

Content Collaboration: Single Sign-On Configuration

PingONE / PingID for MFA

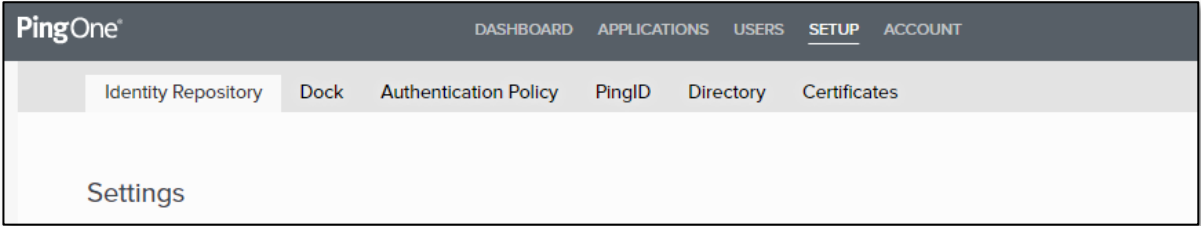
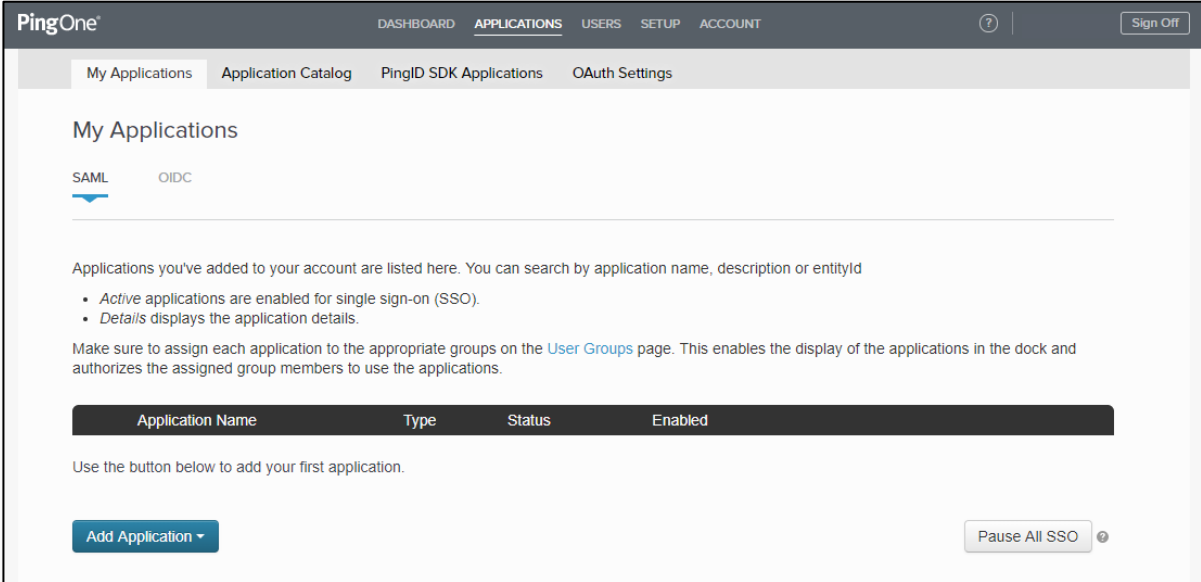
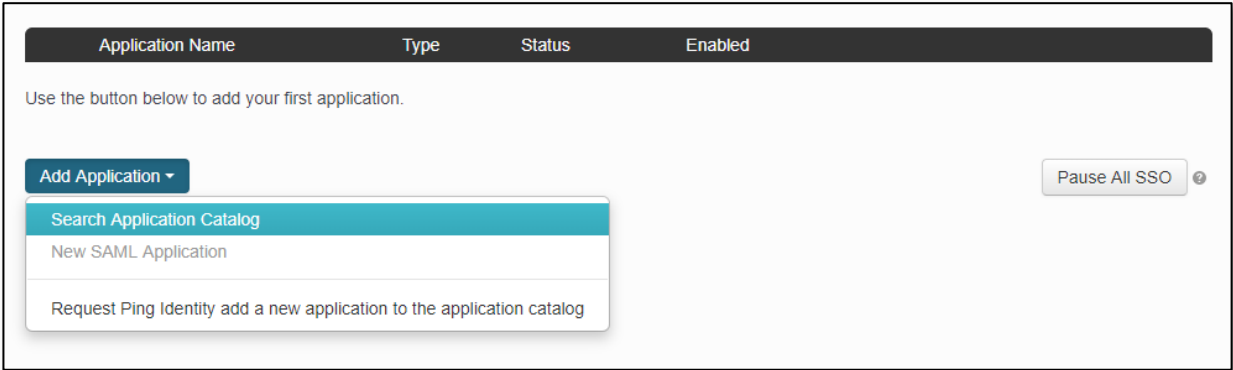


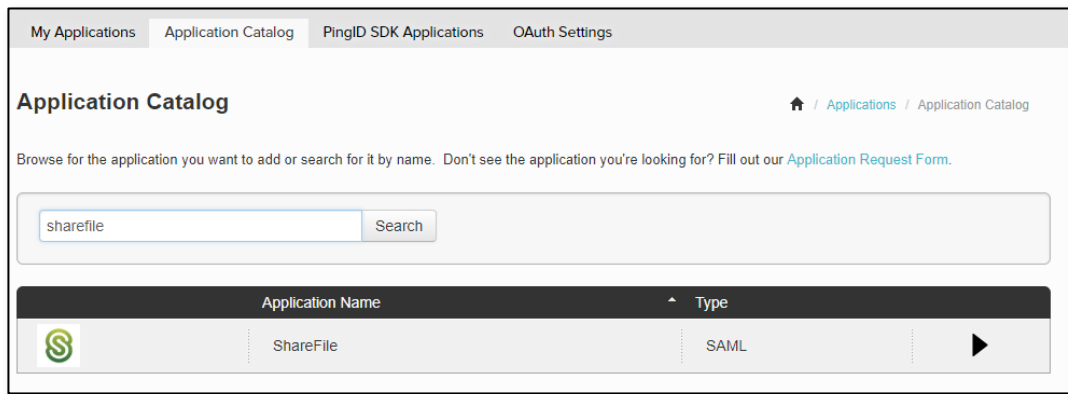
Last Revised: May 2019

LEGAL NOTICE

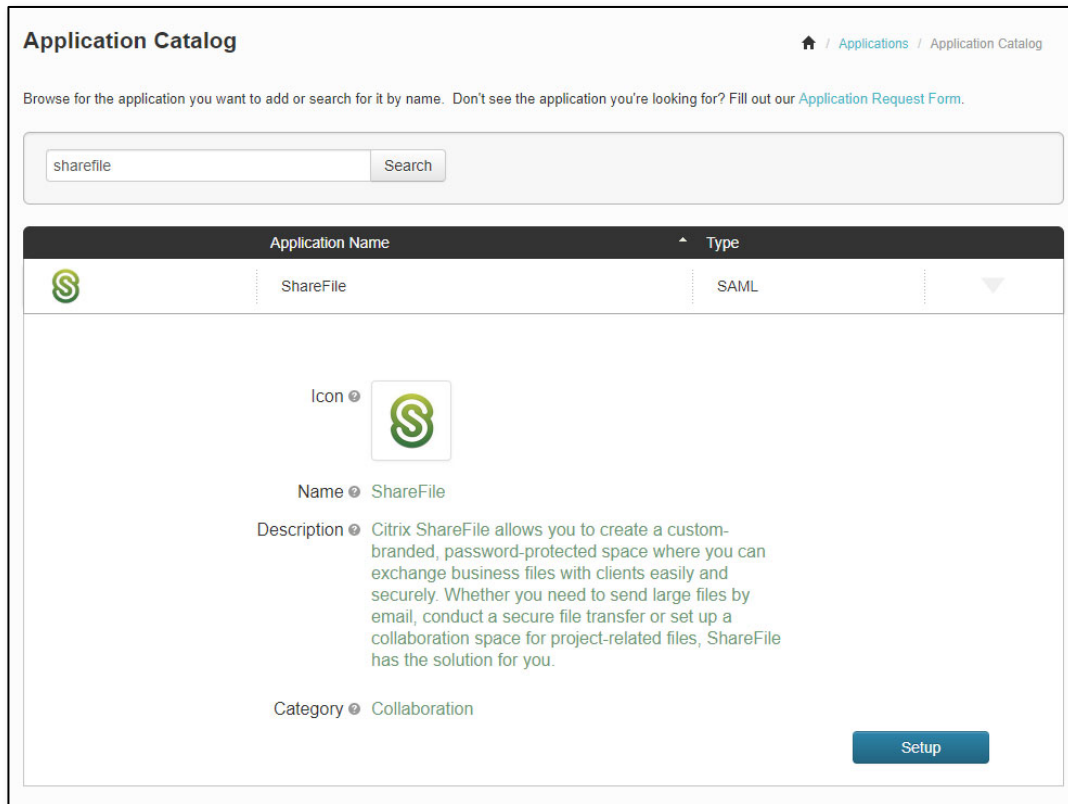
This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc. This document and the software may be used and copied only as agreed upon by the Beta or Technical Preview Agreement.

Copyright © 2018 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Receiver, and StoreFront are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Steps	Description
1.	<p>Log in to the PingOne Administrator site.</p> <p>For example, login to https://admin.pingone.com/</p>
2.	<p>Be sure the account is connected to an Identity Repository. Check Setup for Repository type.</p>  <p>The screenshot shows the PingOne administrator interface. At the top, there are navigation tabs: DASHBOARD, APPLICATIONS, USERS, SETUP, and ACCOUNT. Below these, a secondary navigation bar contains: Identity Repository (selected), Dock, Authentication Policy, PingID, Directory, and Certificates. The main content area shows the word 'Settings'.</p>
3.	<p>Click on Applications.</p>  <p>The screenshot shows the PingOne administrator interface with the 'APPLICATIONS' tab selected. The navigation bar includes: My Applications (selected), Application Catalog, PingID SDK Applications, and OAuth Settings. The main content area is titled 'My Applications' and has sub-tabs for SAML and OIDC. Below the sub-tabs, there is a paragraph of text: 'Applications you've added to your account are listed here. You can search by application name, description or entityId'. This is followed by a bulleted list: <ul style="list-style-type: none"> • Active applications are enabled for single sign-on (SSO). • Details displays the application details. Below the list, another paragraph states: 'Make sure to assign each application to the appropriate groups on the User Groups page. This enables the display of the applications in the dock and authorizes the assigned group members to use the applications.' At the bottom of the main content area, there is a table header with columns: Application Name, Type, Status, and Enabled. Below the header, there is a text prompt: 'Use the button below to add your first application.' At the bottom left, there is a blue 'Add Application' button with a dropdown arrow. At the bottom right, there is a grey 'Pause All SSO' button with a gear icon.</p>
4.	<p>Click on Add Application > Search Application Catalog.</p>  <p>The screenshot shows the same 'My Applications' page as in step 3. The 'Add Application' button is now open, showing a dropdown menu. The first option, 'Search Application Catalog', is highlighted in teal. Other options in the menu include 'New SAML Application' and 'Request Ping Identity add a new application to the application catalog'. The rest of the page content remains the same as in step 3.</p>
5.	<p>Search for “sharefile” in the Application Catalog and select play button.</p>



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.

```

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? X
pingone-signing.crt
1 -----BEGIN CERTIFICATE-----
2 MIIDWjCCAkKgAwIBAgIGAWqdFziPMA0GCSqGSIb3DQEBCwUAMG4xCzAJBgNVBAYTA1VTMQswCQYD
3 VQQIEwJDTIzEPMA0GA1UEBxMGRGVudmVvMRYwFAYDVQQKEw1QaW5nIE1kZW50aXR5MSkwJwYDVQDD
4 EyA5YjI3ZTVhMGQ3MWE0MGUzYTMxY2FhYTIxNGE0ZWVhMDAeFw0xOTA1MDkxNDU1MDVaFw0yMjA1
5 MDgxNDU1MDVaMG4xCzAJBgNVBAYTA1VTMQswCQYDVQDEwJDTIzEPMA0GA1UEBxMGRGVudmVvMRYw
6 FAYDVQQKEw1QaW5nIE1kZW50aXR5MSkwJwYDVQDEwJDTIzEPMA0GA1UEBxMGRGVudmVvMRYw
7 NGE0ZWVhMDAeFw0xOTA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVa
8 a1UzZTVhMGQ3MWE0MGUzYTMxY2FhYTIxNGE0ZWVhMDAeFw0xOTA1MDkxNDU1MDVaFw0yMjA1MDkx
9 NDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1
10 MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0y
11 MjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVa
12 Fw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1
13 MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkx
14 NDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1
15 MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0y
16 MjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVa
17 Fw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1MDVaFw0yMjA1MDkxNDU1
18 -----END CERTIFICATE-----
length: 1,221 lines: 1 Ln: 5 Col: 77 Sel: 0 | 0 Unix (LF) UTF-8 INS

```

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

Admin -> Configure Single Sign-On

	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.

NEXT: Connection Configuration

Cancel **Continue to Next Step**

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

2. Connection Configuration

Assign the attribute values for single sign-on (SSO) to the application.

Upload Metadata [Or use URL](#)

ACS URL *
Replace the parameter(s) "\${mydomain}" above with your configuration information.

Entity ID *
Replace the parameter(s) "\${mydomain}" above with your configuration information.

Target Resource

Single Logout Endpoint

Single Logout Response Endpoint

Primary Verification Certificate No file chosen

Secondary Verification Certificate No file chosen

Force Re-authentication

Encrypt Assertion

Signing Sign Assertion Sign Response

Signing Algorithm

PingOne dock URL

Default PingOne dock URL Use Custom URL

NEXT: Attribute Mapping

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

3. Attribute Mapping

Map your identity bridge attributes to the attributes required by the application.

Application Attribute	Description	Identity Bridge Attribute or Literal Value
1 SAML_SUBJECT *	\${map to your email}	<input type="text" value="Email"/> <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>

* Indicates a required attribute.


NEXT: PingOne App Customization - ShareFile

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

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

13. Customize **ShareFile App** in for PingOne dock.

4. PingOne App Customization - ShareFile

Icon 

Select image

Name

Description

Category

NEXT: Group Access

Cancel Back Continue to Next Step

14. **Select** user groups that should have access to single-sign-on into the ShareFile application.

5. Group Access

Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.

Search


Group Name	
Users@directory	Remove
Domain Administrators@directory	Add

NEXT: Review Setup

Continue to Next Step

15. Review setup settings for ShareFile Application.

Test your connection to the application

Icon 

Name **ShareFile**

Description Citrix ShareFile allows you to create a custom-branded, password-protected space where you can exchange business files with clients easily and securely. Whether you need to send large files by email, conduct a secure file transfer or set up a collaboration space for project-related files, ShareFile has the solution for you.

Category **Collaboration**

Connection ID 2a1723ec-0b1d-458c-aa9c-67f57bbf7cba

You may need to configure these connection parameters as well.

saasid 953c1d25-1f5-4657-b5c6-6cd2422efe91

Issuer <https://pingone.com/idp/cd-2070333814.citrix>

Signing Assertion

Signing Algorithm RSA_SHA256

Encrypt Assertion false

ACS URL <https://subdomain.sharefile.com/saml/acs>

SP entityId subdomain.sharefile.com

Initiate Single Sign-On (SSO) URL <https://sso.connect.pingidentity.com/sso/sp/initss?saasid=953c1d25-1f5-4657-b5c6-6cd2422efe91&idpid=765ac29c-7c4b-4484-afc9-0dae218c6a2e>

Single Sign-On (SSO) Relay State <https://pingone.com/1.0/953c1d25-1f5-4657-b5c6-6cd2422efe91>

Single Logout Endpoint

Single Logout Response Endpoint

Force Re-authentication false

Signing Certificate [Download](#)

SAML Metadata [Download](#)

Application Attribute	Description	Identity Bridge Attribute or Literal Value
1	SAML_SUBJECT *	\$(map to your email) SAML_SUBJECT

16. 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**.

17. Configure **Single sign on / SAML 2.0 Configuration** with the below:

Basic Settings

- **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

- **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>.)

The screenshot shows two panels. The left panel lists various SSO settings, and the right panel shows the 'Basic Settings' configuration. Red arrows indicate the following mappings:

- Issue URL: `https://pingone.com/idp/cd-2070333814.citrix` maps to 'Your IDP Issuer / Entity ID'.
- ACS URL: `https://subdomain.sharefile.com/saml/acs` maps to 'ShareFile Issuer / Entity ID'.
- SP entityId: `subdomain.sharefile.com` maps to 'Your IDP Issuer / Entity ID'.
- Initiate Single Sign-On (SSO) URL: `https://sso.connect.pingidentity.com/sso/sp/initss0?saasid=953c1d25-1ff5-4657-b5c6-6cd2422efe91&idpid=765ac29c-7c4b-4484-afc9-0dae218c6a2e` maps to 'Login URL'.
- Single Sign-On (SSO) Relay State: `https://pingone.com/1.0/953c1d25-1ff5-4657-b5c6-6cd2422efe91` maps to 'Logout URL'.

18. **Optional Settings**

- **Require SSO Login: *Optional***
After single-sign-on is successfully validated, checking **Yes** for this option will require 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**

Optional Settings

Require SSO Login: (?)
 Yes No

SSO IP Range: (?)

SP-Initiated SSO certificate: (?)
HTTP Redirect with no signature ▾

Enable Web Authentication: (?)
 Yes No

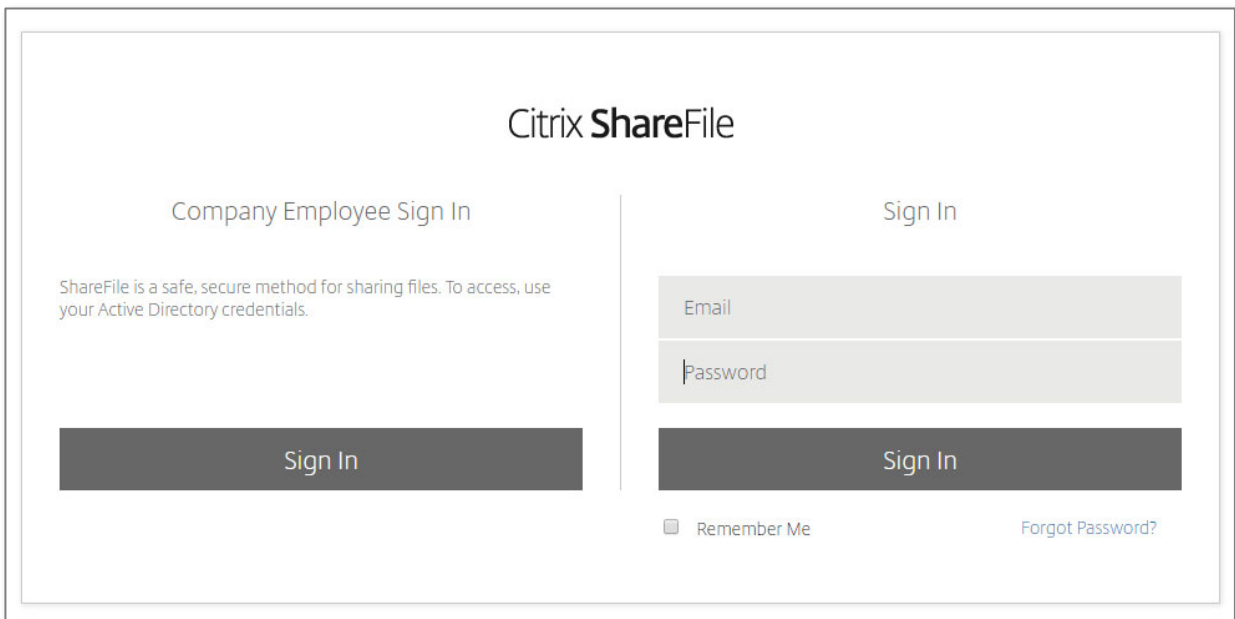
SP-Initiated Auth Context: (?)
User Name and Password ▾ Minimum ▾

Active Profile Cookies: (?)

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**



Citrix ShareFile

Company Employee Sign In

ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.

Sign In

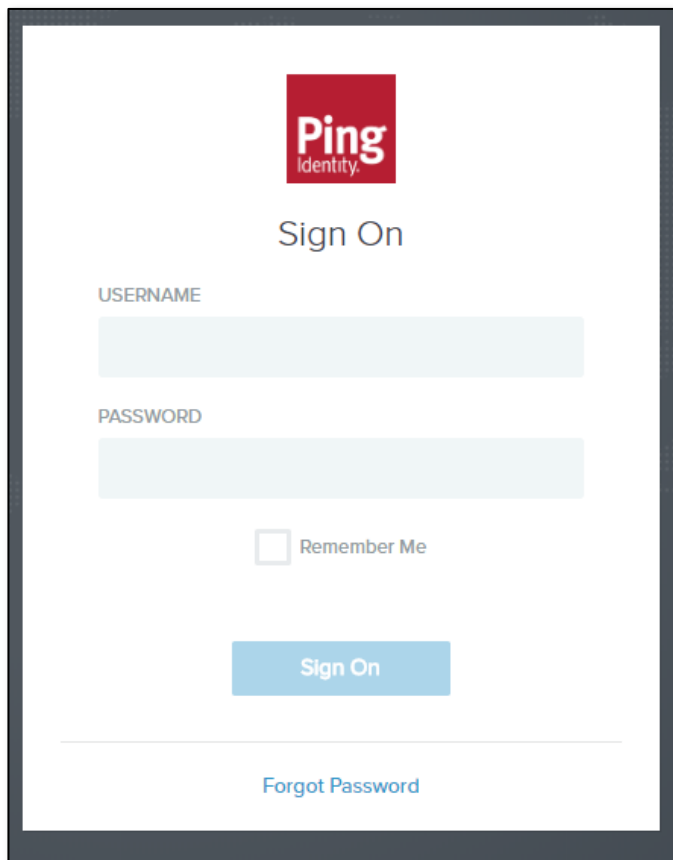
Sign In

Remember Me [Forgot Password?](#)

The image shows the Citrix ShareFile login interface. It is divided into two main sections. The left section is titled 'Company Employee Sign In' and contains a brief description of ShareFile as a secure file-sharing method, followed by a 'Sign In' button. The right section is titled 'Sign In' and features input fields for 'Email' and 'Password', a 'Sign In' button, a 'Remember Me' checkbox, and a 'Forgot Password?' link.

****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:



Ping Identity

Sign On

USERNAME

PASSWORD

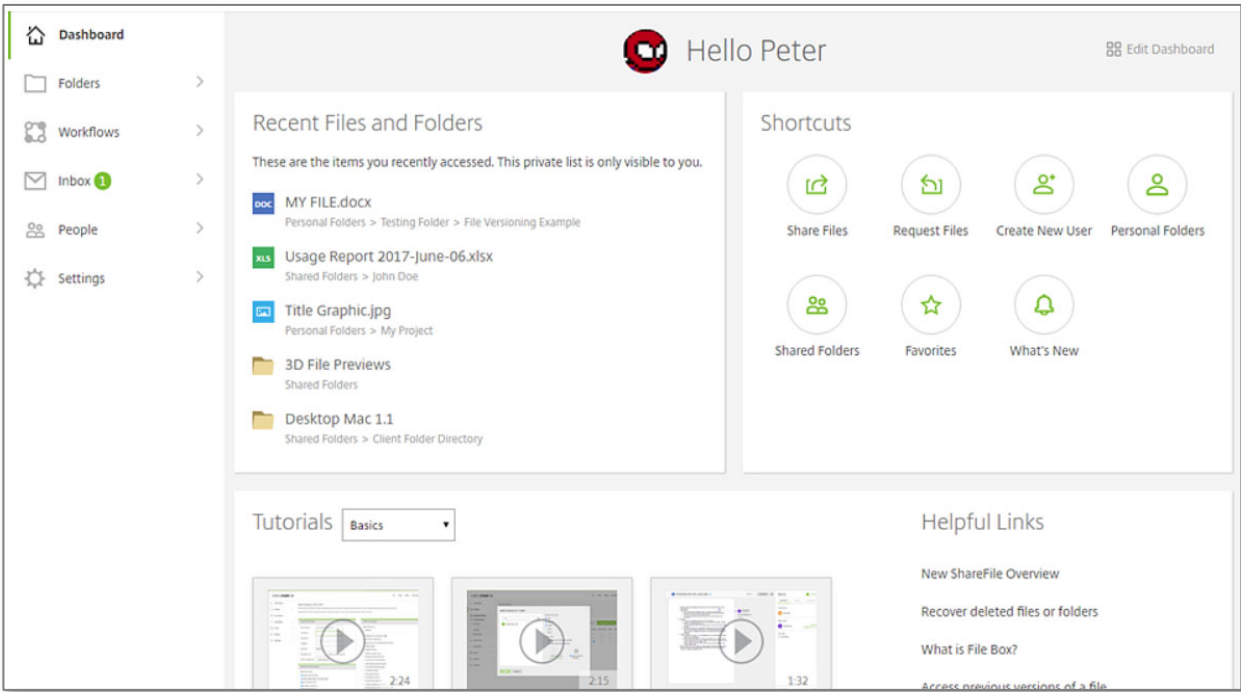
Remember Me

Sign On

[Forgot Password](#)

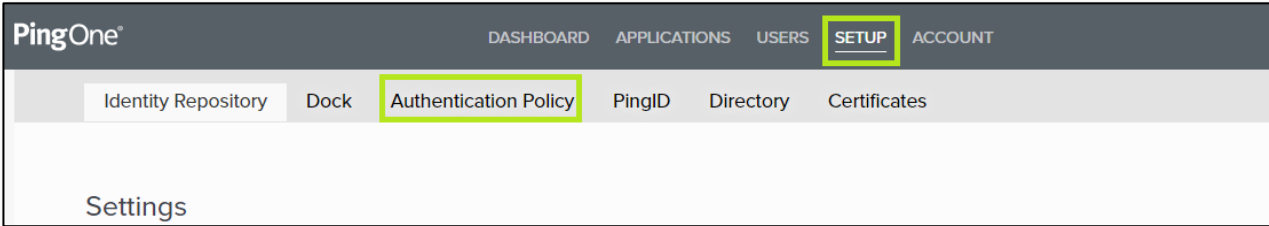
The image shows the Ping Identity 'Sign On' page. It features the Ping Identity logo at the top, followed by the title 'Sign On'. Below the title are two input fields labeled 'USERNAME' and 'PASSWORD'. A 'Remember Me' checkbox is positioned below the password field. A blue 'Sign On' button is centered below the input fields. At the bottom of the page, there is a link for 'Forgot Password'.

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

Identity Repository

Dock

Authentication Policy

PingID

Directory

Certificates

Authentication Policy Editor

Cancel

Authentication Providers

?

Enable authentication policy



* Authenticate users with



PingID

4.

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

Authentication Filter

?

Apply policy to



All cases



Selected groups



All IPs except

* Selected groups

Type to filter user groups by name



Check all 1 to 2 of 2



Domain Administrators@directory



Users@directory

PingOne Admin Portal Configuration

?

Apply authentication policy to
PingOne Admin Portal

Authentication Policy Context

?

Apply to all sign-on attempts



* Apply on application launch

Type to filter apps by name



Check all 1 to 2 of 2



ShareFile

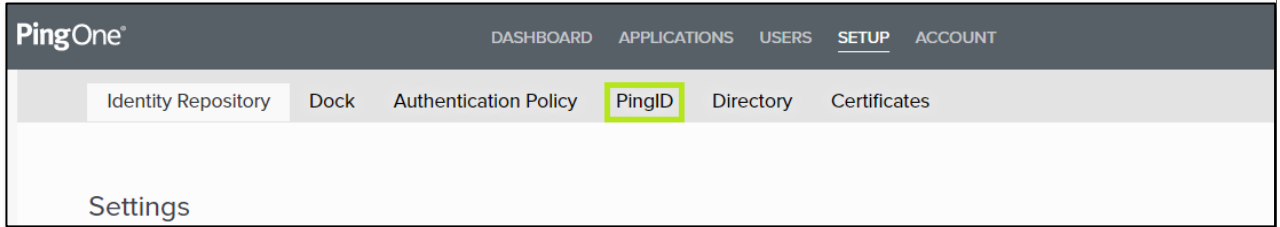


PingOne Dock

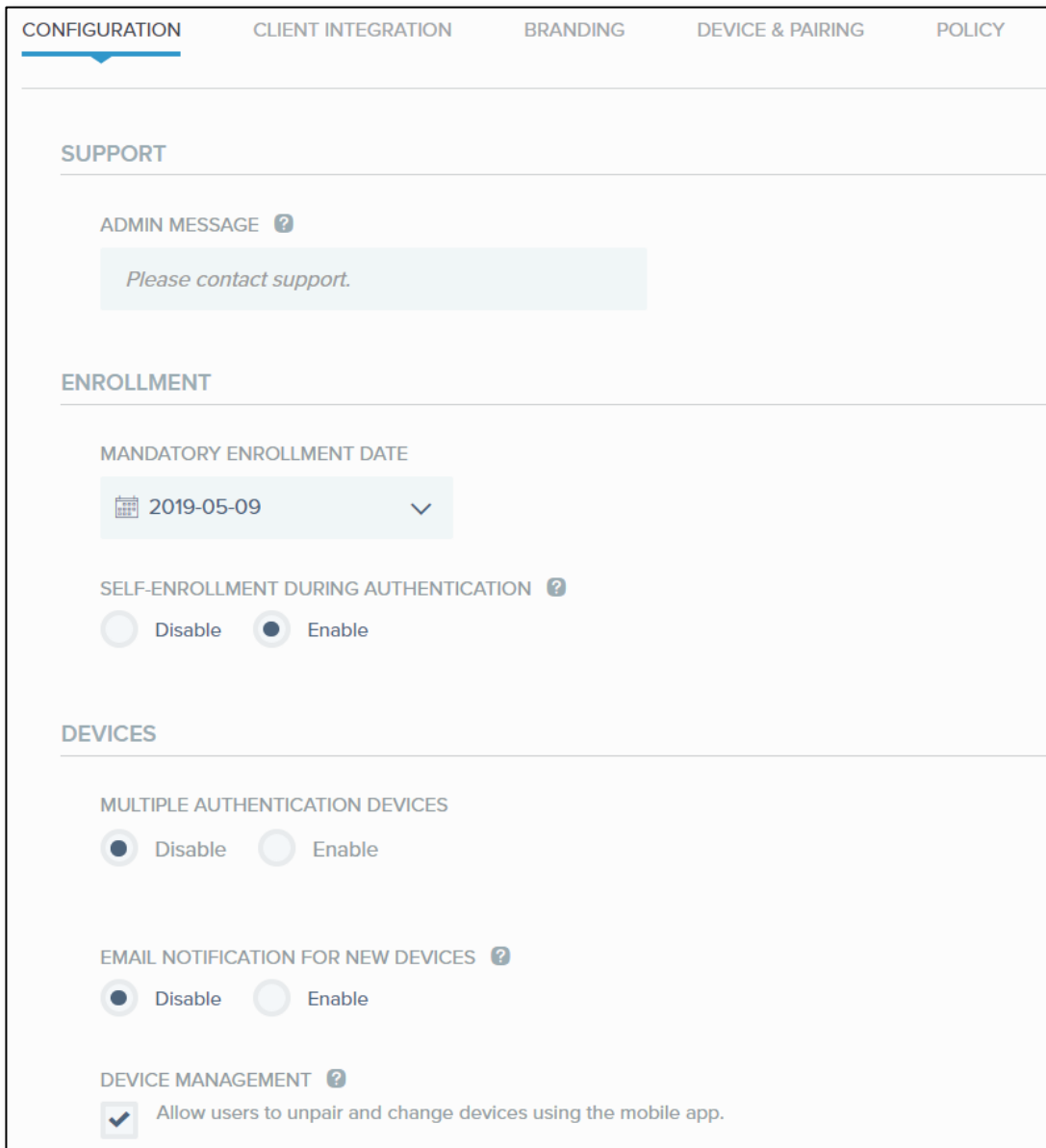
Cancel

Save

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.

AUTHENTICATION

Authentication features marked with iOS or Android are only available for that platform.

NEW REQUEST DURATION ?

Default Global Advanced

ONE-TIME PASSCODE FALLBACK ?

Disable Enable

DIRECT PASSCODE USAGE ?

Disable Enable

FINGERPRINT AUTHENTICATION

Disable Enable Require

ENABLE ON

iOS Android

AUTHENTICATION WHILE DEVICE IS LOCKED ? Android

Disable Enable

8. Choose appropriate **Alternate Authentication Methods**.

ALTERNATE AUTHENTICATION METHODS

For authentication methods that use a phone number or email address, you can pre-populate that information from your user directory and restrict the use of only directory information if needed.

	ENABLE	PRE-POPULATE ?	RESTRICT ?	BACKUP AUTHENTICATION ?
SMS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VOICE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EMAIL	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
YUBIKEY	<input type="checkbox"/>			
DESKTOP	<input type="checkbox"/>			
SECURITY KEY	<input type="checkbox"/>			

VOICE

LOCAL LANGUAGE FOR VOICE CALLS ?

Disable Enable

SMS / VOICE

TWILIO ACCOUNT

Ping Identity Custom

Third-party authentication methods are subject to additional terms and can incur additional costs. [Learn more](#)

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

POLICY

ENFORCE POLICY

Disable Enable

ENFORCE POLICY FOR WINDOWS LOGIN

Disable Enable

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**

Citrix **ShareFile**

Company Employee Sign In

ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.

Sign In

Sign In

Email


Password

Sign In

Remember Me [Forgot Password?](#)

****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:



Sign On

USERNAME

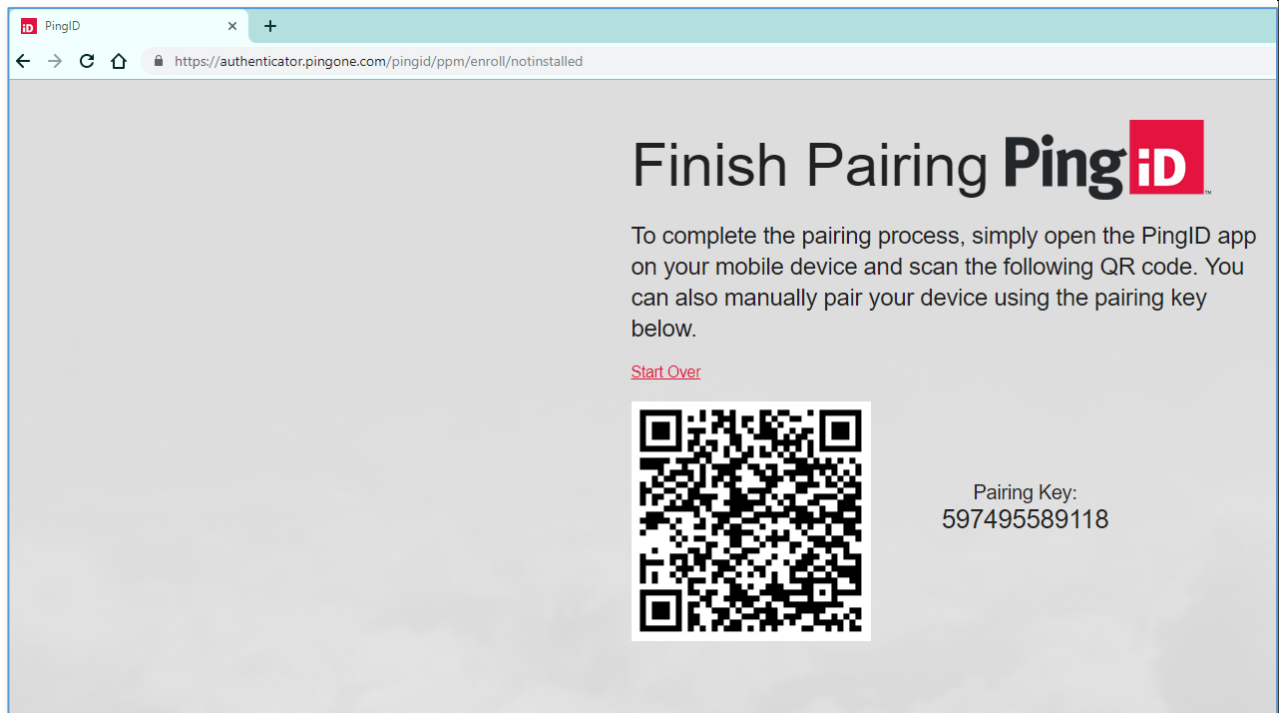
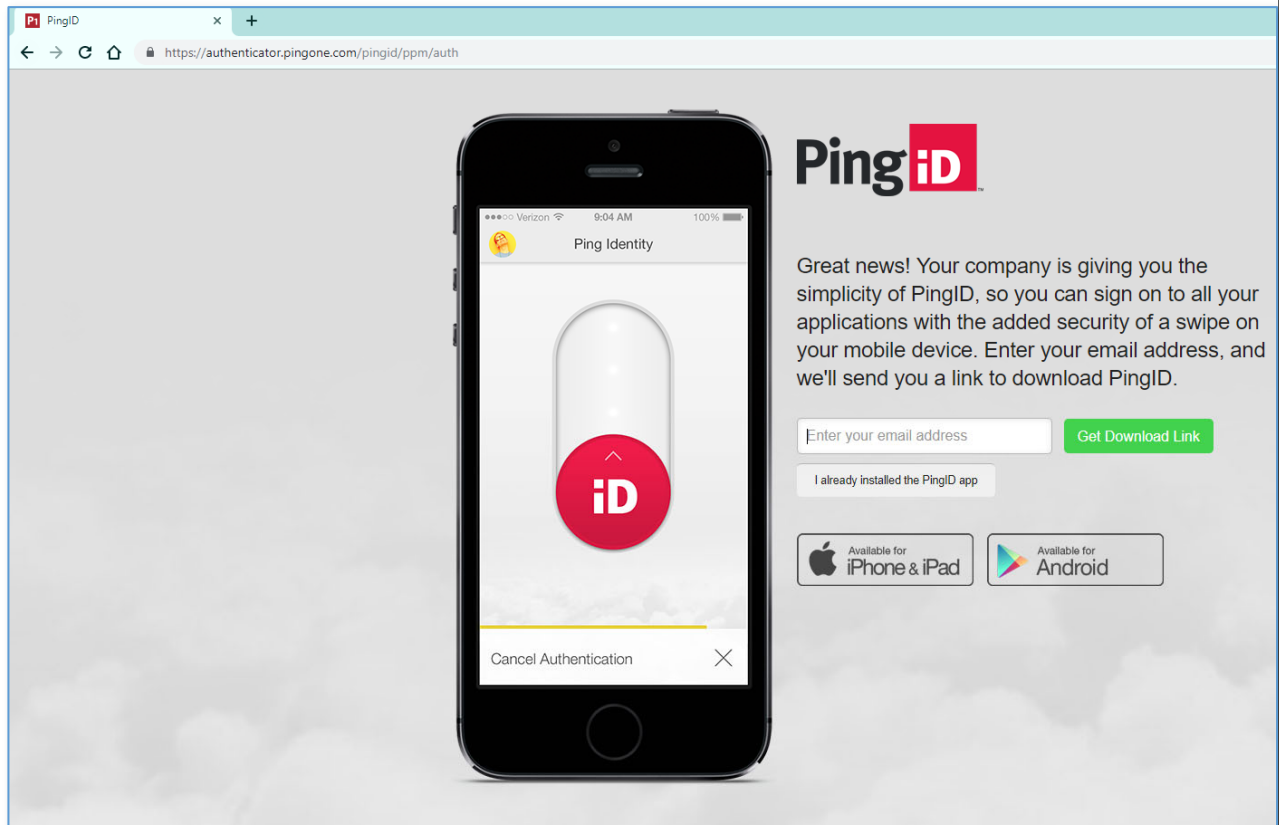
PASSWORD

Remember Me

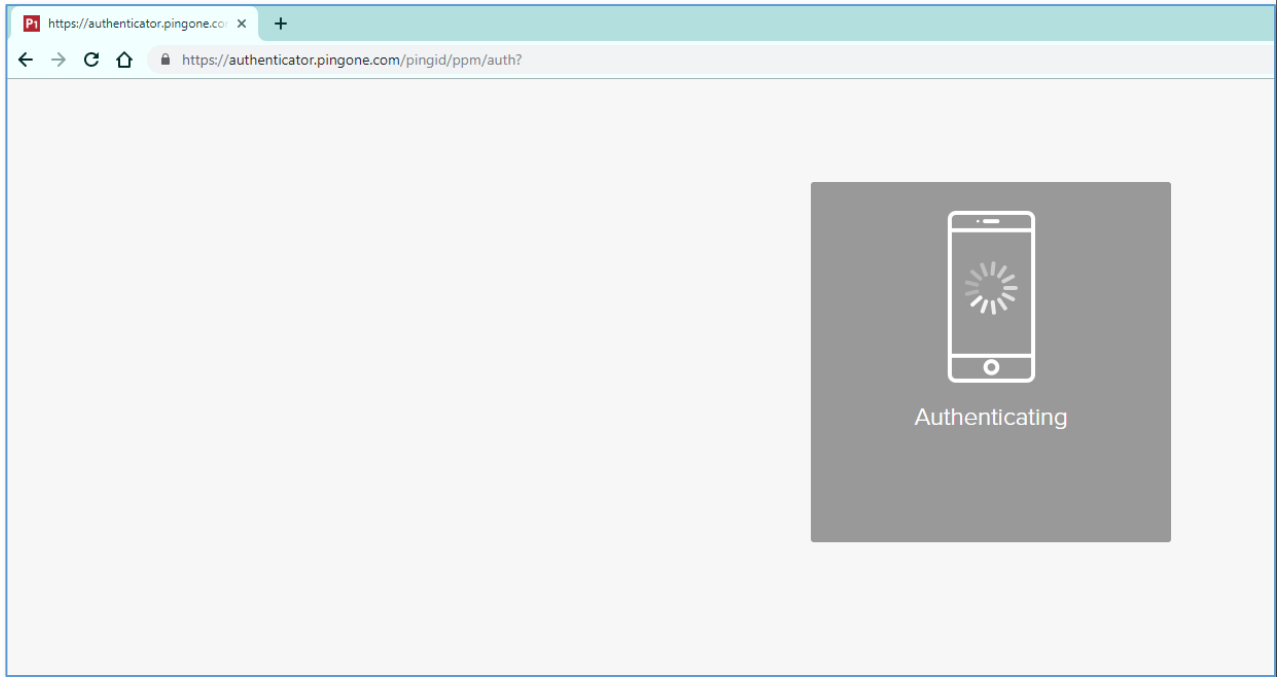
Sign On

[Forgot Password](#)

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



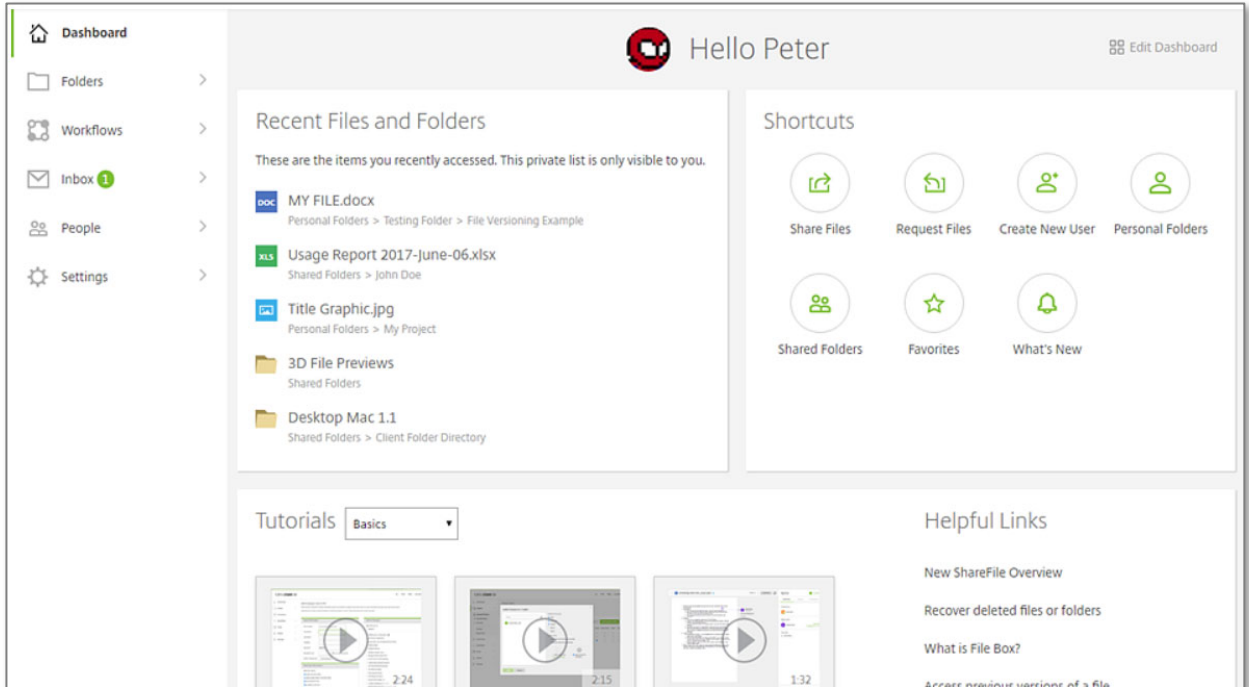
12. User will complete setup on their mobile device. Successful mobile app authentication will begin **authenticating...**



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!