



Getting Started with Client Restrictions

Client Restriction Policies allow an organization to control which computers and devices can be used with Syncplicity by controlling which can be part of your organization's Virtual Private Cloud depending upon your organization's needs. In more permissive organizations, users are generally allowed to synchronize their files to all of their devices and can access their files from anywhere. In higher compliance organizations, IT may need to more strongly control where files can go, such as prohibiting synchronization of folders or web access to files from unauthorized machines such as a non-company owned computer.

Syncplicity Business Edition's Client Restriction Policies allow administrators to control:

- 1) Which computers are allowed to run Syncplicity
- 2) Whether Syncplicity mobile apps can be used
- 3) Whether users can access their accounts via web browser on computers that don't have the Syncplicity client installed

Enabling Client Restrictions

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. The Client Restriction Policies are a set of three policies.

Desktop Client Active Directory Restriction Policy

Company users can install and run Syncplicity on any computer

Company users can install and run Syncplicity only on computers joined to the following Active Directory domains:

Only apply this policy to desktop clients running on Windows PCs

Mobile Application Access Policy

Company users can access their accounts using Syncplicity's native mobile applications for iPhone, iPad, and iPod Touch

Access from Syncplicity's native mobile applications is restricted

Website Access Policy

Company users can access My Syncplicity and the mobile website from a web browser on any computer

Company users can access My Syncplicity only from computers running an authenticated Syncplicity client. The mobile website will be inaccessible

DESKTOP CLIENT ACTIVE DIRECTORY RESTRICTION POLICY

The Desktop Client Active Directory Restriction Policy allows an organization to only allow Syncplicity clients to be used if they are installed on computers joined to the corporate Active Directory Domain.



Active Directory domain names are usually the full Domain Name System (DNS) name of the domain. However, for backward compatibility, each domain also has a pre-Windows 2000 name for use by computers running pre-Windows 2000 operating systems which is sometimes also used. For example, a user may have the DNS form login “leonard@corp.syncplicity.com” and the pre-Windows 2000 login “SYNCPLICITY\leonard”. The Active Directory domain name in the first example would be “corp.syncplicity.com” while the Active Directory domain name in the second example is “SYNCPLICITY”.

To enable Desktop Client Active Directory Restriction Policy, click on the option **“Company users can install and run Syncplicity only on computers joined to the following Active Directory domains”** and enter the authorized Active Directory domain name into the text box. If you have multiple Active Directory domain names, use commas to separate each one.

You will also need to decide whether you want to have this policy apply to only Windows computers or to all operating systems. Note that MacOS computers are not able to natively join an Active Directory domain so if you leave this box unchecked only Windows domain joined computers will be able to use the Syncplicity client. If the box is checked, enforcement of the policy is only performed on Windows computers and not on non-Windows operating systems.

This change takes effect immediately for all new computers and within 90 minutes for all computers with Syncplicity already installed.

MOBILE APPLICATION ACCESS POLICY

IT administrators can restrict whether users are allowed to use Syncplicity’s mobile apps to access their account through the Mobile Application Access Policy. If the policy is set to **“Access from Syncplicity’s native mobile applications is restricted”**, no users within the organization will be able to use Syncplicity’s mobile apps including all users who are already using a mobile app. This policy does not affect the ability of users to access their account via mobile web browsers. Website access is controlled through the **Website Access Policy**.

This change takes effect within five minutes.

WEBSITE ACCESS POLICY

Website Access Policy allows organizations to restrict access to Syncplicity through both desktop and mobile web browsers to prevent access from anonymous devices. If the policy, **“Company users can access My Syncplicity only from computers running an authenticated Syncplicity client”** is enabled, users can only access their Syncplicity accounts through a properly authenticated Syncplicity client on their computer. If users attempt to login without using their authenticated Syncplicity client, the login will fail with an error.

Note: The company account owner and users with administrator access always have the ability to login directly from a web browser.



To access their account through My Syncplicity, Windows users can right-click on the Syncplicity icon on the taskbar and click **Browse to My Syncplicity**. Additionally, they can also click on the Syncplicity icon, click **Display detailed status**, and then click **Browse to My Syncplicity**. MacOS users can access My Syncplicity by clicking on the Syncplicity icon in the menu bar and then selecting **Browse to My Syncplicity**.