

Getting Started with Remote Wipe and Folder Retention Policy

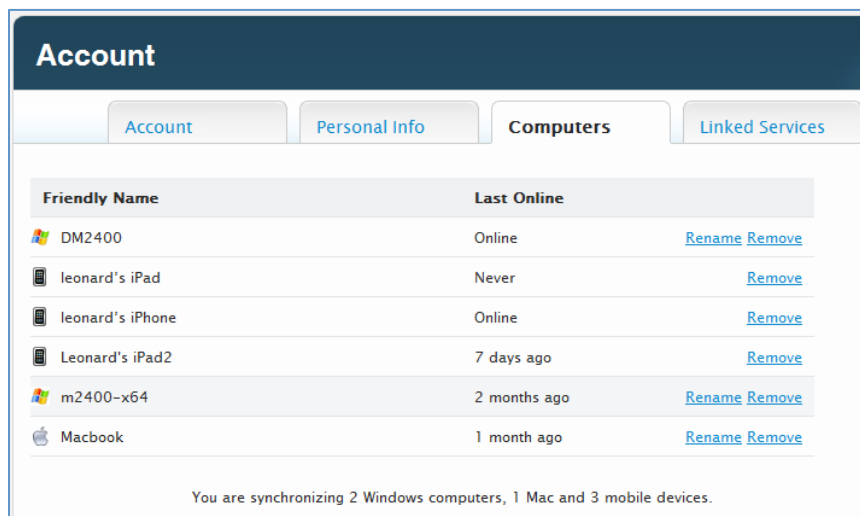
Remote Wipe and Folder Retention Policy are two of the Business Edition features that allow users and administrators to remove files from locations where files and folders are no longer needed to ensure personal and corporate files are not stored on unauthorized locations.

Using Remote Wipe

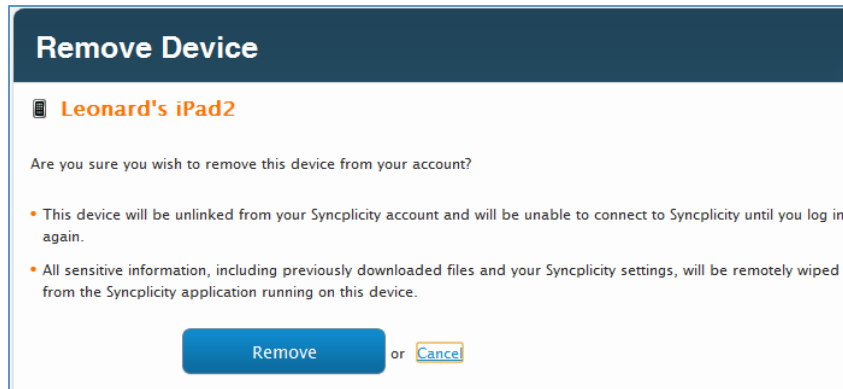
Remote Wipe allows users and administrators to send a command to a mobile device to remove all data and login information stored by Syncplicity in cases where a device is lost, stolen, or otherwise no longer authorized to hold and access user and corporate data. The wipe is done remotely and requires the Syncplicity mobile application is installed on the user's smartphone or tablet.

To initiate a remote wipe for a device, login to your Syncplicity account at www.syncplicity.com. If you are an IT administrator and you are performing a remote wipe on behalf of a user, after logging into your account, you will next need to impersonate the user whose device you wish to wipe. If you are unfamiliar with impersonation, click here to learn more [<http://manual.syncplicity.com/w/page/38337528/How%20do%20I%20remotely%20support%20my%20users>].

Once logged in, click on **Account** tab at the top of the screen and then the **Computers** tab. Click **Remove** on the mobile device you wish to remotely wipe.



A confirmation screen will appear for the device. Click **Remove** to send the remote wipe command or **Cancel** to return to the previous screen.



When the remote wipe command is sent, the Syncplicity app on the smartphone or tablet will permanently delete all files and folders it has stored on the device, will deauthorize the device, and will clear any stored credentials. Depending upon the mobile operating system, this will happen immediately and in the background or will happen the next time the Syncplicity app is started by a user to access their Syncplicity account.

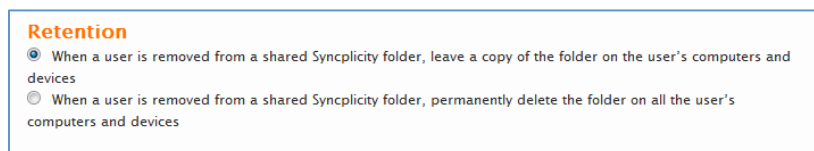
After a remote wipe has occurred, the Syncplicity app will automatically quit but remain installed on the user's device. If the user wants to access their Syncplicity account from the device again, such as in cases where a phone may be lost and then later found, the user will need to start the app and login with their username and password once again to regain access.

Using Folder Retention Policy

Syncplicity Business Edition allows administrators to control whether files and folders are automatically deleted from a user's devices and cloud applications when he or she loses access to a folder such as in a case where a user who has access to a shared folder is removed from the share by the folder owner. When access to a folder is lost, a folder retention policy determines whether the user will continue to have access to files and folders already downloaded or synced to their devices and cloud applications.

To change the Folder Retention Policy, go to www.syncplicity.com and login as an administrator. Click on the **Console** tab and then click on **Set organizational policy**.

A screen will appear that displays all organizational policies within your Business Edition account. Under the **Retention** section, select which folder retention policy you want enforced within your organization and then click **Submit** to save your changes. The new policy will take effect immediately.





There are two policies:

“When a user is removed from a shared Syncplicity folder, leave a copy of the folder on the user’s computers and devices”

If this policy is selected, after a user’s access to a shared folder is removed, that folder and any downloaded or synchronized files will no longer synchronize but will continue to exist on their devices and cloud apps, such as their Windows computer and their Google Docs account. The user will no longer have access to the folder through the Online File Browser or on their mobile device.

“When a user is removed from a shared Syncplicity folder, permanently delete the folder on all the user’s computers and devices”

If this policy is selected, after a user’s access to a shared folder is removed, that folder and any downloaded or synchronized files will no longer synchronize and any files and sub-folders within that folder will be permanently deleted from their devices and cloud apps. The user will no longer have access to the folder through the Online File Browser or on their mobile device. If a device is offline when access is removed, the folder will be wiped the next time the device connects to the internet.

Any new folder retention policy will automatically take effect for all unshare operations performed after the change is set.