



Getting Started with AD/LDAP SSO

Active Directory and LDAP single sign-on (SSO) with Syncplicity Business Edition accounts allows companies of any size to leverage their existing corporate directories and authentication systems to authorize employee access to Syncplicity. Instead of setting up yet another username and password for each employee in Syncplicity, IT administrators are now able to configure Syncplicity to delegate authentication to their own systems. This process is also referred to as federated authentication because Syncplicity's servers and the company's servers work together, in federation, to process authentication requests.

When AD/LDAP SSO is enabled within a Syncplicity Business Edition account, users no longer enter their Syncplicity username and password to access Syncplicity on the desktop, the web, and mobile devices. Instead, they leverage their existing corporate credentials to log in and, in many cases, do so in a completely transparent way with absolutely no forms to fill out. Furthermore, because authentication is delegated to secure, authorized servers outside of Syncplicity's control, Syncplicity servers are never privy to the corporate passwords used in any way – authentication credentials remain squarely in the control of the corporate system.

This presents several key benefits to any AD/LDAP-enabled organization:

- One less password for users to remember and IT to manage
- Simplified user provisioning and management within Syncplicity
- Support for custom authentication schemes, such as two-factor authentication
- Improved security through a centralized credential store and a single authentication endpoint
- Transparent login on AD/LDAP-joined devices (via Windows Integrated Authentication)

Technical Details

Syncplicity's support for AD/LDAP SSO is built on top of an industry-standard SAML 2.0 protocol. This widely supported protocol enables federated authentication between SaaS applications, like Syncplicity, and on-premise directory systems, like Active Directory and LDAP. Key to SAML-based federated authentication is an intermediary server – often referred to as the Identity Provider (IdP) – that speaks the SAML 2.0 protocol and services actual authentication requests. It is usually hosted on-premise with direct access to the AD/LDAP directory for credential validation.

The end-to-end process can be roughly described as follows:

1. An unauthenticated user visits My Syncplicity or runs a Syncplicity client
2. Syncplicity redirects the user to the Identity Provider (i.e. SAML server)
3. The IdP prompts the user for credentials if it hasn't received them already
4. The IdP validates the credentials with the AD/LDAP directory
5. The IdP redirects the user back to Syncplicity and tells Syncplicity who the user is



6. Syncplicity receives the assertion and logs the user in

If the Identity Provider supports Windows Integrated Authentication (like Active Directory Federation Services 2.0) and the user was attempting to log in from an AD/LDAP-joined computer, the entire process takes place behind the scenes, unbeknownst to the user. In other cases, the IdP may prompt the user for their corporate credentials.

There are several ways Syncplicity can determine which Identity Provider to send the user to in step 2. These are discussed further down in this document.

Identity Providers

As mentioned previously, Syncplicity supports all SAML 2.0-compliant Identity Providers. This includes providers such as:

- Microsoft Active Directory Federation Services (ADFS) 2.0
- Ping Identity PingFederate
- Oracle Identity Manager 11g

A guide for configuring Microsoft ADFS 2.0 for SAML-based authentication with Syncplicity is available as a separate download.

Configuration

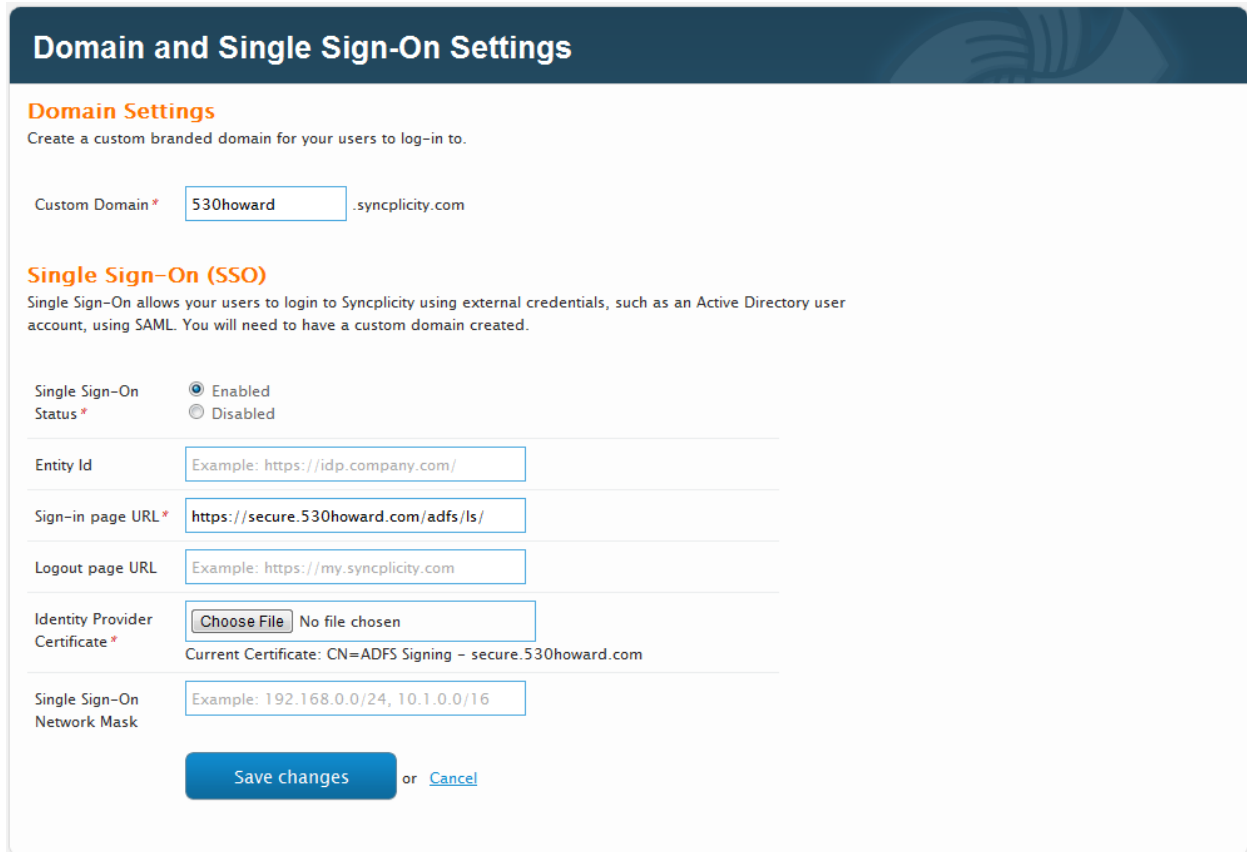
To enable AD/LDAP- based SSO for their account, an IT administrator will need:

- A Syncplicity Business Edition account
- An on-premise Active Directory or LDAP directory service
- A SAML 2.0-compatible Identity Provider server
- A custom branded domain for My Syncplicity
- A sign-in page URL on the Identity Provider used
- The public certificate of the Identity Provider used

Once a Syncplicity Business account is provisioned and a SAML 2.0-compatible Identity Provider installed and configured, Syncplicity must be configured for SSO. The SSO configuration screen is accessible by logging into Syncplicity with an administrative account and clicking on step 5: Configure Single Sign-On:

1. [Set organizational policy](#)
2. [Add new users](#)
3. [Manage user accounts](#)
4. [Edit company properties](#)
5. [Configure Single Sign-On](#)

The Single Sign-On configuration page looks as follows:



Domain and Single Sign-On Settings

Domain Settings
Create a custom branded domain for your users to log-in to.

Custom Domain * .syncplicity.com

Single Sign-On (SSO)
Single Sign-On allows your users to login to Syncplicity using external credentials, such as an Active Directory user account, using SAML. You will need to have a custom domain created.

Single Sign-On Status * Enabled Disabled

Entity Id

Sign-in page URL *

Logout page URL

Identity Provider Certificate * No file chosen
Current Certificate: CN=ADFS Signing - secure.530howard.com

Single Sign-On Network Mask

or [Cancel](#)

Note: form fields marked with a red asterisk are required.

Custom Domain

The Custom Domain field allows administrators to specify the unique URL that they and their users will use when visiting the My Syncplicity website. In addition to branding benefits, this URL allows Syncplicity to immediately determine the company account the user is attempting to log into and redirect the user



to the Identity Provider configured for said account. If users forget to navigate their browsers to the company's custom domain, log in will still be possible; Syncplicity will simply require that user's type in their corporate email address first. The email address is then used to look up the company account.

Single Sign-On Status

The Single Sign-On Status field allows administrators to quickly enable or disable AD/LDAP SSO on their account. It is especially useful when SSO is being first configured: an administrator can fill out and verify all the required fields before officially enabling SSO for their account. This can also be a quick way to disable SSO without losing all the settings that were already configured.

Entity Id

The Entity Id field is optional and further identifies the identity provider used for authentication. Some SAML 2.0-providers require it and when entered, Syncplicity will use it when creating and validating SAML requests and responses.

Sign-In Page URL

The Sign-In Page URL field represents the address on the Identity Provider users will be redirected to for authentication purposes. This URL can be obtained from the Identity Provider.

Logout Page URL

The Logout Page URL field represents the address users will be taken to after they log out of Syncplicity. The My Syncplicity URL at <https://my.syncplicity.com> can be used freely if another custom or specific URL is unavailable or unnecessary.

Identity Provider Certificate

The Identity Provider Certificate field is used to upload the public key of the so-called signing certificate used by the Identity Provider. SAML requires that Identity Providers cryptographically sign their SAML assertions (containing confidential user identity information) and Syncplicity validates the signatures to confirm that the assertion came from a trusted source – that is, the configured Identity Provider. The public key provided in this field will be used to perform the validation.

Click the Choose File button to pick a Base-64 encoded X.509 certificate (usually with a .PEM or .CER file extension) on your computer. Once uploaded, Syncplicity will display information about the certificate underneath the form field.

Single Sign-On Network Mask

The Single Sign-On Network Mask holds the IP address, set of IP address, or an IP address range that users must be visiting from in order to be redirected to the Identity Provider. This security feature limits access to the Identity Provider and thus access to Syncplicity, which may be desirable in certain high-



security environments. On the other hand, it also has the side effect of disallowing users from accessing their data wherever they may be – a potentially undesirable limitation of the service.

The field accepts comma separated values in CIDR notation. More information about the CIDR notation is available at <http://en.wikipedia.org/wiki/Subnetwork>.

Sign In (My Syncplicity)

There are two ways to sign into My Syncplicity with AD/LDAP credentials.

The preferred and recommended way is for users to visit the custom domain their administrator configured on their Business Edition account. For example, when unauthenticated users visit <https://530howard.syncplicity.com>, from the example above, Syncplicity will automatically redirect them to <https://secure.530howard.com/adfs/ls/> for authentication. Furthermore, if the SAML server Syncplicity redirects the user to supports Windows Integrated Authentication and the user is on an AD/LDAP-joined computer, the authentication process will happen automatically in the background and the first page the user sees will be My Syncplicity.

Alternatively, users can continue to log in from the default My Syncplicity login page at <https://my.syncplicity.com>.

Effortless synchronization, backup and sharing
Access your files anywhere, anytime, on all your computers or on the web

Login to Syncplicity

Email*

Password*
[Forgot your password?](#)

or

In this case, users will click the “Login with another account” link (see above), then type in their corporate email address and click Log in (see below).

Effortless synchronization, backup and sharing

Access your files anywhere, anytime, on all your computers or on the web

Login to Syncplicity with a Corporate or Google Apps Account

Corporate Email *

Log In

or [Login with a Syncplicity account](#)

Syncplicity will look up the user's company and its configured SAML server based on the email address the user typed in. It will then redirect the user to the correct SAML server and proceed as normal.