplicity**
3. Your folder should now appear with the Syncplicity logo - this means that your computer is now processing the initial sync

Once a folder is added to the Syncplicity Business Edition, all the folder contents are automatically backed up on the local machine at the managed location and at the Syncplicity server's in real time. Any future changes to the folder contents will now be automatically detected, backed up, and versioned.

To see which documents have been backed up on the local machine, navigate to the managed location on the machine and all documents with a Green checkmark have been backed up to the Syncplicity servers.




## Action: Exclude Folder

To stop the sync process (but keep files in your Syncplicity account):

1. Right click on the Syncplicity tray icon and select **Manage and Share Folders** from the menu
2. Click once on the folder you are removing, to select it and use the **Exclude it** command located on the upper right hand side of the view
3. Click **OK**, then click **OK** at the bottom of this view when you are done

This means that Syncplicity will stop monitoring a given folder for changes, but will keep the files (as is) in your Syncplicity account.

## Action: Exclude Subfolder

**Note:** A sub-folder is a folder that is located within an added folder

To stop the sync process of a subfolder (but keep the subfolder backed up in your Syncplicity account):

1. Right click on the Syncplicity tray icon and select **Manage and Share Folders** from the menu
2. Navigate to the subfolder you would like excluded, then uncheck the box next to the subfolder name
3. Click **OK** to confirm the exclusion of the subfolder.

## INSTANT SYNC BETWEEN ANY DATA SOURCE WITH INCLUSION AND EXCLUSION

Users can edit and save files in any managed location; audit trails of past revisions are visible and available for download or for restoration.

### Action: Set Folder Location

When the Syncplicity client is first run and a folder has been shared or synced with the user's account, a dialog will appear asking the user whether they wish to accept and sync the folder onto this computer or not. This dialog will also appear any time a new folder is added to the user account from another machine or shared with the user by another person.

By default, Syncplicity will sync folders to a file path that looks something like "C:\Users\<username>\Documents\Syncplicity Folders\<share name>" depending upon the version of Windows the client is running on. The dialog presents the option to either sync the folder with a default location or to customize the location:

1. To keep the default folder location, simply click **Accept** on the dialog box. Syncplicity will begin to sync the new folder to the default location given in the dialog box.
2. To change the location, click the **Choose** button and set your custom location, then click **Accept**

### Action: Change Folder Location

You can change the folder path on any folder to change the location it syncs to. To change a folder location:

1. Click on the Syncplicity icon in your system tray
2. Select **Manage and Share Folders**
3. Temporarily exclude the folder from your sync by clicking the folder name and then the **Exclude it** link on the right
4. Re-include the folder by clicking the **Add this folder** link on the right.
5. A dialog box will appear with the default location. Click **Change location** to customize the file path
6. Click **OK**

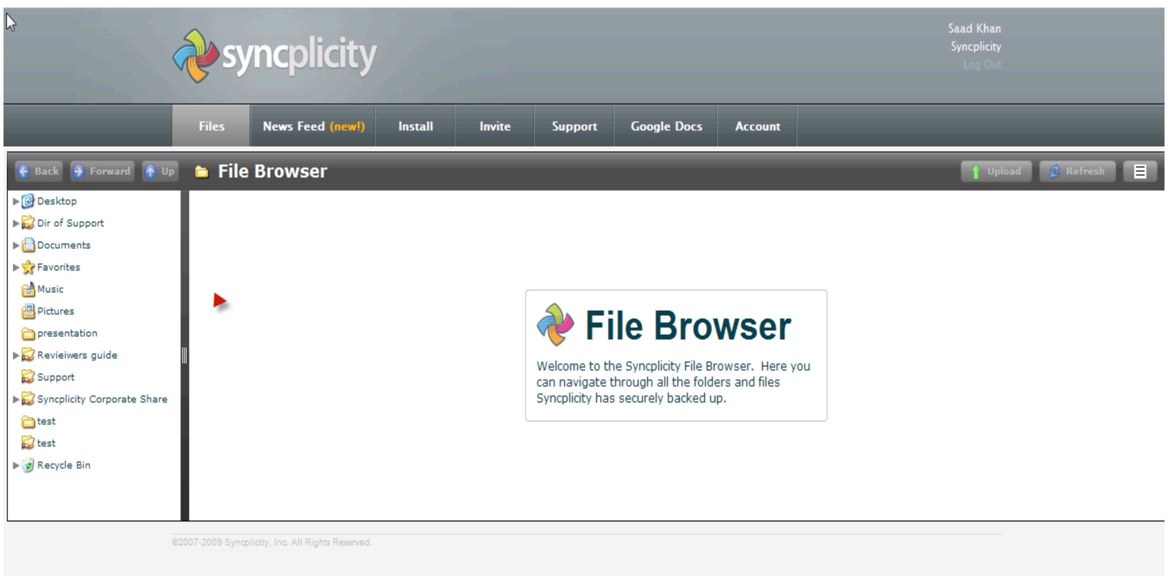
Please keep in mind that the **Change location** link will be missing for each of the five default folders – Desktop, Documents, Pictures, Music, and Favorites. These folders are special locations and will automatically choose to sync to the OS specified locations on each platform.

## INSTANT RESTORE OF ANY PREVIOUS FILE OR FILE VERSION BY A USER OR REMOTELY BY AN IT ADMIN

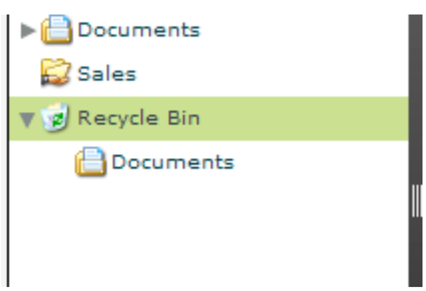
Users can restore content from their Syncplicity account: Any deleted files from synced folders will appear in the Syncplicity **Recycle Bin**. Content that has been accidentally deleted from a computer can be restored from this area. User can also view and restore versions of files from the Syncplicity **Recycle Bin**.

### Action: Restore by User

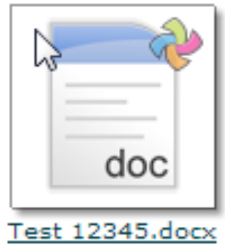
1. Sign in to your Syncplicity account at my.syncplicity.com
2. Click on the **Files** tab



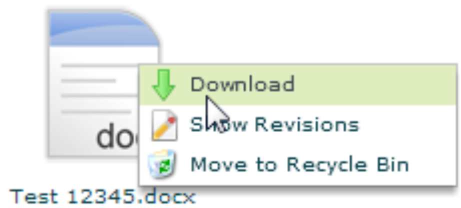

3. Click on **Recycle Bin**



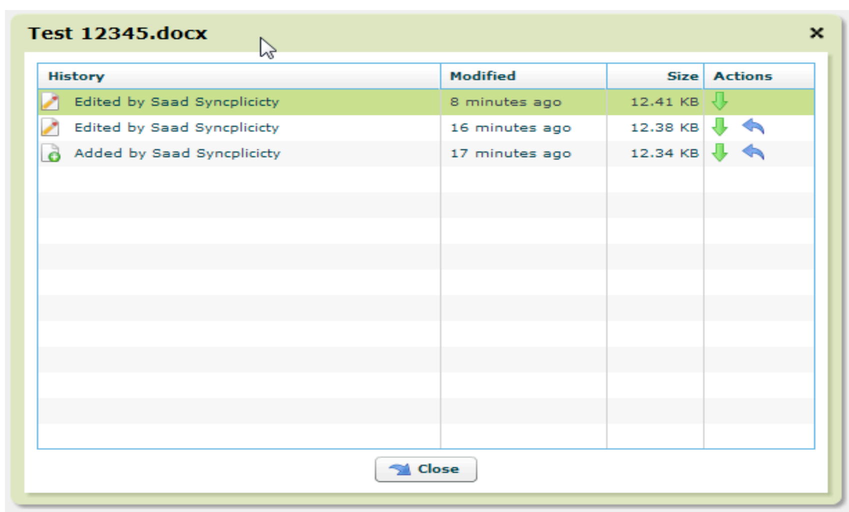

4. Find the folder that contains the file that should be restored
5. Hover over the file thumbnail until the Syncplicity icon appears




6. Click on the Syncplicity icon. To download the latest version, click Download. Previous versions of the file can be accessed by clicking **Show Revisions**




Previous revisions will be show along with a time stamp for audit purposes. Previous versions can be restored by clicking on the corresponding blue arrow or can be downloaded by clicking on the green download arrow.



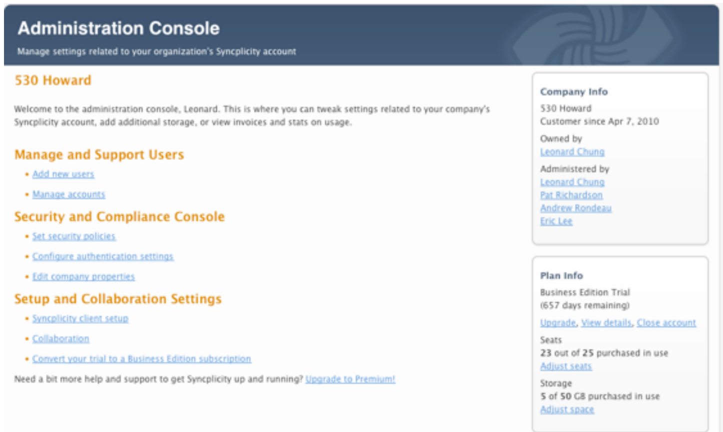

## Action: Restore by an Admin

An Admin can remotely restore a file on behalf of a user by using the **Impersonate** feature.

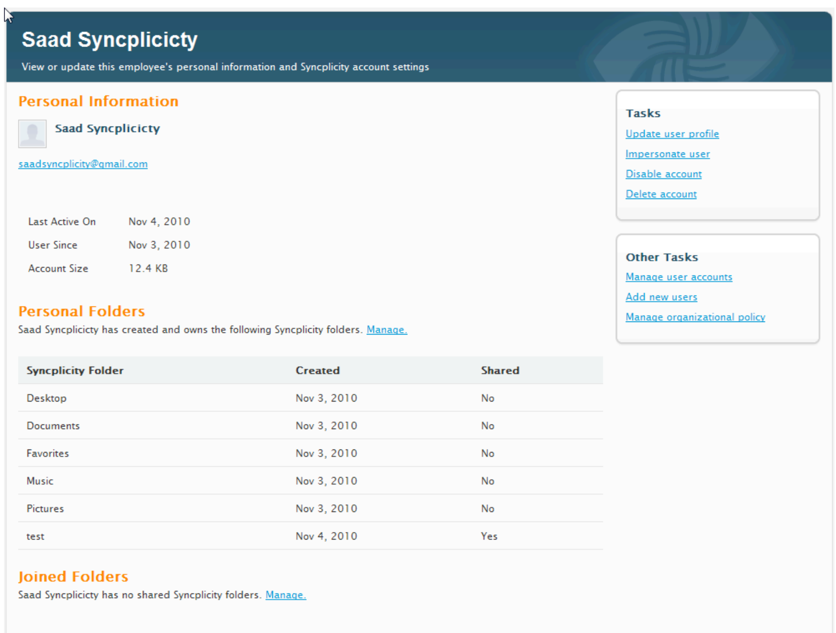
Company administrators have the ability to impersonate different company employees. This allows the admin to see the interface as the user sees it, and help troubleshoot any issues that may be occurring. To impersonate a user:

1. Sign into the Admin Syncplicity account at my.syncplicity.com

2. Click on the **Console** tab




3. Click **Manage Accounts** under the **Manage and Support Users** category.
4. Find the user you with to impersonate and click on their name to open their user information
5. Click the **Impersonate user** link




6. The Admin will now view the console as that user. The Admin can follow the same steps above that a user would perform to restore folders and files to do the restoration on their behalf. To finish impersonating that user, simply click the **Return to Console** text in the orange banner across the top of the screen.

When accounts are impersonated, both the administrators and the impersonated user will receive notification of the impersonation session.

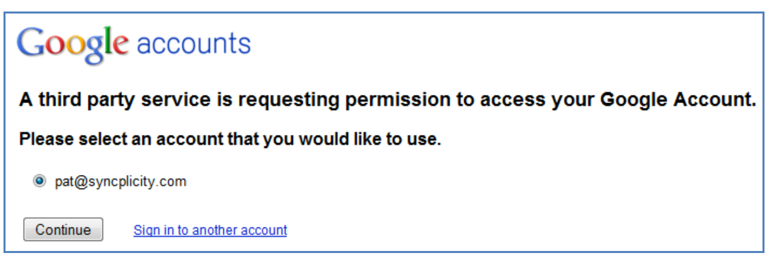
## GOOGLE APPS INTEGRATION WITH SINGLE SIGN-ON AND COMPREHENSIVE GOOGLE DOCS SUPPORT

Syncplicity users can sync Word Documents, PowerPoint Presentations, and Excel Spreadsheets with their Google Docs account. If they have a Google Apps Premier account, they can also sync any other files such as PDFs and ZIP files with Google Docs as well.

### Action: Link and Synchronize Documents with Google Docs

1. If you are linking with a Google Apps account (typically e-mail addresses in a custom, non-Google domain), you will need to have logged into your account at least once through your browser and selected "Stay signed in" for the first linking. You are free to sign out after the initial linkage has occurred.
2. Login to the Syncplicity user account at http://my.syncplicity.com


3. Click on the **Google Docs** tab
4. Click on **Link to Google Docs** button
5. Log into your account
    a. If you are linking to a Google Account (typically accounts ending in @gmail.com), enter in your login credentials into the window and click continue.




    b. If you are linking to a Google Apps Account (typically accounts in a non-Google domain), you should see a screen similar to that above asking you which Google Apps account you wish to link to. If you are instead prompted for a login, you will need to exit this process; your account has not been remembered on this machine. You will need to start the process again from step 1.

6. Grant access to allow Syncplicity to access and synchronize with your Google Docs account
7. Choose a folder in your Syncplicity Account to synchronize with Google Docs. The content of this folder will be uploaded to Google Docs and content from Google Docs will be synchronized to this folder. The recommended setting is My Documents.
8. Select your conversion options. You have a choice of file formats for each file type. When you create a new file within Google Docs, this setting determines what type of file Google Docs will save the new document as on your computer. Existing files and files created in any Google Docs supported file format, such as .DOC, .RTF, and .TXT, on your computer that are modified in Google Docs will always synchronize to and from your computer as their original file type as long as the type is supported. Recommended settings for each file type are the Microsoft Office file types.

   **Note**: If you have a Google Apps Premier account, you can also choose to not convert your files. Your files will be synced but not converted by Google Docs. You will be able to view your files but not edit them within Google Docs. New files created within Google Docs will not sync back to your Syncplicity account.
9. Click Finish.

Once Google Docs has been linked with a given user account, Business Edition will immediately begin to upload files to Google Docs. Depending upon the total size, number of files, and current Google server load, it may take between 10 to 20 minutes before files and folders first begin to appear within Google Docs as Google converts and indexes each file.

Future files sync'ed between Syncplicity and Google are processed more quickly, typically taking about two minutes to appear in Google Docs.

**Note**: Google Docs has some limitations on file sizes, types, and may not fully support all Microsoft Office document features. Google Apps Premier currently has a limit of 1GB of storage per user and a 250MB file size limit for any file uploaded. A list of known Google Docs limitations are documented here: http://manual.syncplicity.com/w/page/12564559/Applications#NotesforusingtheGoogleDocsapplication

### Action: Using Google Docs with Desktop Files

1. Create a new file in Word and save it in the Google Docs linked folder or subfolder on your computer.
2. Log into Google Docs, navigate to the parent folder location on the folder display on the left and click on your Google Docs file to open and edit it in Google Docs
3. Click **Save** when you are done editing the file. The file will now be backed up, versioned, and updated within Business Edition and synchronized with your computers and any sharing participants.

### Action: Offline Access and Editing of Google Docs Files

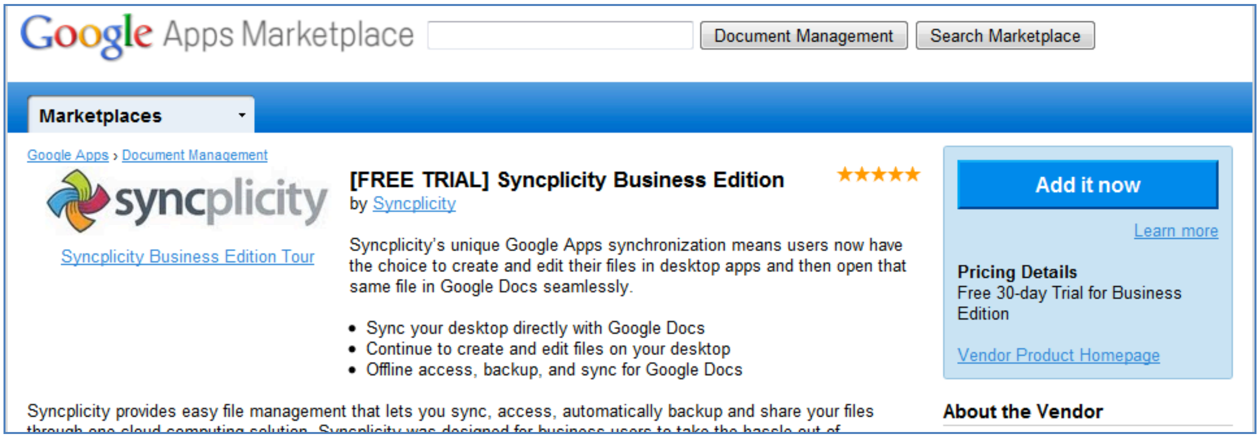
1. Create a file within Google Docs
2. On your computer, open the folder linked with Google Docs
3. Double-click on the name of the file you recently created
4. Your default local application (typically Microsoft Office) will open. Edit and save the file. The file will now be backed up, versioned, and updated within Business Edition and synchronized with your computers, Google Docs, and any sharing participants.

### Action: Enable Single Sign-On with Google Apps Accounts

Rather than require users to remember both a Syncplicity and Google username and password, Single Sign-On allows users to use a single Google username and password to access their user account in both locations.

To enable Single Sign-On with Google Apps,

1. Open the Business Edition product listing within Google Marketplace: https://www.google.com/enterprise/marketplace/viewListing?productListingId=393+9547105767200082343

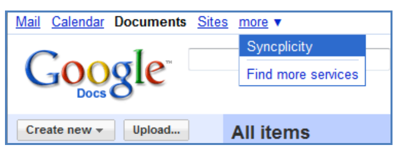



2. Click **Add It Now** and follow the prompts to install and link Google Apps to your Business Edition account. You will need an administrative login for both Google Apps and your company account to continue.

## Action: Associate Google Apps login with an existing Syncplicity Account

Once a Google Apps domain has been enabled for Single Sign-On with Business Edition, users can login by using just their Google Apps credentials.

To access the corresponding Syncplicity user account from Google Apps:




1. Sign into Google Apps account
2. In the top left corner of your Google Apps account, click **More -> Syncplicity**
3. If your Business Edition user account has the same e-mail address as the Google Apps login, Syncplicity will prompt you to review your account information for accuracy, then click **Associate**
4. If your Business Edition user account has a different e-mail address from the Google Apps login and no e-mail address corresponds to the Google Apps login, Syncplicity will prompt you to enter in your existing Syncplicity user account credentials before prompting you to review your account information for accuracy and to click **Associate**.

After performing the first open ID login, users can access the Syncplicity website through the Syncplicity widget under the More menu in Google Apps at any time to gain instant access. In addition, users can use their Google credentials to login directly at my.syncplicity.com.

## POLICY-CONTROLLED MULTI-USER SHARING AND COLLABORATION

### Organizational Policy

Through policies, administrators can define how flexible or locked down they want their Business Edition environment to be. This section of the business console allows company administrators to define general user rights and boundaries. Sharing policies can be defined which control the creation of shares to ensure compliance with corporate data policies. There are four primary policies which control multi-user sharing and collaboration:

- **Registration Wizard Configuration –** Determines whether the user is given the option to configure folders to synchronize and share or to skip user configuration and only use the administrator preconfigured folders and shares.
- **Folder Sharing Policy –** Determines whether users have the ability to share folders with individuals who don't have a Business Edition user account within the company.
- **Shareable Links Policy -** Determines whether users have the ability to share individual files with anonymous people.
- **Share Naming Convention –** Determines whether a share name always has the name of the creator of the share appended to the folder name. Useful for avoiding confusion in situations such as where multiple users may share different folders but name each the same such as "Project Folder".

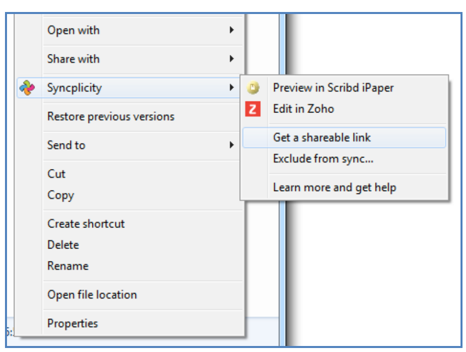
For information on how to modify these policies, please refer to the section below entitled **Central User Creation and Management with Pre-Configuration, And Reporting**.

### Action: Sharing a File as a User

Individual files can be quickly and easily shared through simple URLs called Shareable Links which provide fast, read-only sharing of a file. Shareable Links are links designed with a security code embedded in them to ensure that only people with the full URL can access the file while remaining undiscoverable to people without the URL. In addition, Shareable Links always point to the latest version of a given file. This is useful in cases for reference materials such as a link to an employee handbook which always points to the latest revision of the file.

To create a Shareable Link:

1. On Windows or Mac OS, right-click on the file you wish to share




2. Select **Syncplicity -> Get a shareable link**
3. Copy the link that is produced and provide the URL to those you wish to share the file to

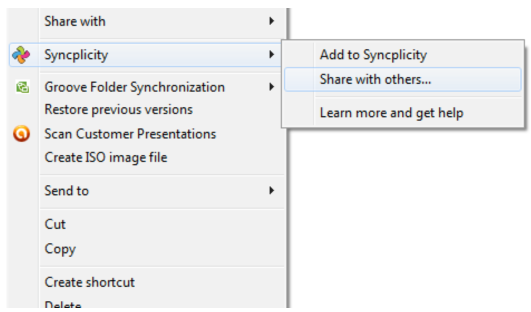
To manage Shareable Links you've created, login to my.syncplicity.com and click on the **Account** tab. Click on the link "View and edit your shared files" to edit or delete sharable links. When a file is deleted, the sharable link associated with it will automatically cease to function.

### Action: Share a Folder

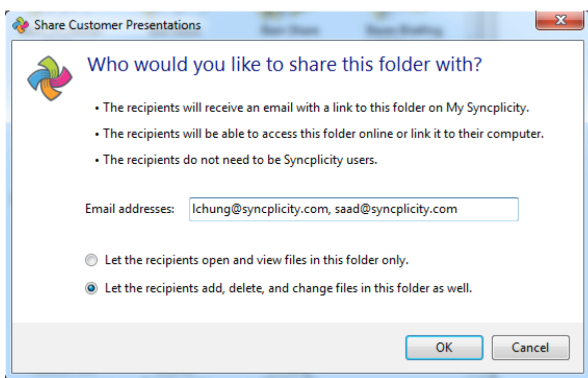
Sharing a folder shares all files and subfolders within it. When adding others to a share, different permissions can be given to different recipients such as restricting some users to only have read access to a given folder through the **Reader** permission versus granting others the **Collaborator** permission to allow them to modify files and folders within a share.

To create a share:

1. On Windows right-click, or on Mac OS Ctrl-click, on the folder you wish to share:




2. Select **Share with others…** from the Syncplicity menu:




3. Enter one or more e-mail addresses of people to share with and click **OK**. The Windows client sharing screen is above. For Mac OS users, a webpage will appear.

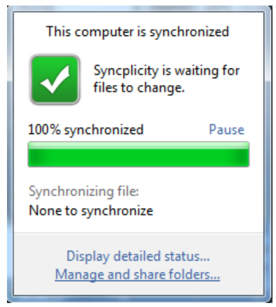
Share recipients are not required to have Syncplicity user accounts, be running the Syncplicity client, or be part of your company account unless an administrator has set policy restrictions prohibiting sharing with non-company users.

**Note:** For more complex sharing, shared folders can be created within folders which are already shared. For example, you may wish to share a Company Share with all of your employees, but right-click and share the Contractor subfolder with just your contractors. Your employees will be able to see and access the Contractor subfolder, but your contractors will not be able to see or access anything beyond the Contractor folder.

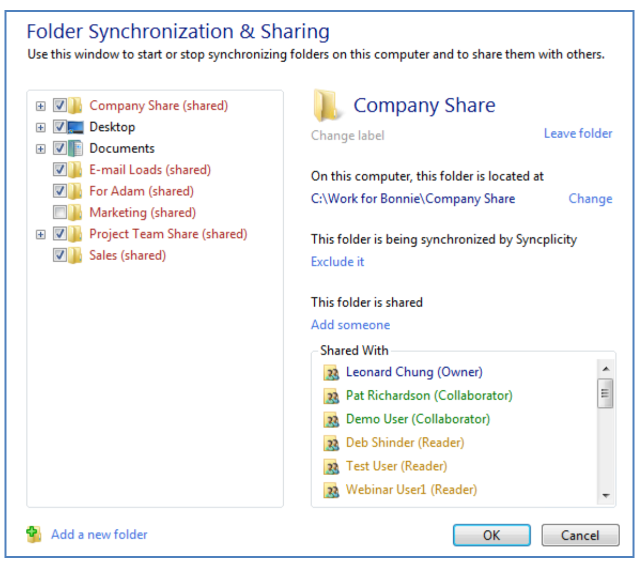
**Note:** The person who creates a share is considered the owner of a share. Unlike other users, this user is the only user who has the ability to empty the Syncplicity Recycle Bin for their folder which means they can erase all record of previously deleted files within folders they own. In addition, owners can add or remove any user, even those who they did not directly invite into their share. In environments with higher security requirements, it is recommended to create shares under a secured administrative account to eliminate the ability of any user to delete from the shared folder's file version histories and audit trails.

## Action: Manage Shared Folders

After a shared folder is created, on Windows a user can click on the Syncplicity logo on the taskbar and click on the **Manage and share folders…** link to open the Folder Synchronization & Sharing window.




Within this window, folders added to the user's account are displayed on the left. The color of the folder name corresponds to its status. Folders in black are private to the user. Folders in dark red and marked **(shared)** are shared with others. By clicking on a shared folder, the user can view information about the share on the right half of the window.

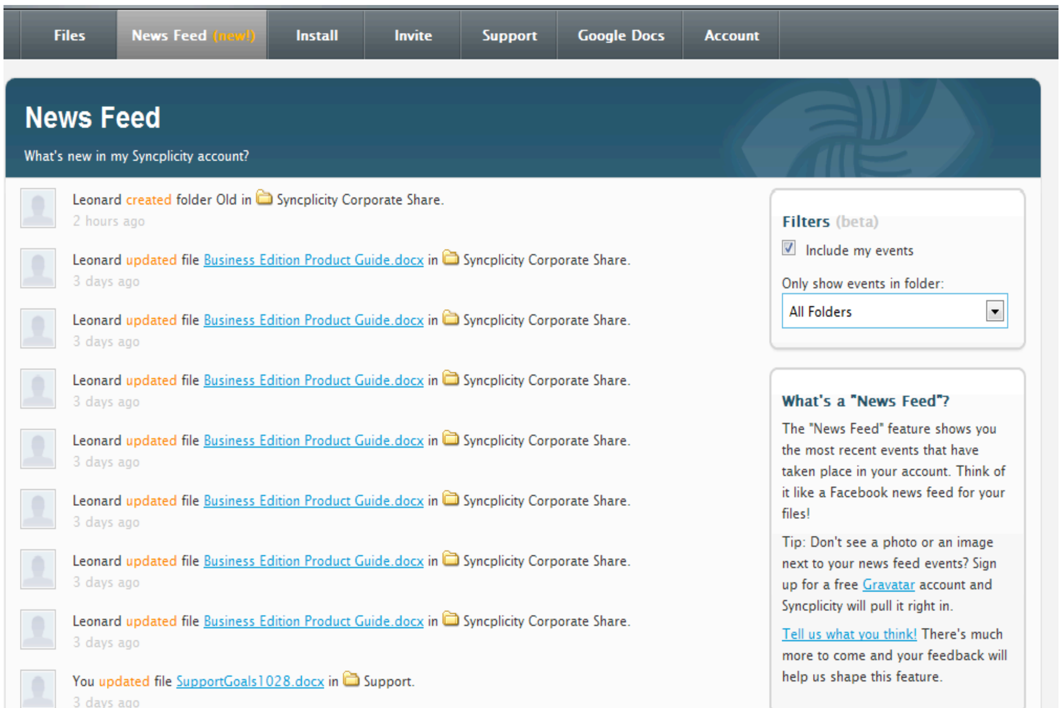



Users the folder is shared with are displayed at the bottom with colors representing their level of access. If the logo to the left of their name is grey instead of in color, this signifies that that user is not synchronizing the folder directly to any of their computers. Red X's will appear to the right of each user name to signify people who the user has permission to remove from the share. Folder owners can remove any sharing participant while individual users can only remove those whom they've invited directly.

To stop sharing a shared folder as a participant, click **Leave Folder**. If the user is the folder's owner, the **Remove Folder** link appears. Clicking this link will remove the shared folder entirely ending the share for all users and removing its existence from the company account.

## NEWS FEED

The News Feed feature shows you the most recent file and folder events that have taken place in your account with information on each action: who performed the action, when it occurred, and where it occurred. Similar events are grouped and previews of image files are displayed inline.




To access the News Feed:

1. Login to my.syncplicity.com
2. Click on the **News Feed** link on the top navigation bar

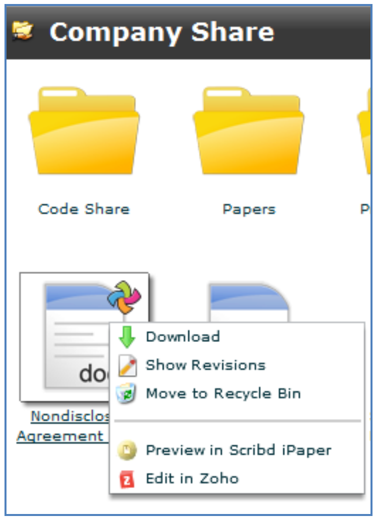
By default, only all of the most recent events are displayed. Events can be filtered by using the filtering options on the upper right of the page.

## ANYWHERE ACCESS TO FILES VIA WEBSITE, CLOUD APPLICATIONS, AND MOBILE DEVICE

Users can access, open, and edit their files across a variety of devices and locations, even if they don't have their computer with them.

### Action: Access via any web browser

1. Using any browser, go to my.syncplicity.com and login
2. Click on **Files** in the navigation bar




3. Navigate to any file and click on it to download the latest version. Previous versions can be accessed by mousing over (putting the mouse pointer over) a file and clicking on the Syncplicity logo that appears on the upper right of the file and selecting **Show Previous Versions**
4. One or more files can be uploaded to a Syncplicity folder through the browser by clicking the **Upload** button on the upper right of the screen.

## Action: View or Edit a file within the browser using Cloud Applications

Syncplicity Business Edition integrates with cloud applications Scribd, Zoho, Picnik and Google Docs for editing and viewing content in a secure environment.

Files can be edited directly via the browser through Business Edition's cloud application integration. To open or edit a file:

1. Mouse over a file and click on the Syncplicity logo.
2. If a supported cloud application is compatible with this file type, it will appear at the bottom of the menu.
3. Select a cloud application with which to open the file and click the corresponding menu option.


4. A new window will appear opening the file within the selected cloud application. If the application supports saving a file, the saved version will be updated within the user account and synchronized.

**Note:** To open and edit files in Google Docs, refer to the Google Apps integration section above.

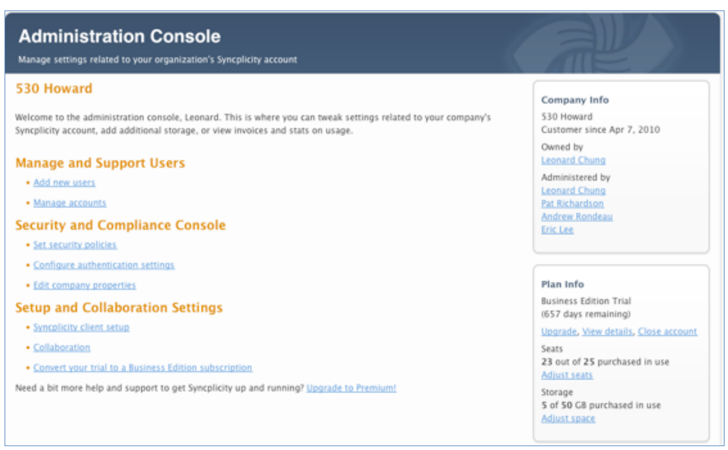
### Action: Access Files via Mobile Devices
A mobile-optimized version of the Syncplicity online file browser is available at m.syncp.com. There is also a third party iPhone app for Business Edition known as MKSync available from the iTunes store

## CENTRAL USER CREATION AND MANAGEMENT WITH PRE-CONFIGURATION, AND REPORTING
Administrators can view and manage all of their users, files, and policies across their organization in a single place using the **Administration Console**.

Through the Administration Console, admins can perform actions such as:

- Bulk create user accounts and pre-configure them with default folders to be backed up and which shared folders each user has access to.
- Set policy controls to automate corporate policy enforcement. For example, pre-configured user account settings can be set to take effect without giving the user the option to modify them.
- Find out what folders Business Edition is managing and protecting down for each user and what data is being shared
- Report on account sizes and last active times across all corporate accounts to understand resource utilization and if there are any users whose computers have not recently checked in and may have unprotected files
- Perform general administration such as activating accounts on behalf of users and changing permissions.

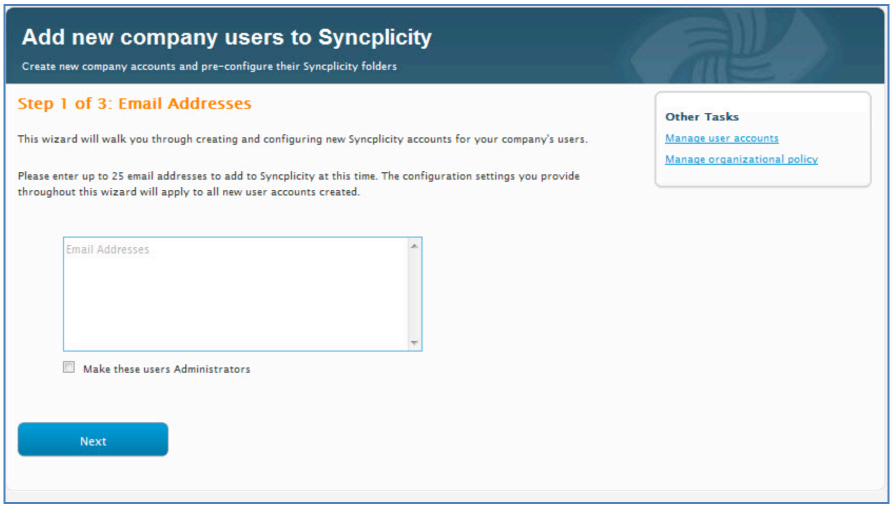
You will need Administrative rights to the company account to access the Administration Console to perform any of the remaining actions in this section. To access the Administration console, go to my.syncplicity.com and login with your administrator account. Click on the **Console** tab to bring up the **Administration Console**.



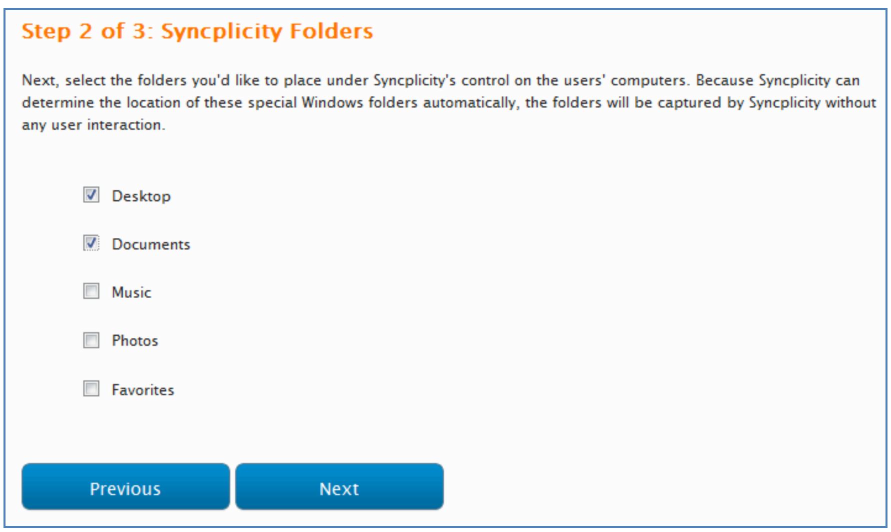

### Action: Adding and Pre-Configuring One or More New Users
Users can be added either one at a time or in bulk. Accounts added can be pre-configured with common settings in a batch to ease provisioning. Since all users added at the same time are configured simultaneously, the recommended practice is to bulk add users by their role so they all have the same configuration.

To add new users to your company account:

1. Click on **Add new users** within the Administration Console.

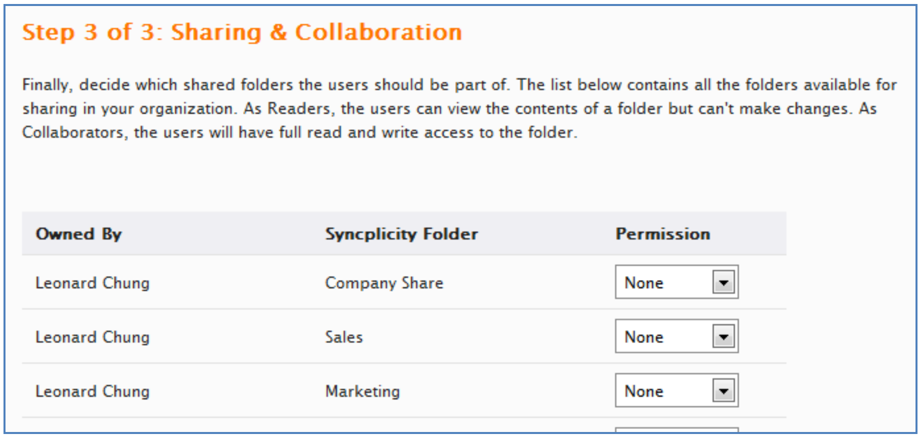



2. Enter the e-mail addresses of users you are creating accounts for with commas between each e-mail address. Alternatively, you can copy and paste a CSV export of accounts.
3. Check the box **Make these users Administrators** if you wish to grant these users administrator rights.
4. Click **Next.**




5. Determine which folders you would like captured and backed up by default on these user's machines. A list of commonly chosen folders is displayed below. Check the box for any folders you'd like backed up and protected by default. These folders will be synchronized and backed up on your employees' computers by default once they install the Business Edition Client.

   **Note**: These are convenient folder defaults. Any folder can be added to a Business Edition account.
6. Click **Next**




7. Decide which shared folders these users should be granted access to. To grant access to a shared folder, change the permission level for a folder from **None** to **Reader** or **Collaborator**. Readers can view files, but cannot edit or otherwise change them. Collaborators can view and edit files and folders within the share. For example here, as new employees, we may grant them Reader access to the Company Share and Collaborator access to the Sales share assuming we are adding a group of sales people.
8. Click **Next**.
9. The settings will be verified and if provisioning is successful, an e-mail will be sent to each user with a link that walks them through the process of setting a password and installing the client. For larger deployments, the Syncplicity client can also be deployed with desktop management systems as well as cloned images.

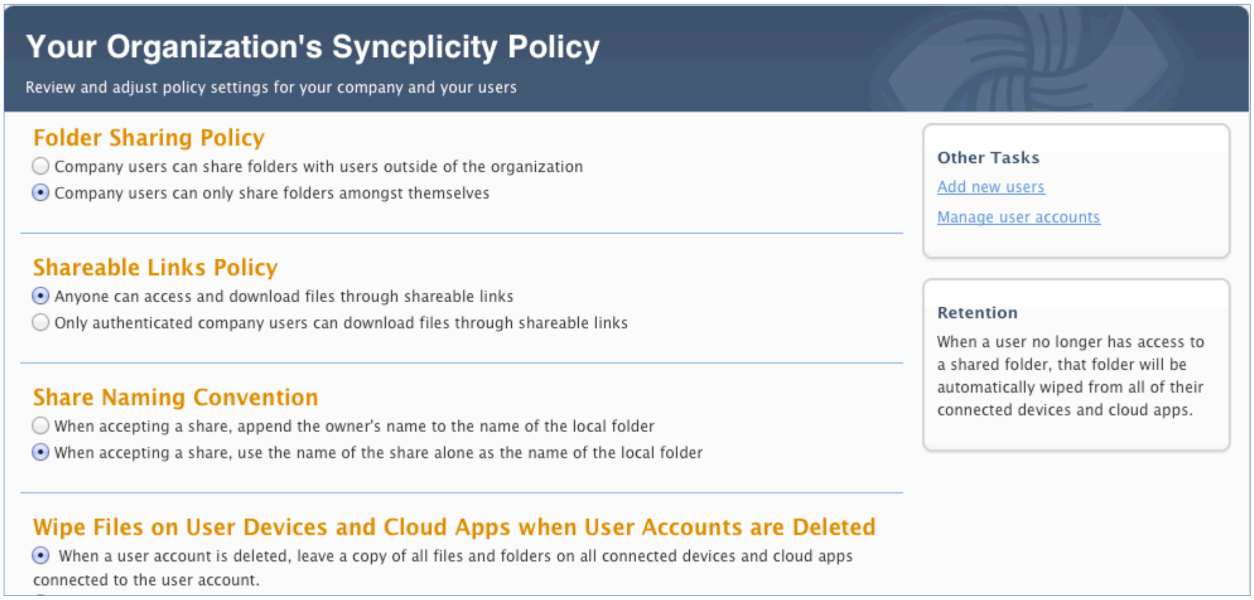
### Action: Define Company Policies

This section of the business console allows company administrators to set core company policy for the use of Syncplicity Business Edition in their organization. There are many different policies that can be set and we encourage you to read about them in the manual. This document covers some of the more basic policy controls with a brief summary of each policy below:

- **Registration Wizard Configuration –** Determines whether the user is given the option to configure folders to synchronize and share or to skip user configuration and only use the administrator preconfigured folders and shares.
- **Folder Sharing Policy –** Determines whether users have the ability to share folders with individuals who don't have a Business Edition user account within the company.
- **Shareable Links Policy -** Determines whether users have the ability to share individual files with anonymous people.
- **Share Naming Convention –** Determines whether a share name always has the name of the creator of the share appended to the folder name. Useful for avoiding confusion in situations such as where multiple users may share different folders but name each the same such as "Project Folder".
- **Client Update Policy –** From time-to-time, new releases of the Syncplicity client are made available with the latest functionality, bug fixes, and performance improvements. This determines whether all installed clients within the company will prompt users to upgrade for any update, required updates, or no updates.

To view and change company policies:

1. Within the Administration Console, under the **Security and Compliance Console** subsection, click **Set security policies**




2. For each policy, check the radio button for the option you wish to set the policy to and click **Submit**

To set **Client Update Policy** and **Registration Wizard Configuration** policies, return to the Administration Console and click **Syncplicity client setup** under the **Setup and Collaboration Settings** subsection.

Policies take effect immediately and affect all future operations but do not affect any pre-existing shares or settings.

## REMOTE HELP DESK

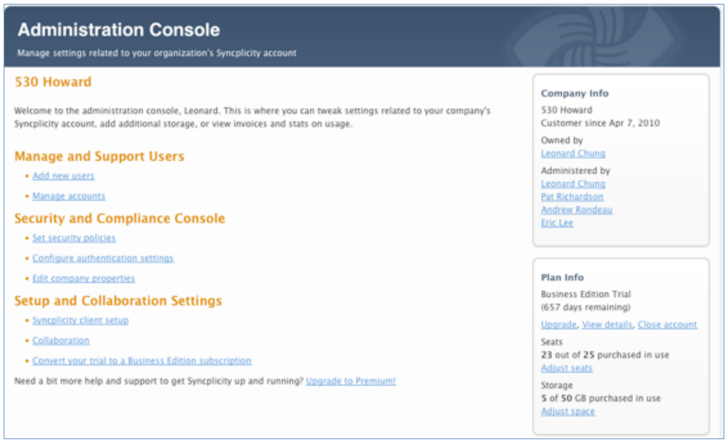
To reduce help desk costs and improve supportability, Administrators can remotely view and modify any user's configuration and perform any action a user can perform on behalf of a user. There are two levels of user management.

### Action: Access and Modify User Account information for a User

In the first level of user management, user account information and all operations which do not involve access or interaction with a user's files are available.

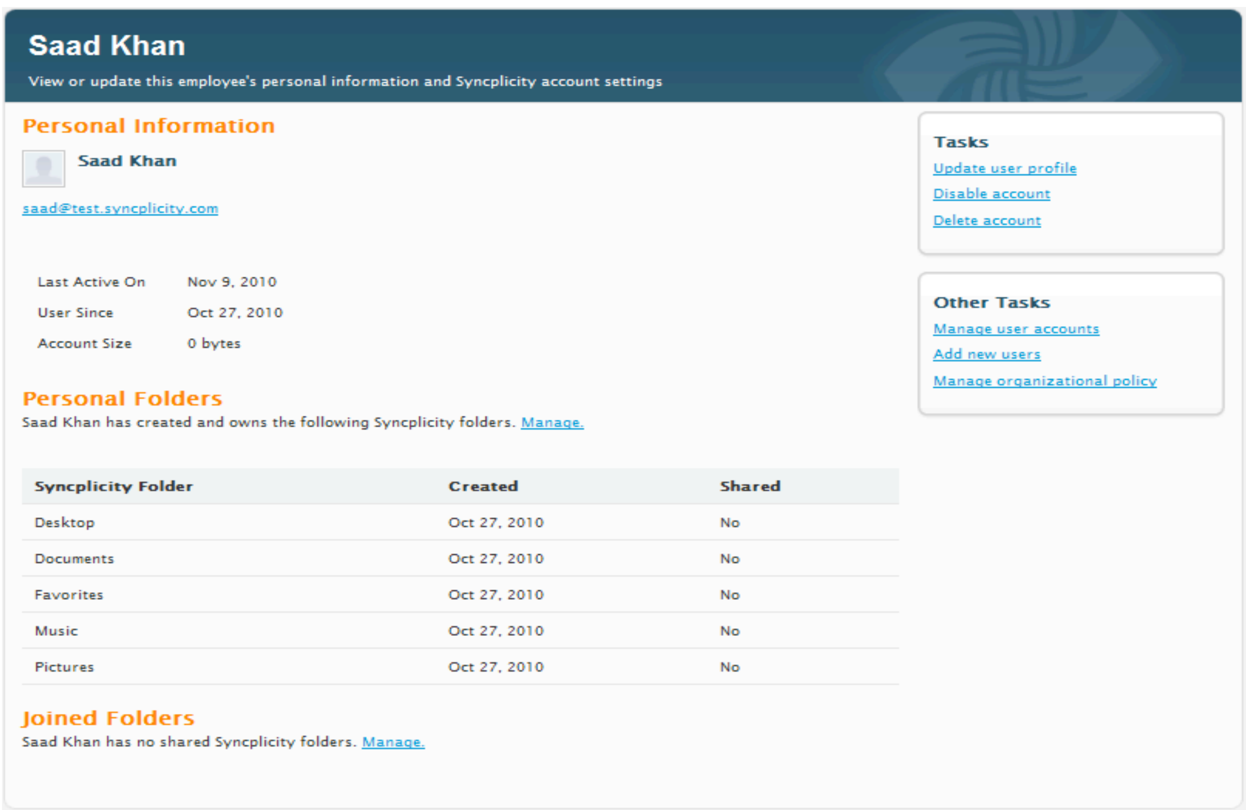
1. Sign into Admin Syncplicity account at my.syncplicity.com

2. Click on the **Console** tab




3. Click **Manage accounts** from the list on the left.

4. Find and click on the user you need to administer. The following screen will appear with the selected user's account information.




This screen displays basic information about the user, as well as which folders are being protected and synced, shared from, and shared with others so an Administrator can view not only folders being managed but also the data flows. By clicking the appropriate **Manage** link, the user's folder and share configuration can be centrally modified here.

To update a user's basic information such as their name or password, click on the **Update user profile** link on the upper right.

## Action: Impersonate a User

Company administrators have the ability to impersonate different company employees. With impersonation, the admin can see and interact with the interface as the user sees it in order to better troubleshoot any issues, perform actions on behalf of the user, or help remotely walk a user through actions over the phone.

**Note**: This is the only area within Business Edition where an Administrator has access to a user's files and file names. For security reasons, when a user account is impersonated, an e-mail is sent to the company account owner, the admin who did impersonation and user who was impersonated to notify them of the impersonation.

To impersonate a user:

1. Bring up a user's account by following the steps above for accessing and modifying a user's account.
2. Click on the **Impersonate user** link
3. You will now view the console as that user and can take actions on their behalf.

To finish impersonating a user, simply click the **Return to Console** text in the orange banner across the top of the screen.

## Business Edition Security Overview

Syncplicity Business Edition delivers a highly secure and dependable file management platform built to meet the requirements of businesses. Ensuring customer data is safe and available are of the utmost importance. In order to achieve the goal of security, Syncplicity's service is built upon many years of experience and uses multiple levels of defense-in-depth to ensure end-to-end confidentiality of customer data.

### Hosting Certifications

All of Syncplicity's servers are housed in data centers that have successfully completed a SAS70 Type II/SSAE-16 audit and testing from independent auditors. SAS70/SSAE-16 certifies that each data center has met rigorous requirements around physical security, physical access, and internal controls.

### Network and Storage Security

All data being transported or stored within Syncplicity is encrypted with the highest levels of encryption available for each phase of its lifecycle to protect files the moment they leave a client's computer. Data in flight and at rest are encrypted using military grade AES encryption set to its highest 256bit level.

AES-256 SSL encryption is used for all authenticated website access, as well as client interactions with the service backend.

All files within Syncplicity are stored with AES-256 encryption using a strongly generated key that is unique to each file revision. In the unlikely case of a brute-force compromise of a given key or a weakness found within the AES encryption algorithm itself, the combination of using the highest level of AES and a unique key per file revision substantially increase security by increasing the level of work required for a compromise and by limiting the potential scope of vulnerability to a single file revision.

All files are stored multiple times in multiple data centers to ensure continued availability. If a file is deleted, the encrypted file itself will be removed from storage and the related encryption key for each of its associated file revisions will be destroyed. When storage is decommissioned, all current providers use the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitation") to destroy the encrypted customer files as part of the decommissioning process.

Internal networks are kept clearly divided from external networks and are protected by industry standard firewall and proxy configurations to prevent unauthorized direct access.

### Two Data Center Policy

For an additional layer of security, Syncplicity maintains all servers responsible for authentication and encryption key management in a separate data center from the data centers housing the encrypted file data. The encrypted file data and proper file version encryption key are brought together only on an as-needed basis and in a tracked manner. By keeping the encryption key completely separate from the file vault, Syncplicity provides a higher level of security by not having a single point of compromise.

### Internal Controls and Process

To ensure proper internal controls on access to customer files, employee access to the Syncplicity infrastructure is controlled and managed. Systems are monitored for security issues and software updates.
Syncplicity only provides data center access to employees who have a legitimate business need. When an employee no longer has a business need, access is immediately revoked. Additionally, employee access to both authentication and key management data centers and encrypted file storage data centers is highly controlled to prevent any potential unauthorized disclosure of customer data

## Additional Resources

User Manual – http://manual.syncplicity.com

Blog – http://blog.syncplicity.com/

Datasheets and Resources – http://www.syncplicity.com/support/resources

Support – https://my.syncplicity.com/Support/