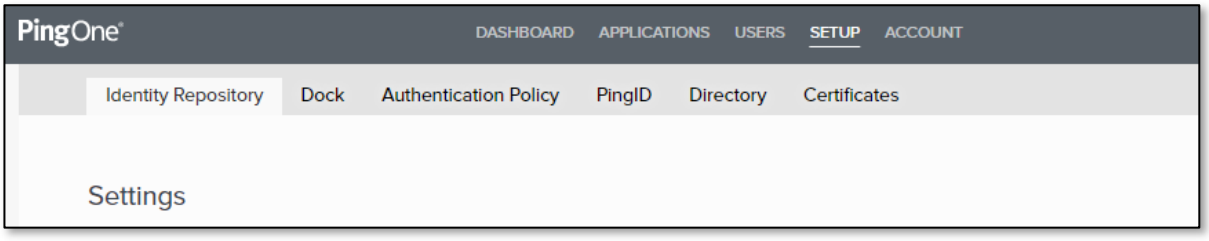
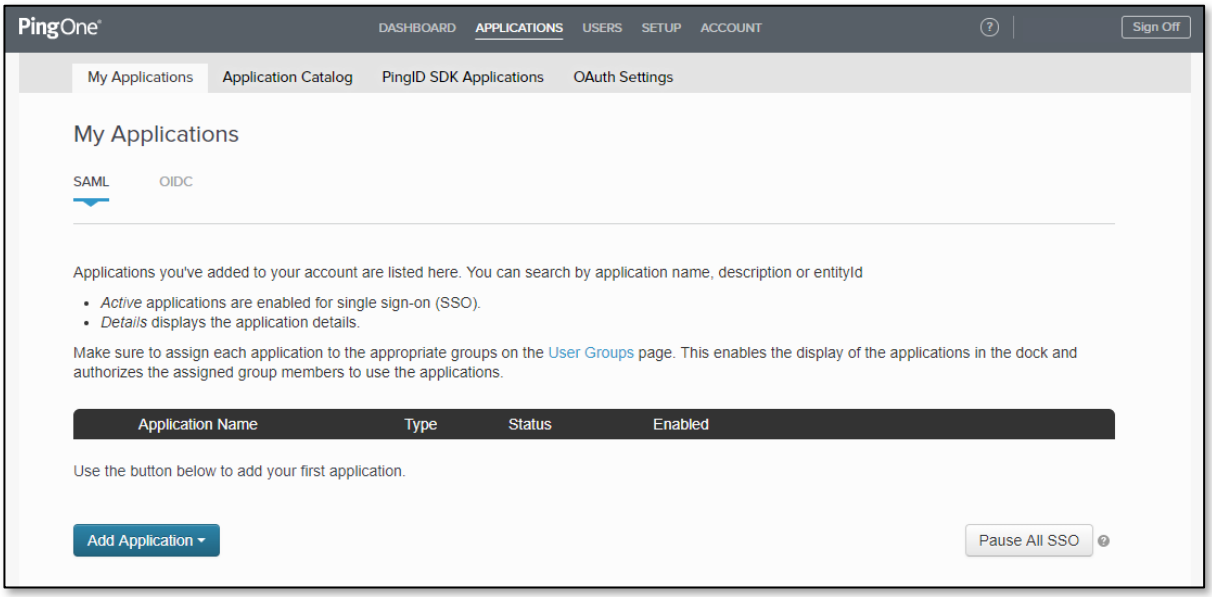
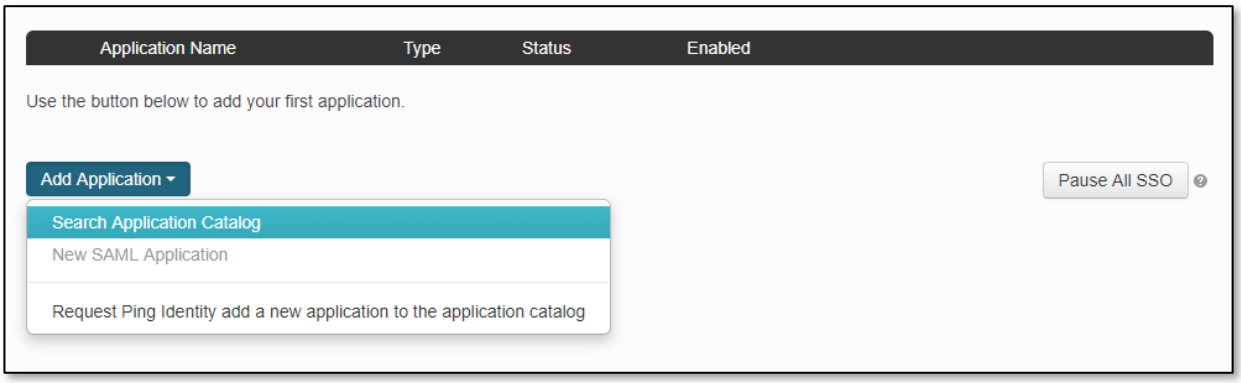
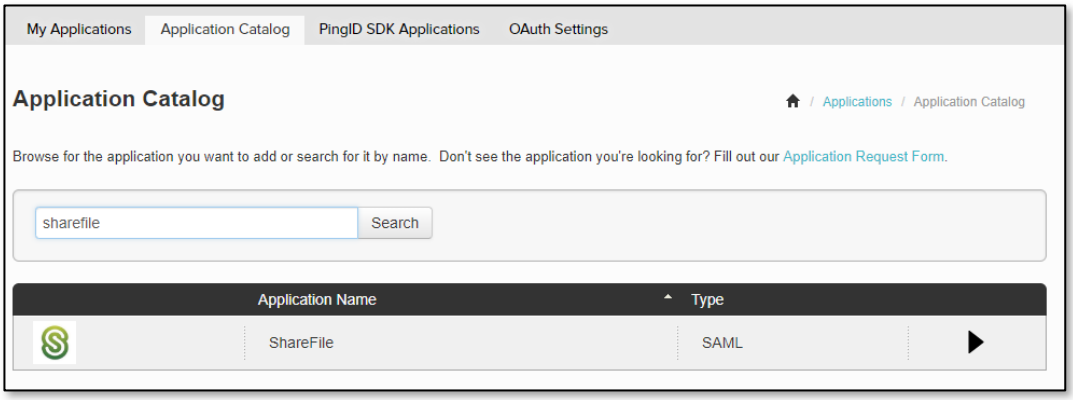
Content Collaboration: Single Sign-On Configuration

PingONE / PingID for MFA

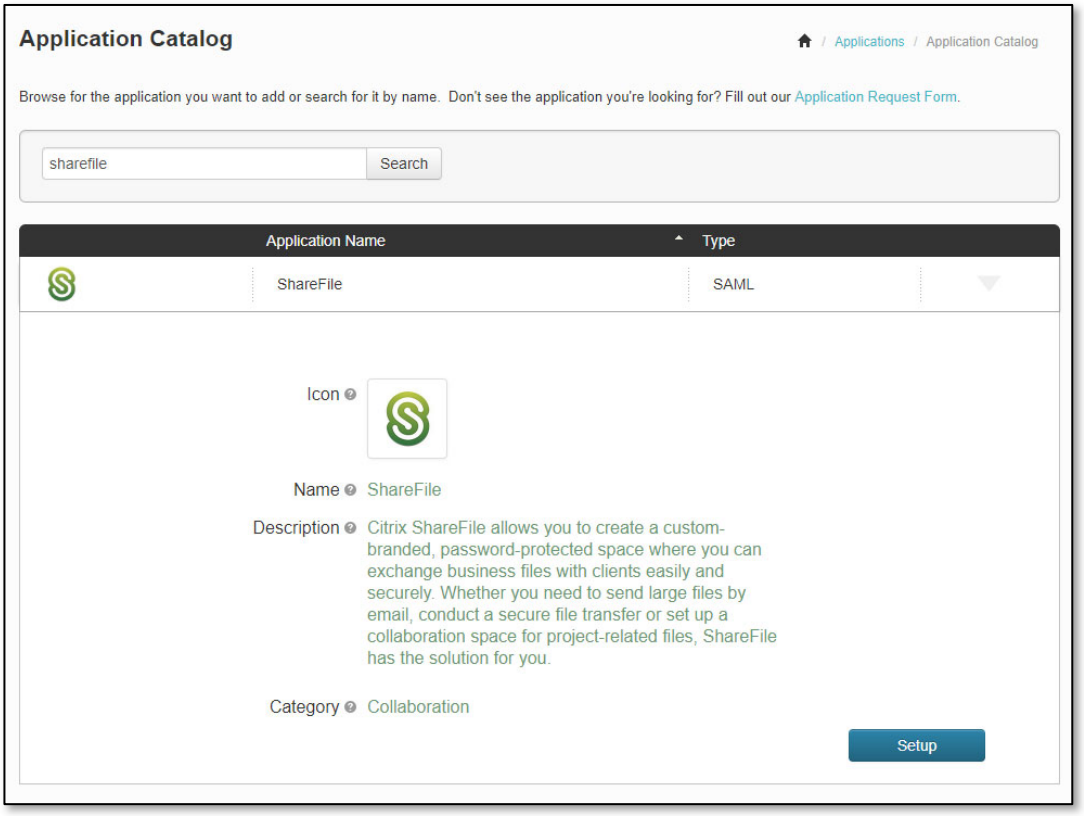
Last Revised: May 2019

LEGAL NOTICE

Steps	Description
1.	Log in to the PingOne Administrator site. For example, login to https://admin.pingone.com/
2.	Be sure the account is connected to an **Identity Repository**. Check Setup for Repository type. 
3.	Click on **Applications.** 
4.	Click on **Add Application** > **Search Application Catalog**. 
5.	Search for “sharefile” in the Application Catalog and select play button.

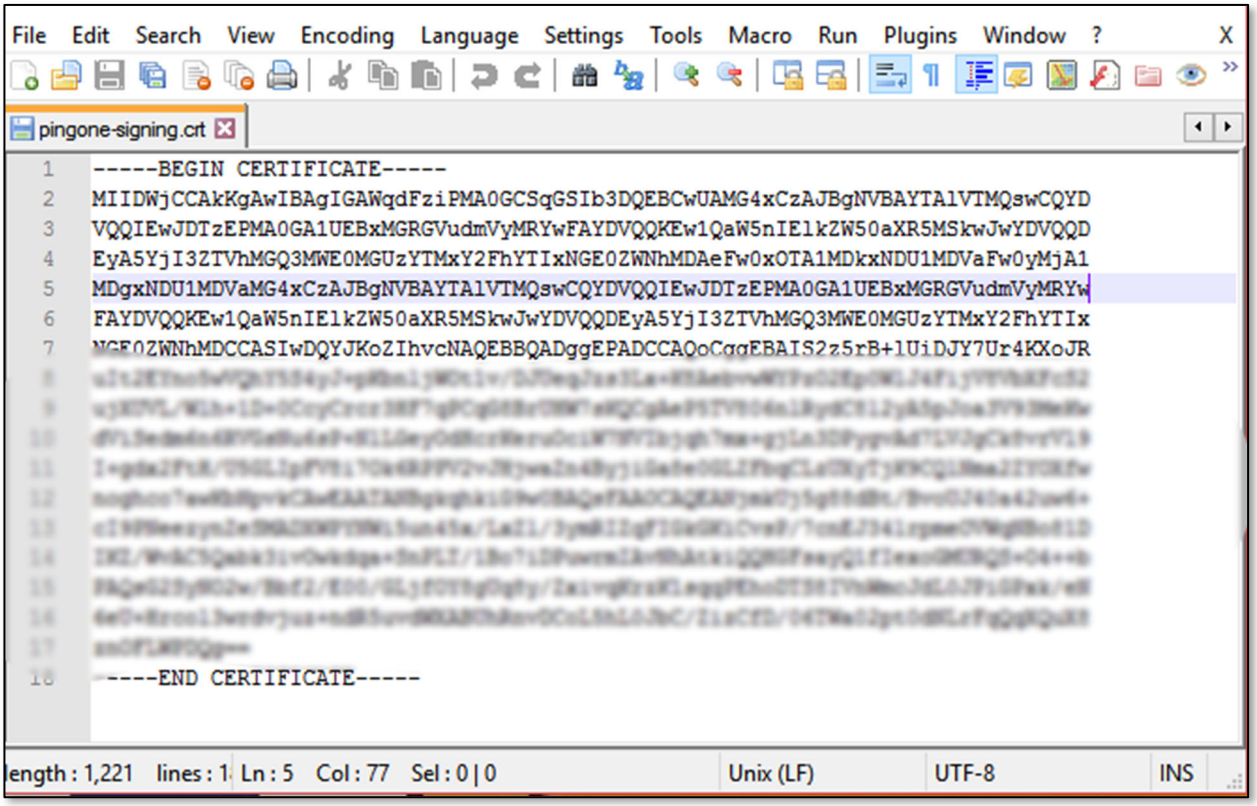


6. Select **Setup** for the ShareFile SAML application.

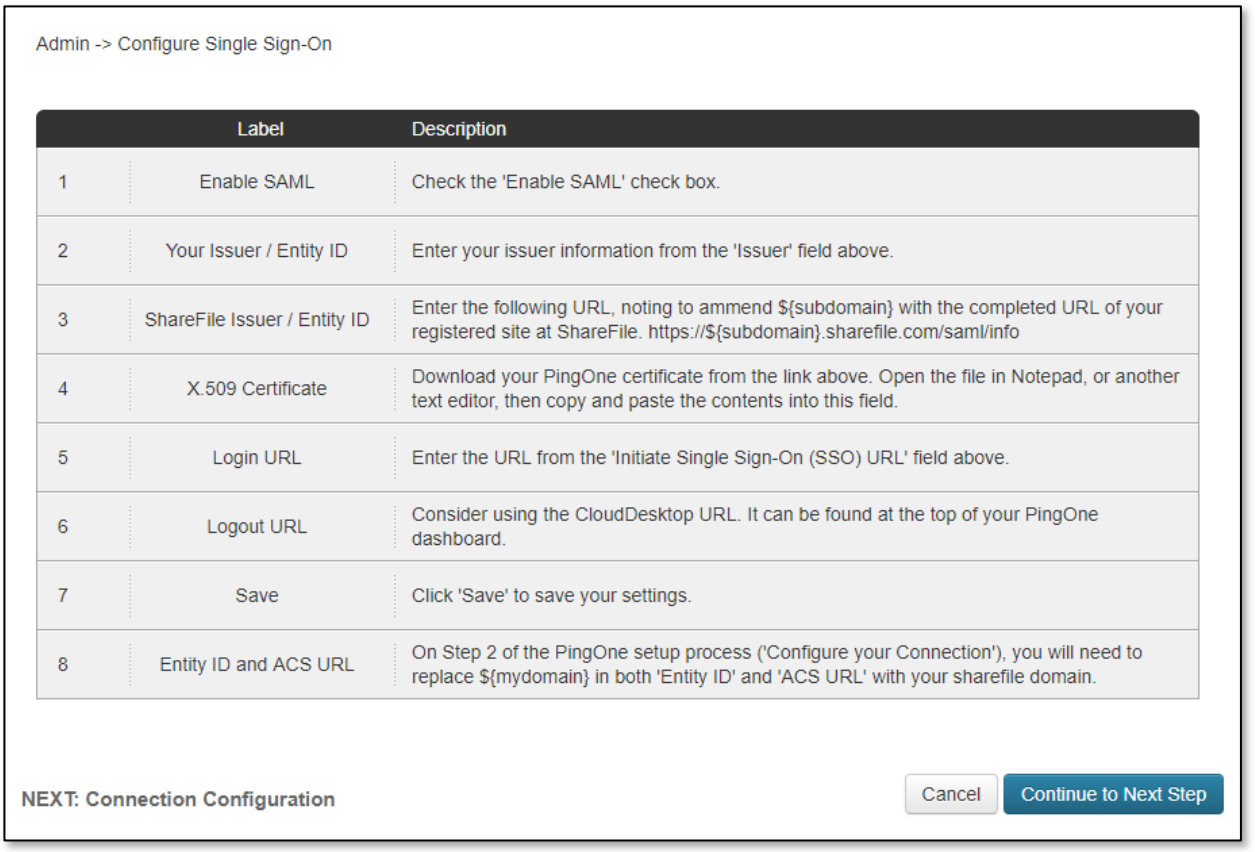


7. Download the Signing Certificate.

8. Open the Signing certificate (.crt) file in Notepad or any text editor.

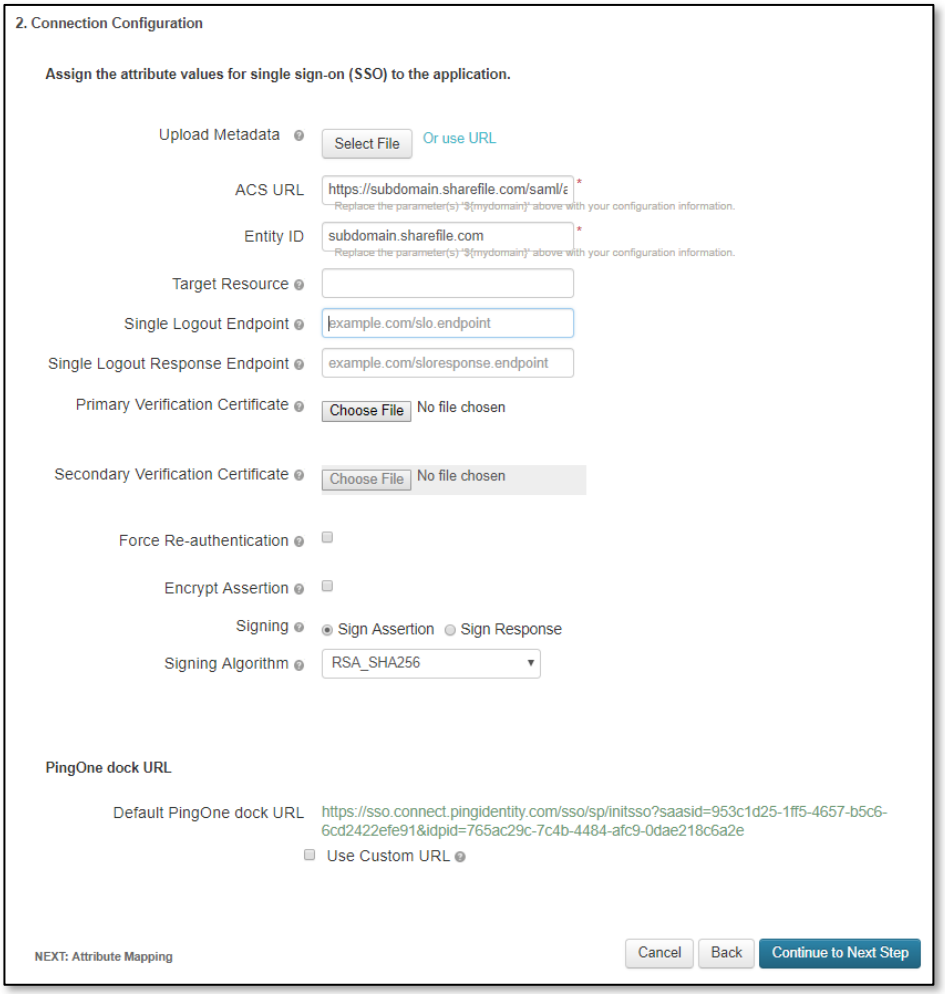


9. In PingOne / PingIdentity, note the table descriptions when configuring ShareFile single sign-on settings and **Continue to Next Step**.

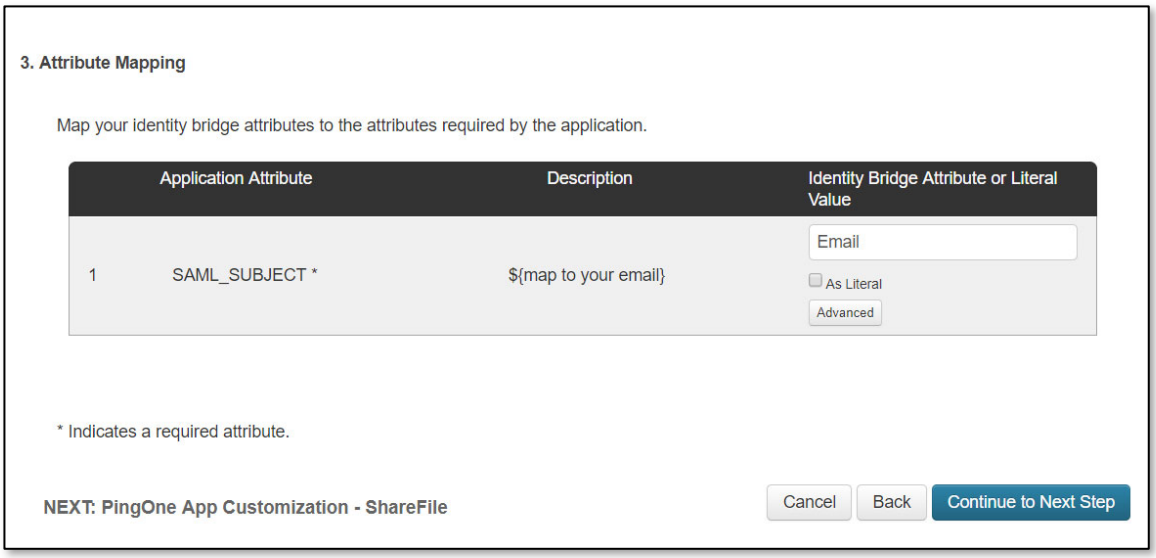


	Label	Description
1	Enable SAML	Check the 'Enable SAML' check box.
2	Your Issuer / Entity ID	Enter your issuer information from the 'Issuer' field above.
3	ShareFile Issuer / Entity ID	Enter the following URL, noting to ammend ${subdomain} with the completed URL of your registered site at ShareFile. https://${subdomain}.sharefile.com/saml/info
4	X.509 Certificate	Download your PingOne certificate from the link above. Open the file in Notepad, or another text editor, then copy and paste the contents into this field.
5	Login URL	Enter the URL from the 'Initiate Single Sign-On (SSO) URL' field above.
6	Logout URL	Consider using the CloudDesktop URL. It can be found at the top of your PingOne dashboard.
7	Save	Click 'Save' to save your settings.
8	Entity ID and ACS URL	On Step 2 of the PingOne setup process ('Configure your Connection'), you will need to replace ${mydomain} in both 'Entity ID' and 'ACS URL' with your sharefile domain.

10. Type in your ShareFile subdomain for **ACS URL** and **EntityID**.

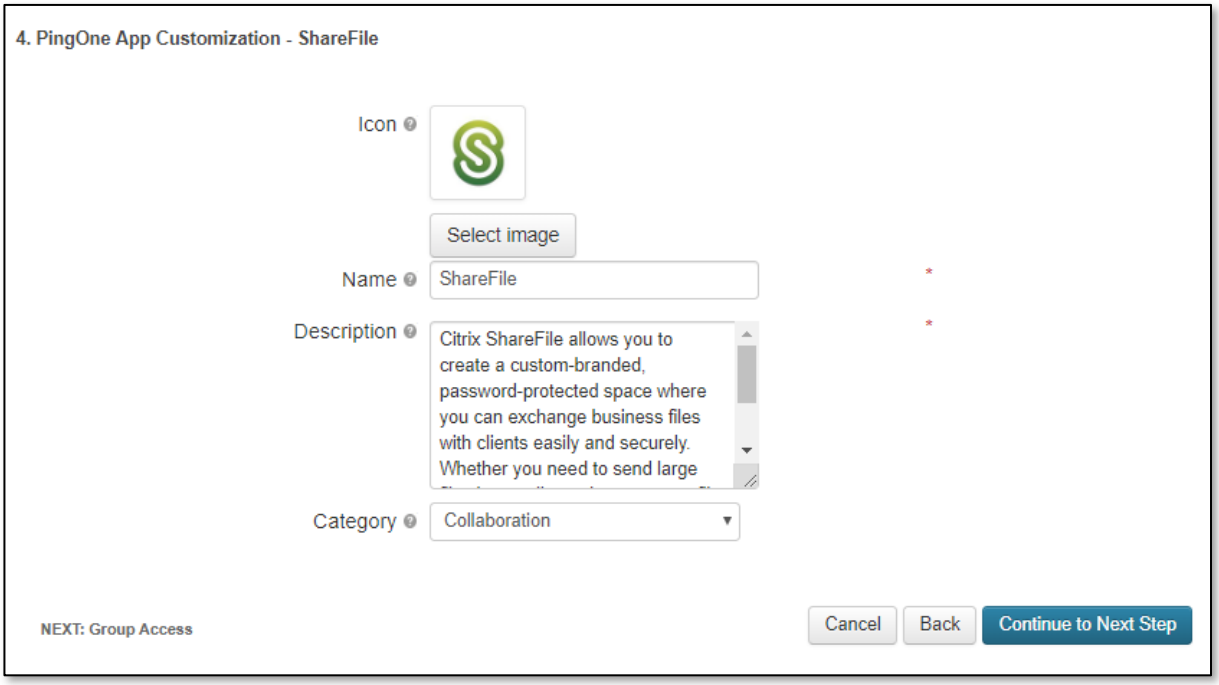
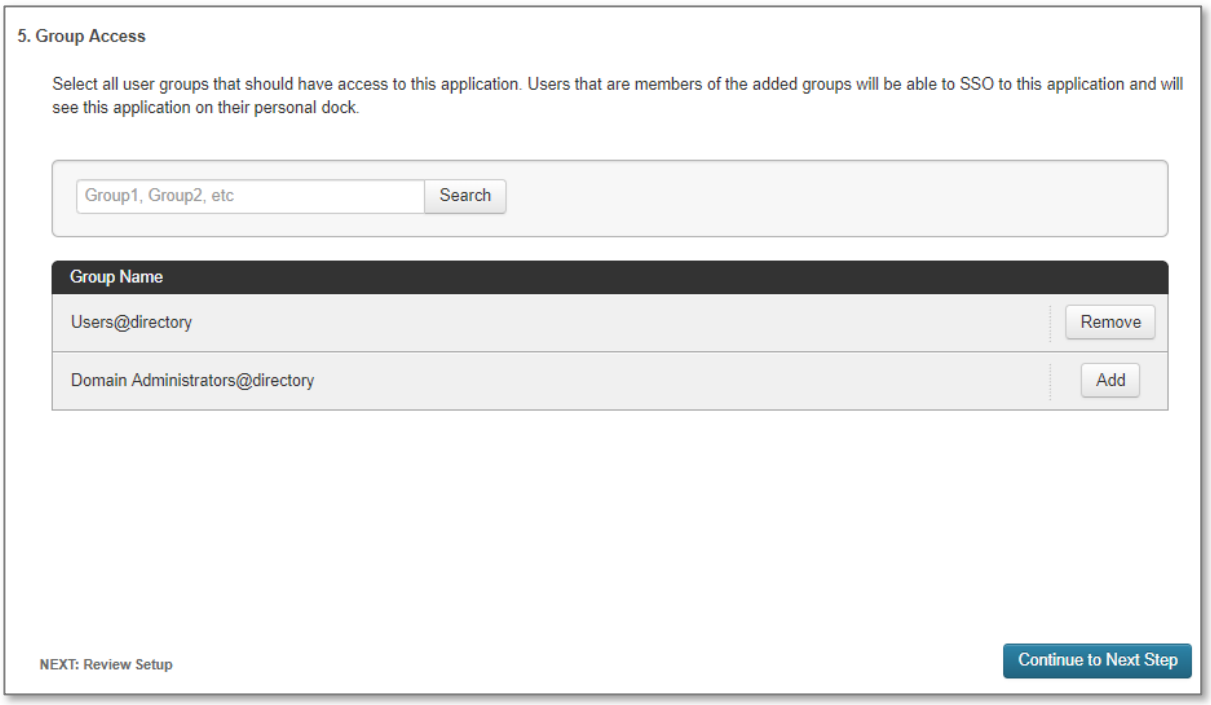


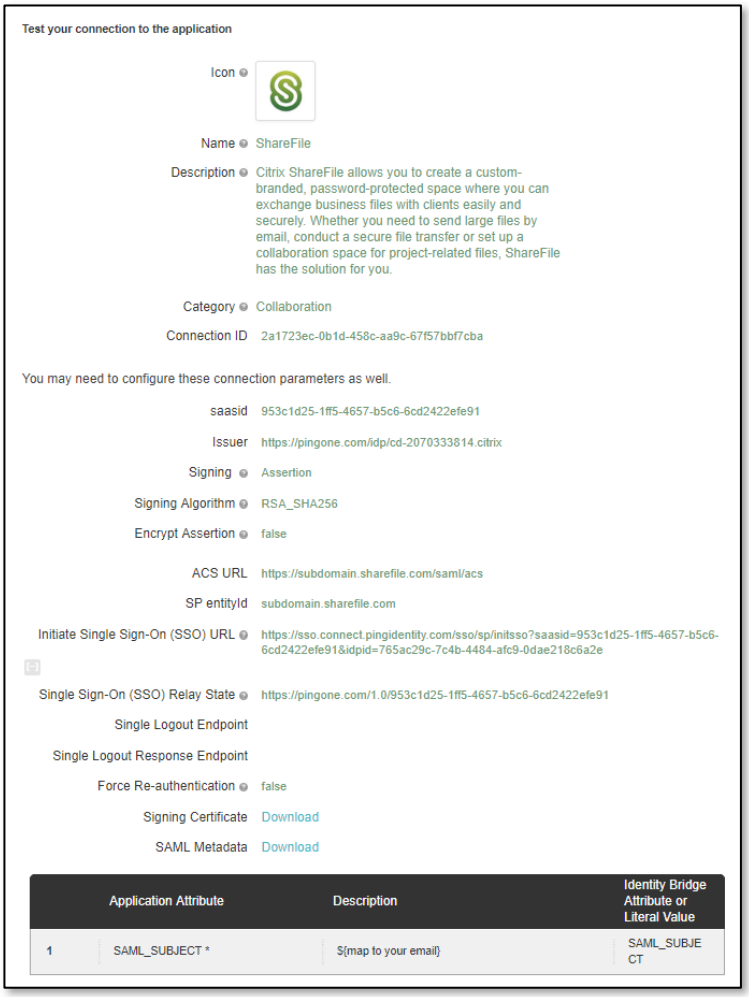
11. In **Attribute Mapping** > **Identity Bridge Attribute or Literal Value** enter **Email**.



***The attribute must map to users email addresses.*

12. Click **Continue to Next Step**.

13.	Customize **ShareFile App** in for PingOne dock. 
14.	**Select** user groups that should have access to single-sign-on into the ShareFile application. 
15.	Review setup settings for ShareFile Application.

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>16.</td><td>Go to your ShareFile account: https://subdomain.sharefile.com

Login with Administrator account > Settings > Admin Settings > Security > Login & Security Policy > scroll down on this page to Single sign on / SAML 2.0 Configuration.</td></tr>
<tr><td>17.</td><td>Configure Single sign on / SAML 2.0 Configuration with the below:

<u>Basic Settings</u>

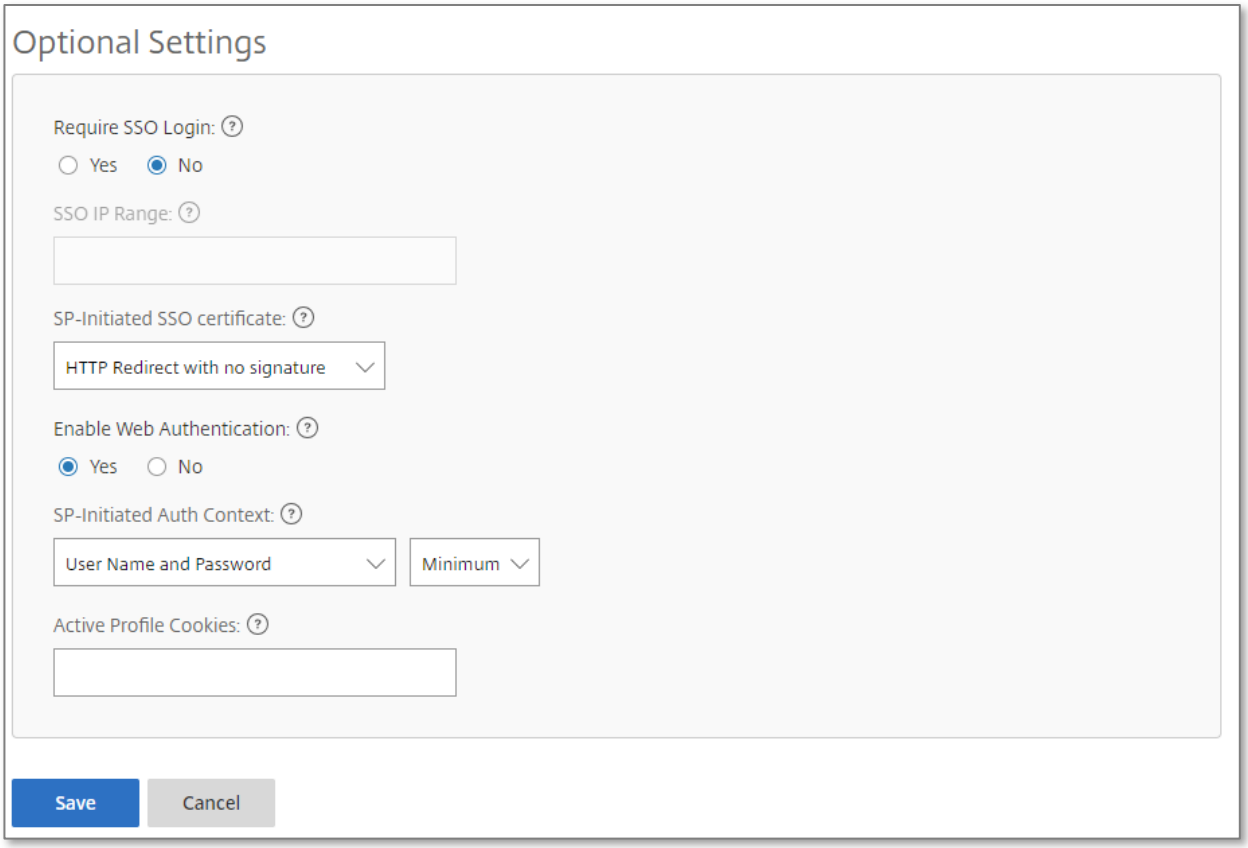
○ Enable SAML: Select Yes

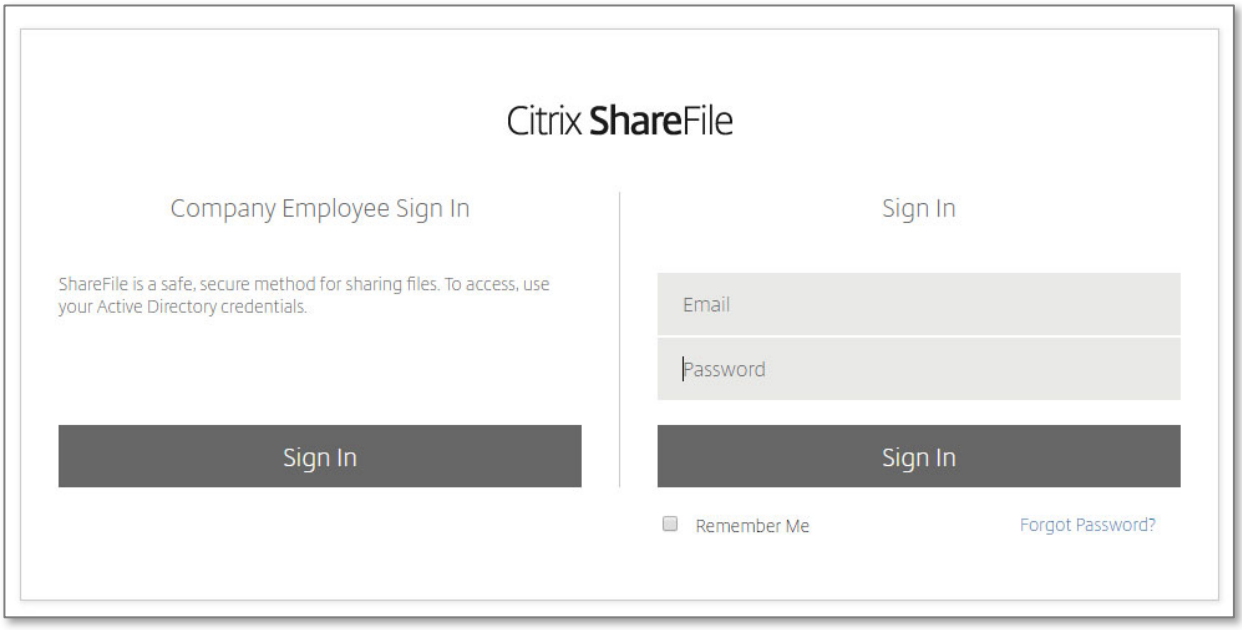
○ ShareFile Issuer / Entity ID: Copy to clipboard the SP entityID from PingOne and paste

○ Your Issuer / Entity ID: Copy to clipboard the Issuer from PingOne / PingIdentity and paste

○ X.509 Certificate: Click Change, then copy and paste the certificate from the Singing Certificate file from the step above</td></tr>
</table>

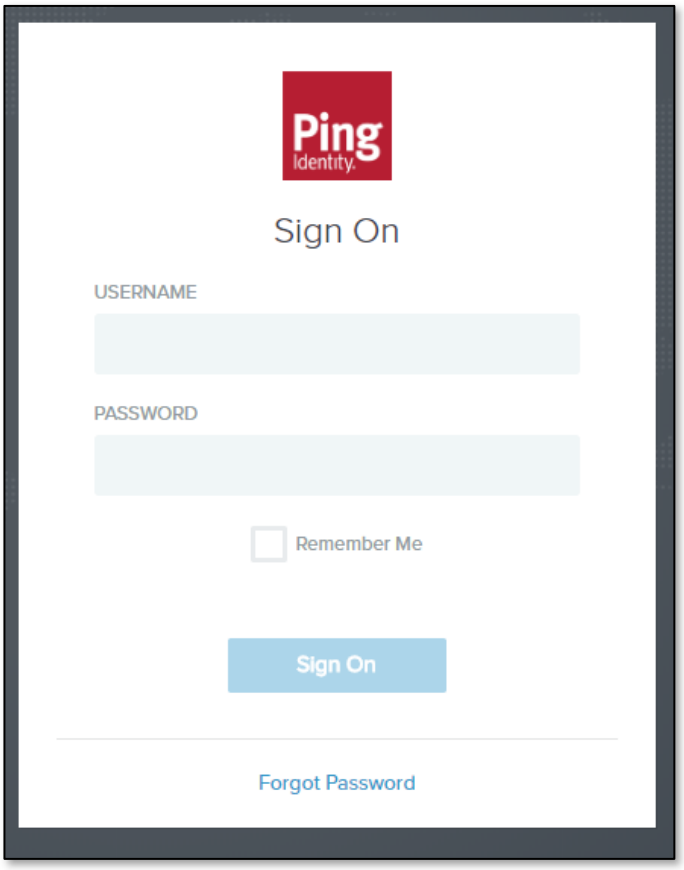
	○ **Login URL**: Add login URL in the form of **https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid>** ****Replace <idpid> with the IPID that can be obtained from **Initiate Single Sign-On (SSO) URL**.* **Example Login URL**: https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=765ac29c-7c4b-4484-afc9-hedf218c6a2e) ○ **Logout URL**: Leave blank (When users log out of ShareFile, they will be redirected to ShareFile login page https://subdomain.sharefile.com.) 
18.	**<u>Optional Settings</u>** ○ **Require SSO Login**: *Optional* After single-sign-on is successfully validated, checking **Yes** for this option <u>will require</u> all non-admin Employees to log in using PingOne / PingIdentity. Admins will have the choice to login using PingOne / PingIdentity (on the left) or their email address as the username and a native ShareFile password (on the right). ○ **SSO IP Range**: *Optional* (Limit requiring non-admin Employees to login from a specific IP range.

	Employees outside of this specified range will not be required to use OneLogin to login.) ○ **SP-initiated SSO Certificate**: Select **HTTP Redirect with no signature** ○ **Enable Web Authentication**: **Yes** (Choose **No** when you do not want to allow single sign on logins via a web browser. This means Windows authentication will need to be available. **No** is not recommended). ○ **SP-initiated Auth Context**: Select **User Name and Password**. ○ **Active Profile Cookies**: Leave blank ○ Click **Save** 
19.	Test successful authentication by going to your ShareFile URL: https://subdomain.sharefile.com ***Testing single-sign-on logins in private/incognito browser mode is best.* Click **Sign in** under **Company Employee Sign In**

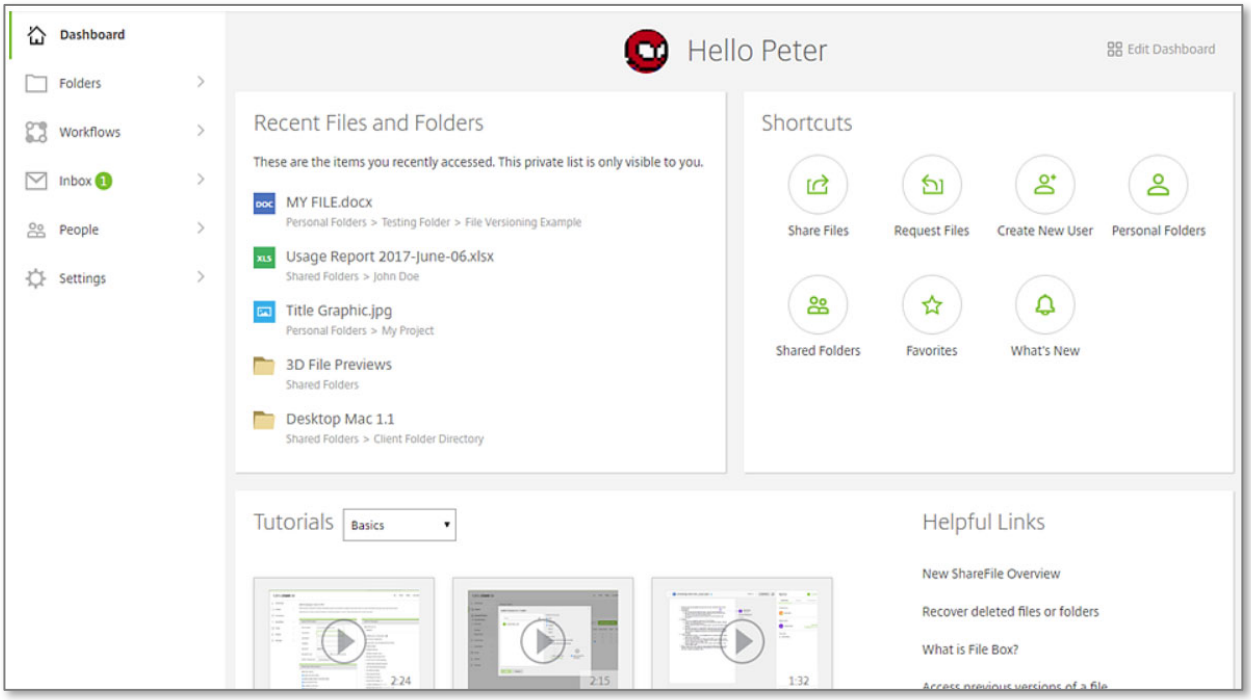


****Make sure the user logging in with single sign-on has an Active Directory or Identity Provider email address that matches their email address in their ShareFile account.**

Sign in will redirect you PingIdentity for sign in:

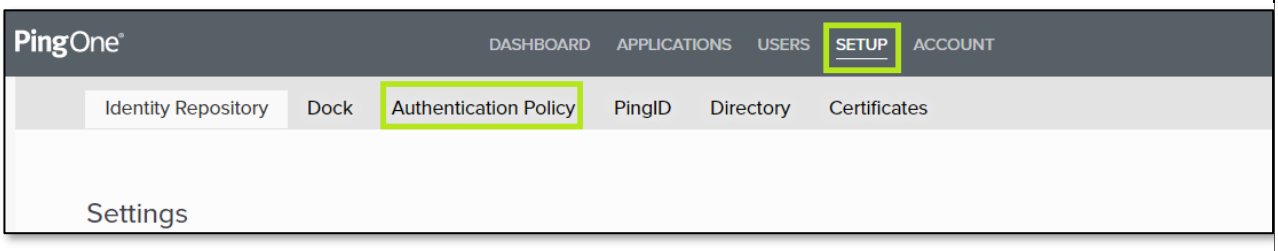


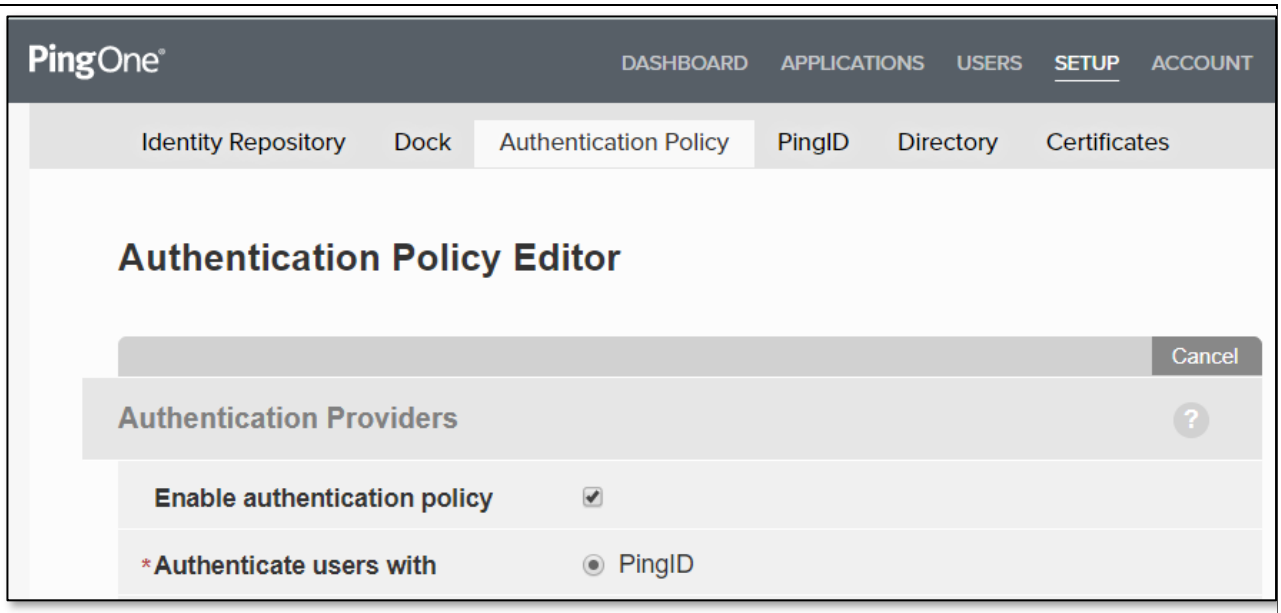
Successful logins will authenticate users into their ShareFile account **Dashboard**.

	
20.	Done!

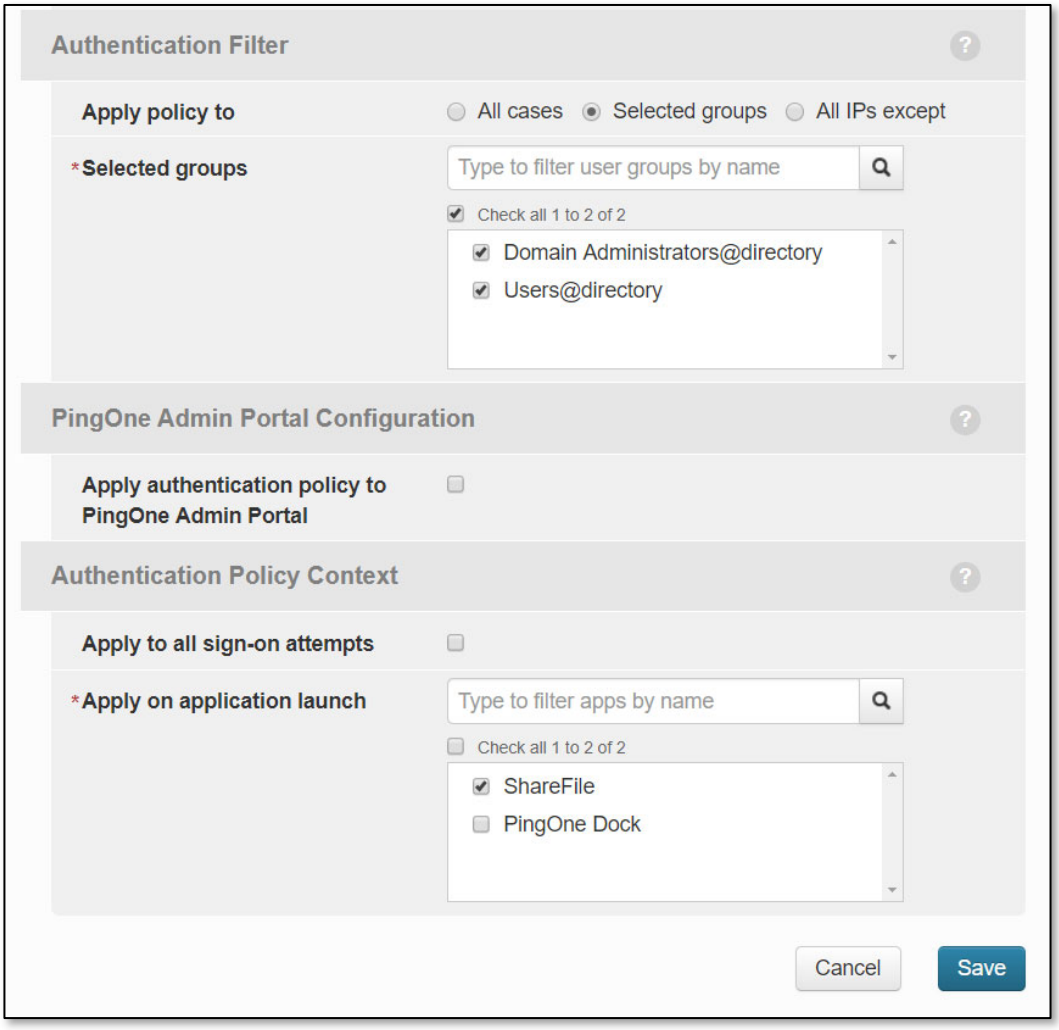
PingID for MFA

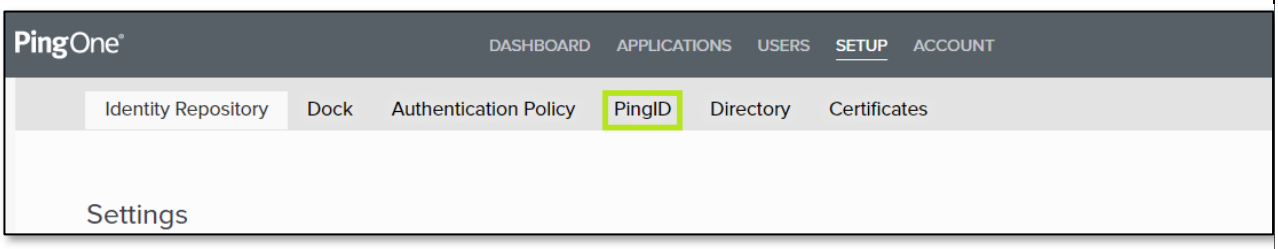
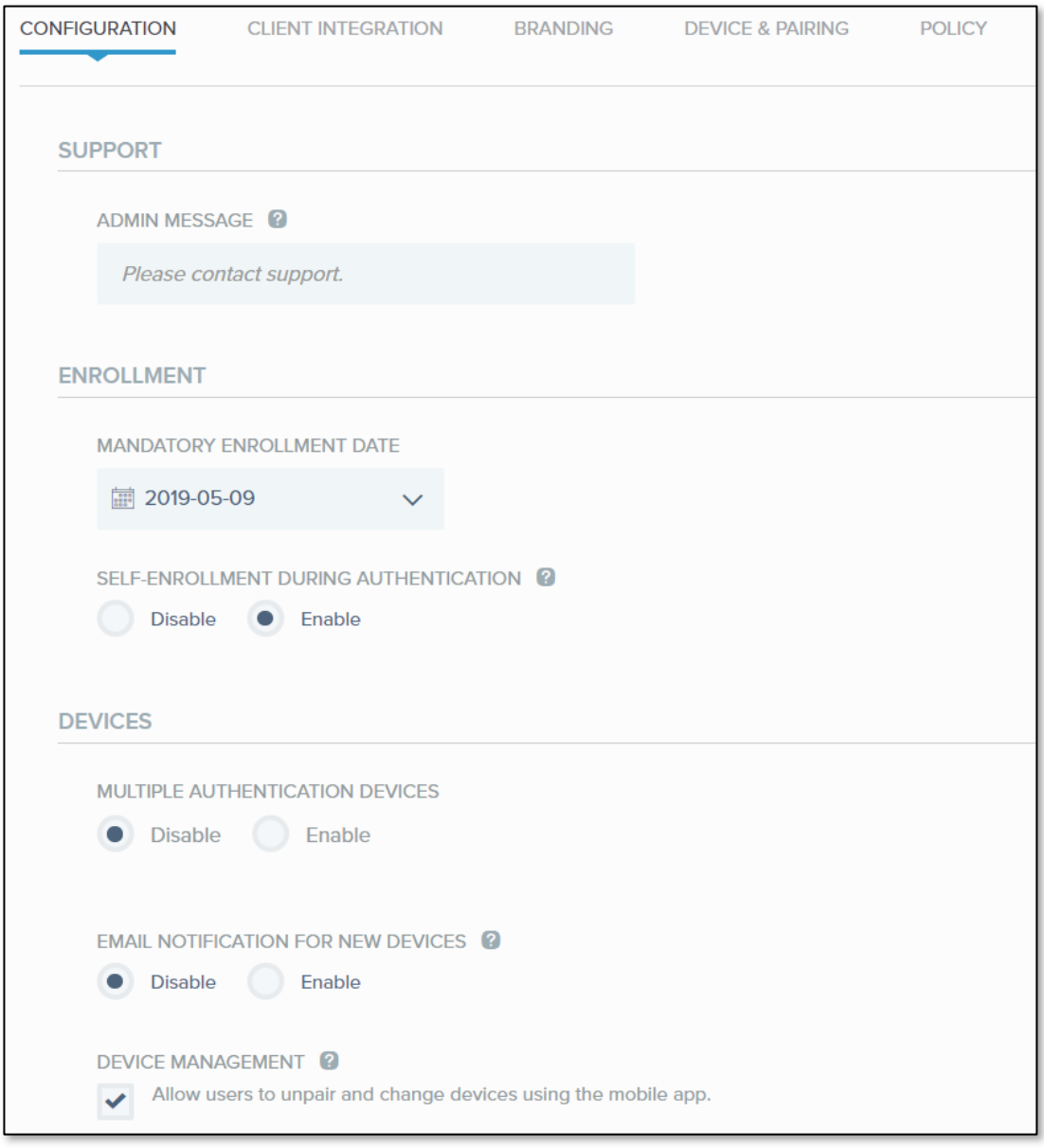
Configure PingOne with Ping ID for SAML and multi/two-factor authentication:

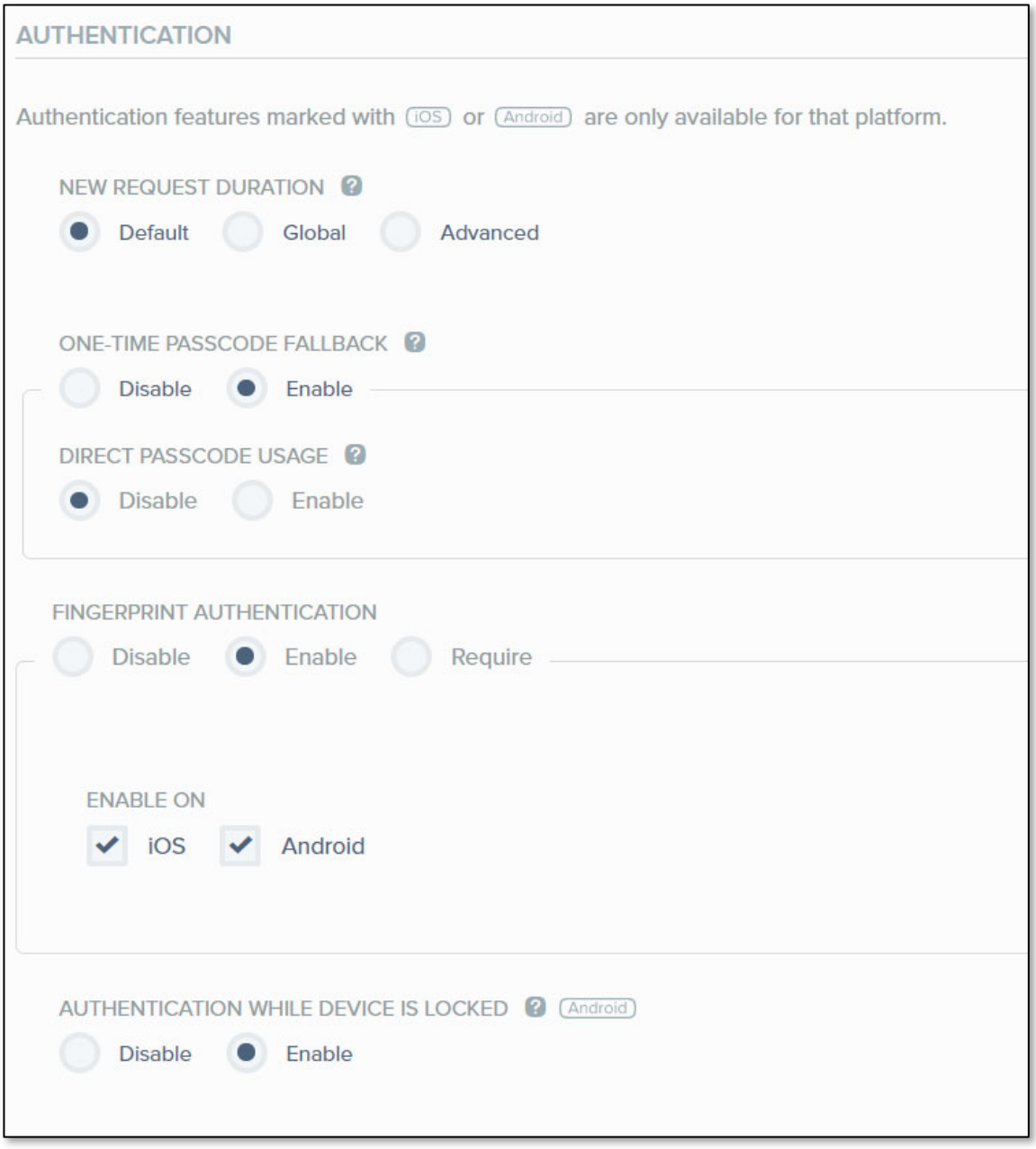
Steps	Description
1.	Log in to the PingOne Administrator site. For example, login to https://admin.pingone.com/
2.	Click on **Setup** in top navigation menu > then **Authentication Policy**. 
3.	For new configurations, select Enable Authentication Policy

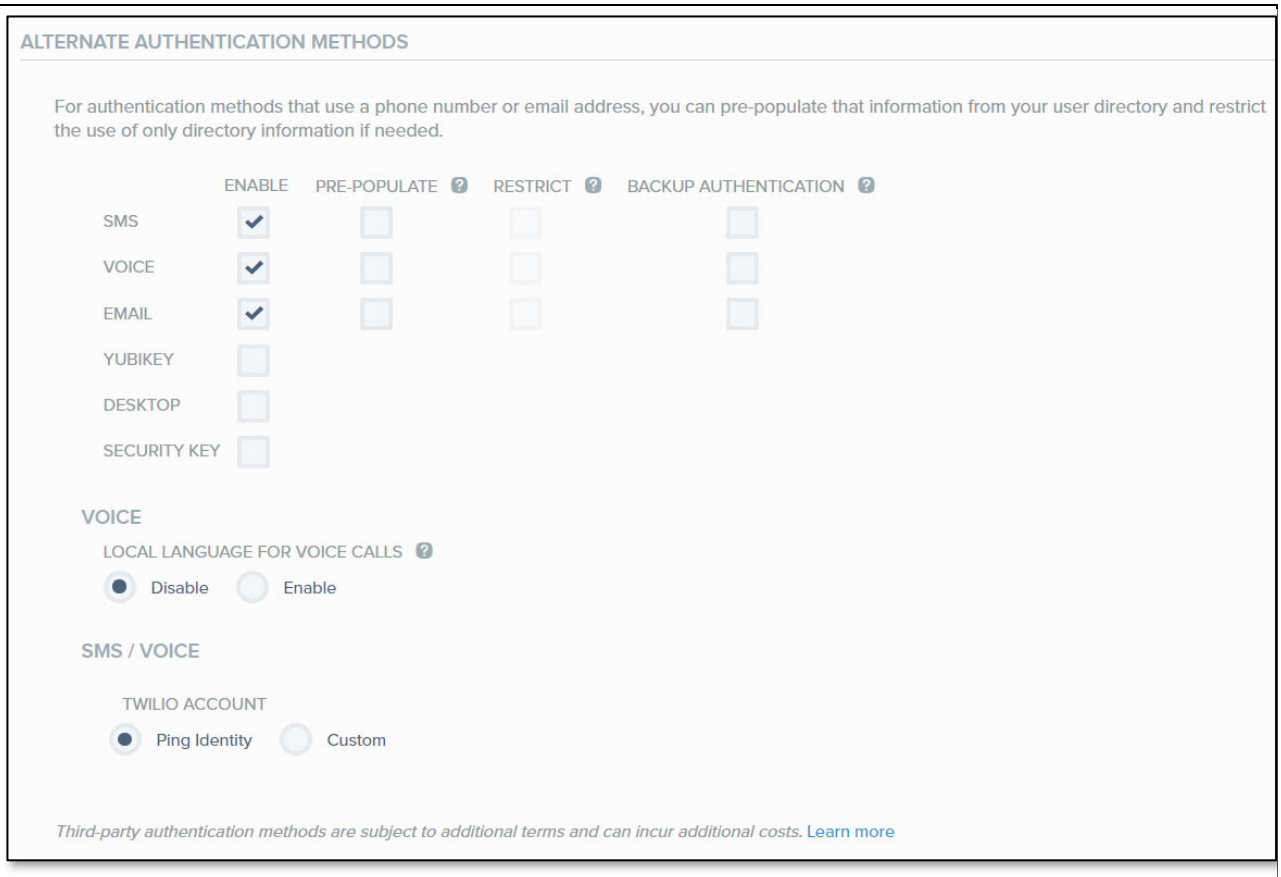


4. Choose which **selected groups** and **apps** this policy applies to:

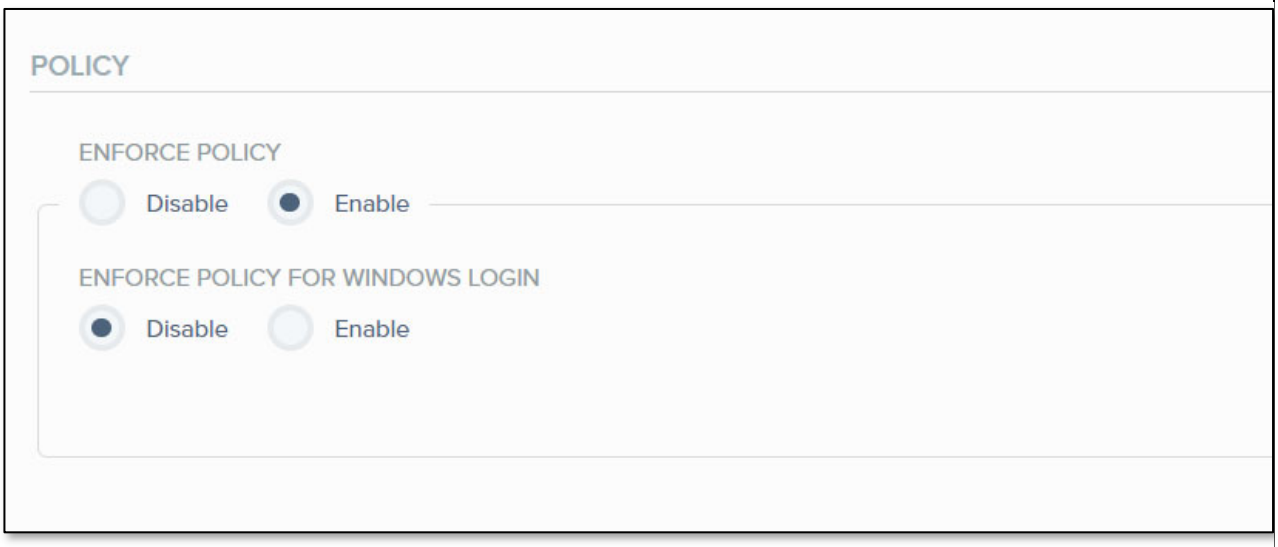


5.	Select **PingID** in top navigation > choose **Edit**. 
6.	Under **Configuration**, choose appropriate settings for **Support Message**, **Mandatory Enrollment Start Date**, **Self-Enrollment**, and **Devices** policies. 

7.	Choose appropriate settings for **Authentication** policies. 
8.	Choose appropriate **Alternate Authentication Methods**.



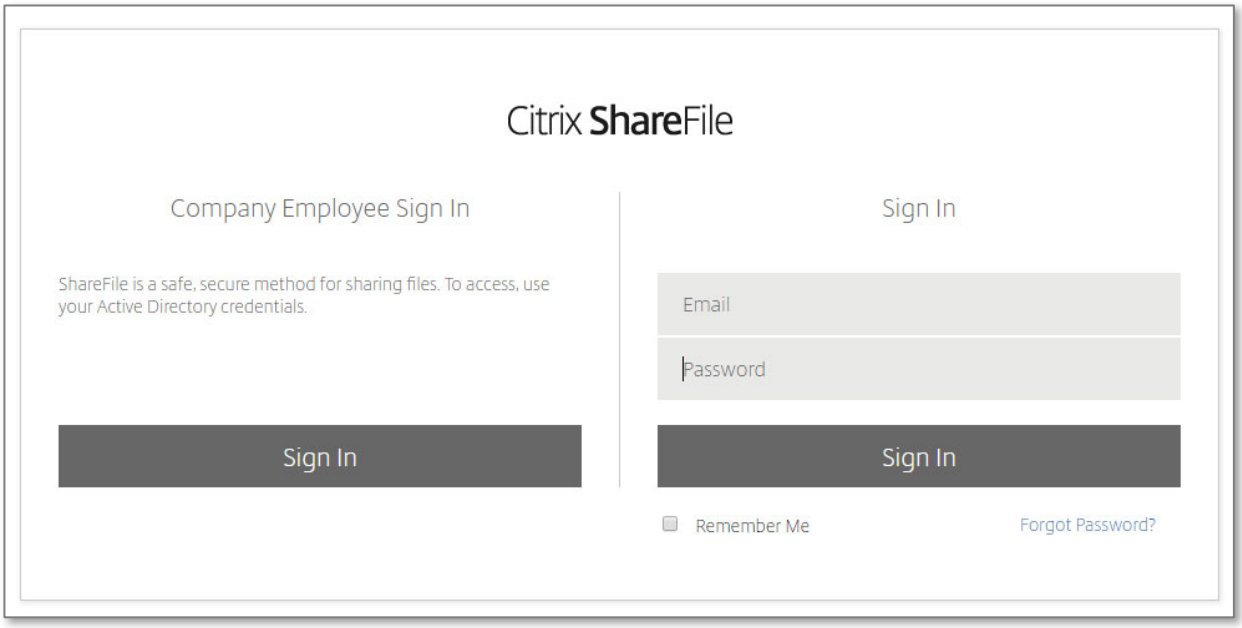
9. **Enable** the Policy. Click **Save** when selecting all settings is complete.



10. Test successful authentication by going to your ShareFile URL: https://subdomain.sharefile.com

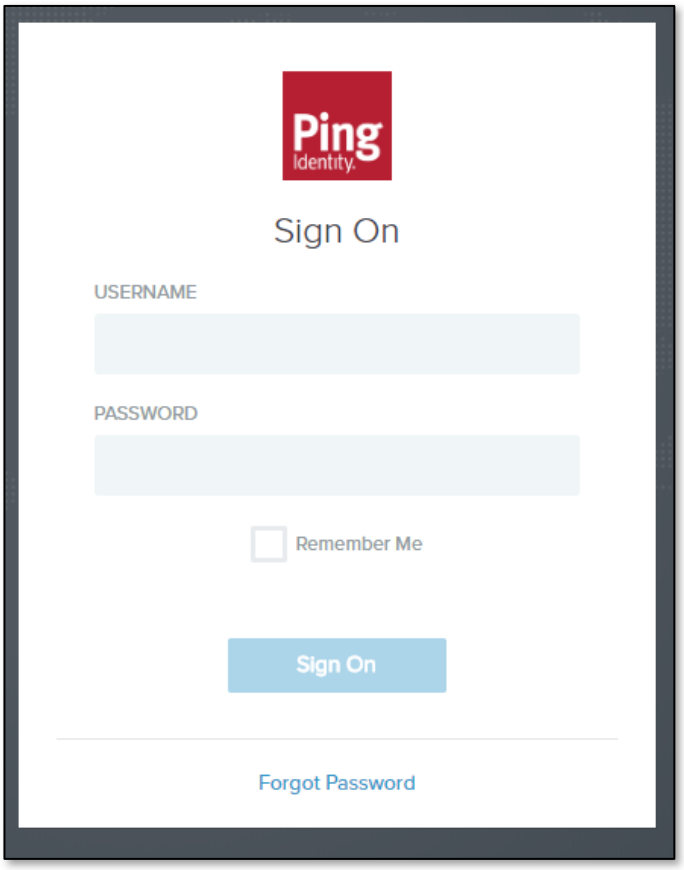
***Testing single-sign-on logins in private/incognito browser mode is best.*

Click **Sign in** under **Company Employee Sign In**

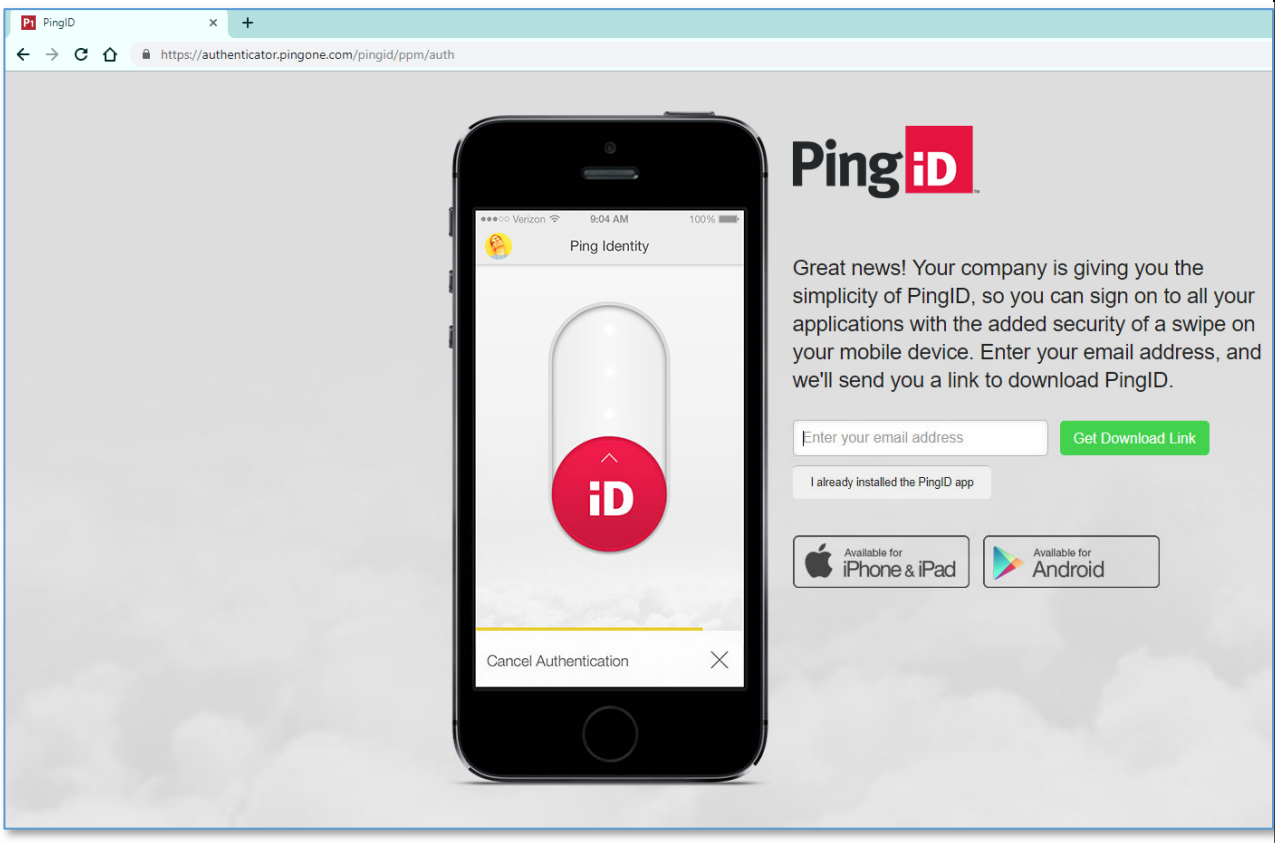


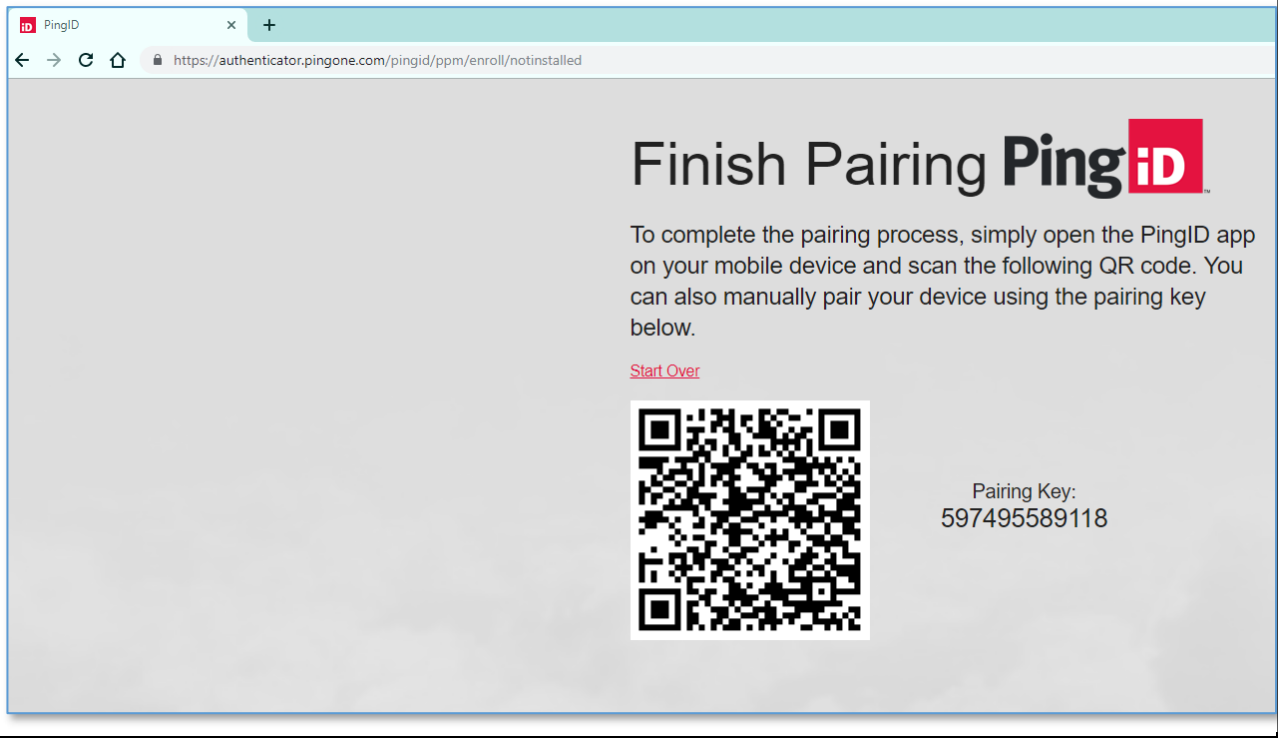
****Make sure the user logging in with single sign-on has an Active Directory or Identity Provider email address that matches their email address in their ShareFile account.**

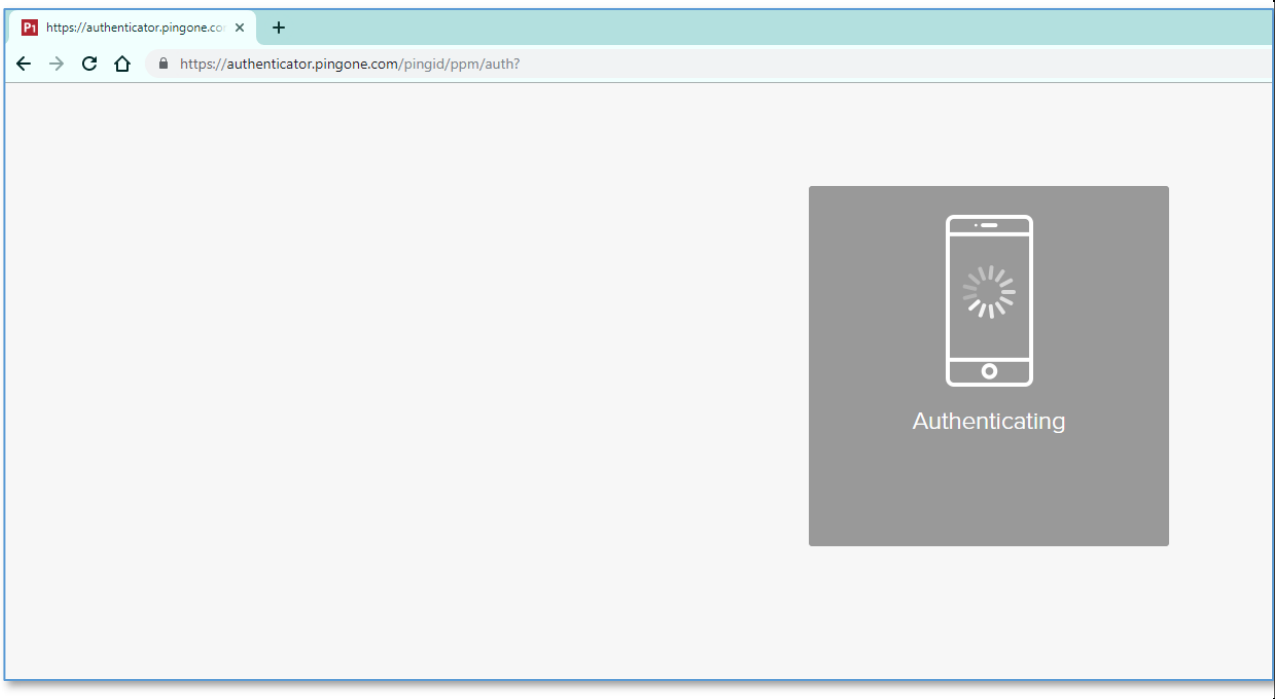
Sign in will redirect you PingIdentity for sign in:

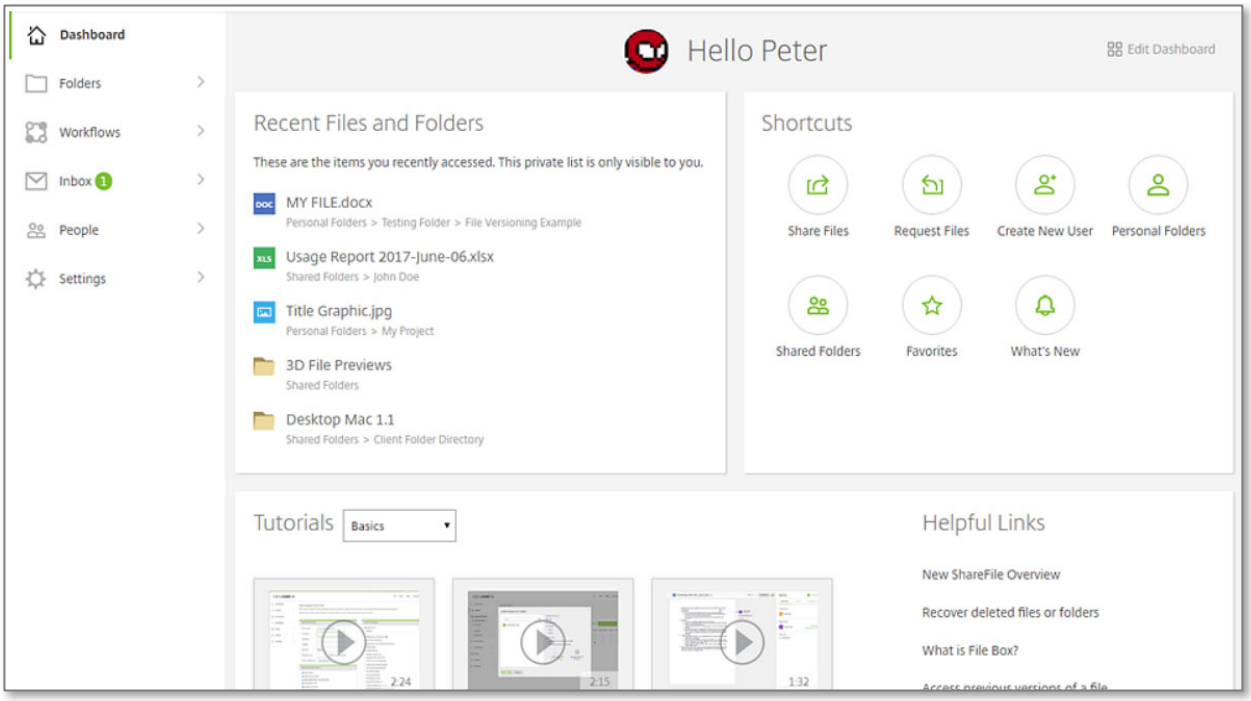


11.	First time logins to **PingID will get a download link** and **QR code** to install the authenticator app on an Android or iOS device





12.	User will complete setup on their mobile device. Successful mobile app authentication will begin **authenticating**… 
13.	User needs to “slide up” on the mobile authenticator app for **Citrix / ShareFile** to complete authentication. 

14.	Successful logins will authenticate users into their ShareFile account **Dashboard**. 
15.	Done!