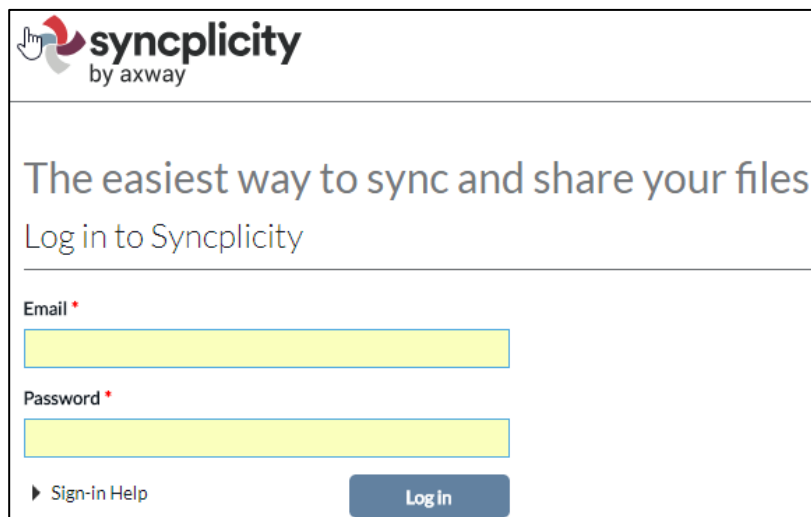


Configuring Syncplicity

Configuring Syncplicity for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to Syncplicity using their enterprise credentials.

To configure Syncplicity for SSO through SAML, follow the steps below:

1. In a browser, type the URL, <https://my.syncplicity.com/> and press **Enter**.
2. Type your credentials, and click **Log In**.



The screenshot shows the Syncplicity login interface. At the top left is the logo with a hand icon and the text "syncplicity by axway". Below the logo is the heading "The easiest way to sync and share your files" and the sub-heading "Log in to Syncplicity". There are two input fields: "Email *" and "Password *", both highlighted in yellow. At the bottom left is a link "Sign-in Help" and at the bottom right is a blue "Log In" button.

3. On the landing page, click **Admin > Mange Settings**.

- From the Manage Settings page, click **Custom domain and single sign-on**.

- The Configure Authentication Settings page appears. Under Domain Settings section, type the following information:

Configure Authentication Settings

Domain Settings

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

Custom Domain* .syncplicity.com **1**

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 **2**
 Disabled

Entity Id **3**

Sign-in page URL* **4**

Logout page URL **5**

Identity Provider Certificate*
 Choose File No file chosen **6**
 Current Certificate
 CN=*.ctxnsqa.com, O="Citrix Systems, Inc.", L=Ft. Lauderdale, S=FL, C=US

Single Sign-On Network Mask **7**

Enable Silent Onboarding - auto-activate users and suppress welcome email (not applicable to self-signup) **8**

or

- i. **Custom Domain**- Type the custom domain, for example, <yourcompanydomain>
- ii. **Single Sign-On Status**- select the **Enabled** radio button.
- iii. **Entity Id**- type a unique issuer ID. For example: yourcompany url
- iv. **Sign-in page URL**- enter the IdP URL, SAML 2.0 endpoint, for example, https://example.com/saml/login.
- v. **Logout page URL**- enter the IdP Log off URL, for example, https://example.com/ cgi/tmlogout.
- vi. **Identity Provider Certificate**- Click **Choose File** to upload the Assertion Signing Certificate. To upload the certificate:
 - a. Remotely access your NetScaler instance using PuTTY.
 - b. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
 - c. Type cat <certificate-name> and press Enter.

```
1 -----BEGIN CERTIFICATE-----
2 MIIFPzCCBCegAwIBAgIQApjY189Tw/6/mHRS5nGDuzAMBgqhkiG9w0BAQsFADBN
3 NQs=
4 allc
5 HTe
6 BAe
7 LJE
8 ADC
9 yVj
10 Kjf
11 vde
12 RK2
13 RYC
14 MBa
15 +Cc
16 Y2V
17 BBy
18 LyS
19 Ois
20 MDC
21 dCE
22 GGF
23 Y2V
24 dDA
25 PA6
26 +Xz
27 gSt
28 c+r
29 UOZLmnmupre1cnaJjor3tiwIL2ckp0u9TqenWZwLAdQ0aLz/m7az0qBzy4ND
30 6EDS
31 -----END CERTIFICATE-----
32
```

d. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

- vii. **Single Sign-On Network Mask**- type the IP address network mask.
- viii. Select the checkbox to enable silent onboarding.

6. Click **Save Changes**.