Configuring Thycotic Secret server

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

Prerequisites

- Licensing & Version
  Secret Server Professional Edition or higher and SAML Add-on Feature License, upgraded to version 10.5 or later
  To install a new SAML license, navigate to Admin > Licenses > Install New License.
- .NET Framework 4.6.2+
  To use SAML 2.0, you need to install .NET Framework 4.6.2 or higher on your web server.

For more information about the prerequisites, refer
https://thycotic.force.com/support/s/article/SS-SAML-Config-Guide#servprov

Administer Configuration SAML Role Permission
To grant a user this permission, from an Administrator account:

1. In a browser, type the URL, https://<domainname>.secretservercloud.com/login.aspx and press **Enter.**

2. On the Home page, navigate to **Admin > Roles > Create New.**

3. In the Role Name field, type the role name. For example, SAML.

4. Check **Enabled**.

5. Select **Administer Configuration SAML** under the right side "Permissions Unassigned" box and move it into the left "Permissions Assigned" box using the arrow buttons.

6. Click **Save**.

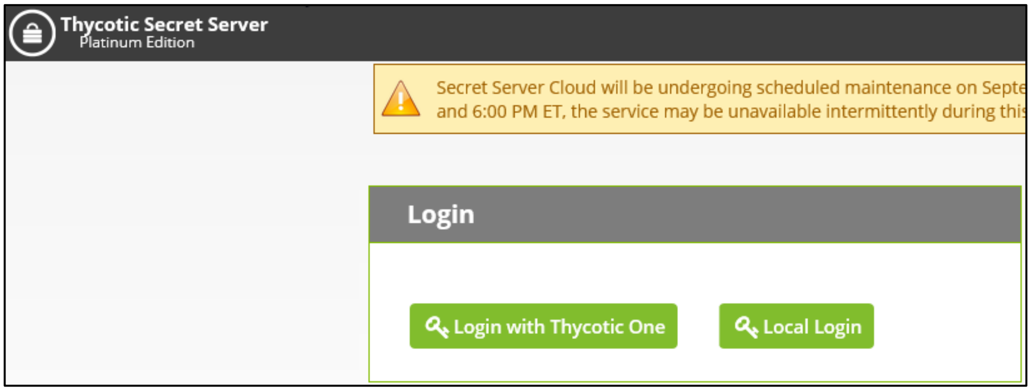
7. Click Back to return to the Roles page, then Assign Roles. Select the Role previously created in the dropdown Role box, then click **Edit**.

8. Assign Users to this role using the arrow buttons and click **Save**.

To configure Thycotic Secret server for SSO through SAML, follow the steps below:

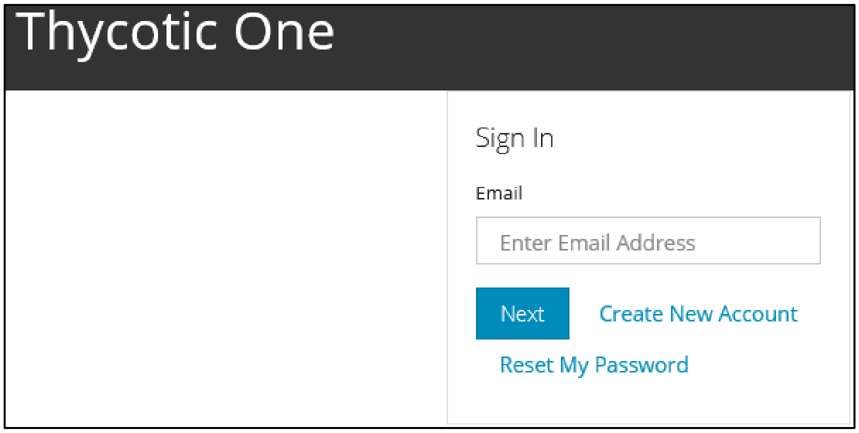
1. In a browser, type the URL, https://<domainname>.secretservercloud.com/login.aspx and press **Enter.**

2. Click **Login with Thycotic One**.



Secret Server Cloud will be undergoing scheduled maintenance on Septe
and 6:00 PM ET, the service may be unavailable intermittently during this

3. Type your email address and click **Next**.



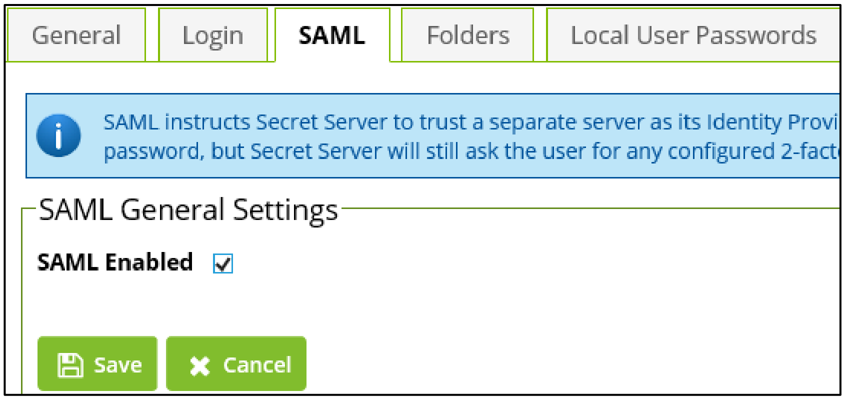
Email

Enter Email Address

4. Type your Password and click **Next**.

5. On the Home page, navigate to **Admin > Configuration > SAML.**

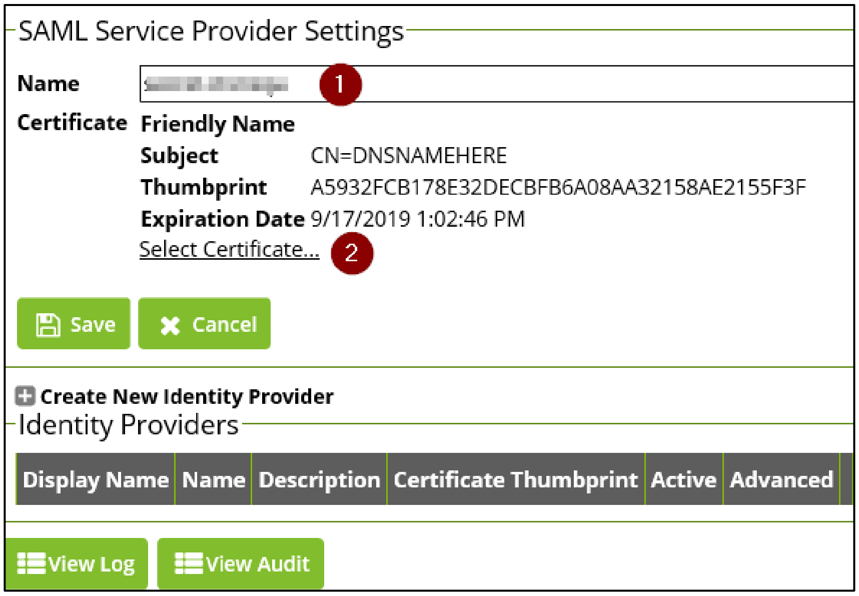
6. Under SAML General Settings, click **Edit**, and check the **SAML Enabled** checkbox. Click **Save.**



SAML instructs Secret Server to trust a separate server as its Identity Provi
password, but Secret Server will still ask the user for any configured 2-fact

SAML Enabled ☑

7. Under SAML Service Provider Settings, click **Edit**. Type the following information:



SAML Service Provider Settings

Name [redacted]

Certificate

Friendly Name

Subject CN=DNSNAMEHERE

Thumbprint A5932FCB178E32DECBFB6A08AA32158AE2155F3F

Expiration Date 9/17/2019 1:02:46 PM

Identity Providers

Display Name	Name	Description	Certificate Thumbprint	Active	Advanced

i. **Name**: Type the name of your Secret Server Service Provider. For example, SecretServerServiceProvider.

ii. Click **Select Certificate**. The Upload Certificate dialog box appears. Type **Password** and click **Upload Certificate**.
Note: You can upload SAML certificate in .pfx file format only.

- For on-premises instances, the uploaded certificate should match the one used for Secret Server's HTTPS configuration, OR it can be created as a self-signed certificate. Refer Powershell script.

- For Secret Server Cloud users, you will need to generate your own certificate using the Powershell script.

When the certificate is uploaded, click **OK**. Then click **Save**.

Note: You need to convert the SP certificate from .pfx to .pem format and then it can be configured on IDP side.

The SSO configuration is completed.