

Azure migration timeline – PrismRBS-managed DNS customers

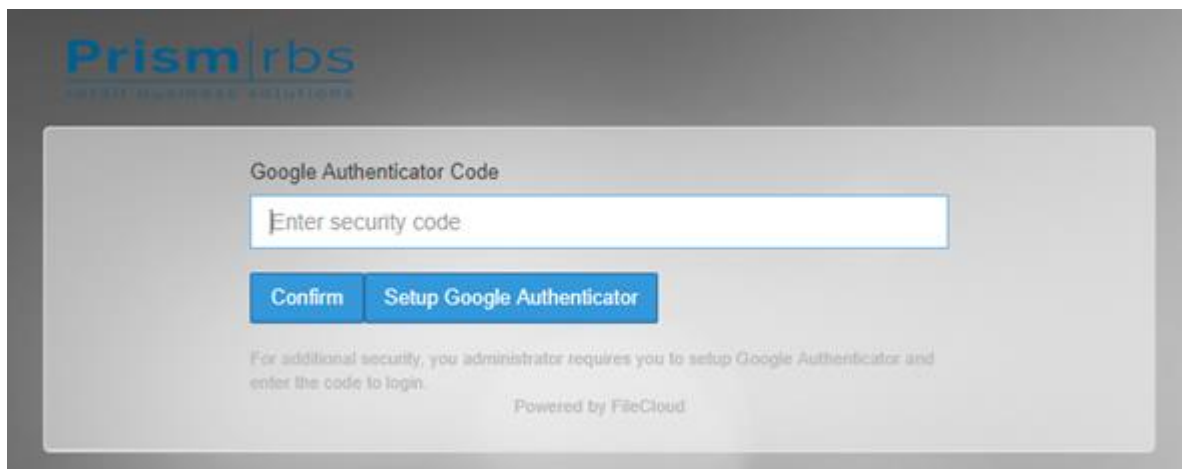
The below timeline outlines the process for the cutover of your site to the new PrismWeb environment:

Activity	Responsible	Time
Email on date and time of cutover	PrismRBS	One week prior to cutover
**If access is needed to your PrismCore system – must coordinate with your IT team	Customer	One week prior to cutover
Reminder email about date and time of cutover	PrismRBS	One day prior to cutover
Website put in maintenance mode	PrismRBS	Start of cutover
Migrate site files from old environment to Azure	PrismRBS	During cutover
Adjust DI and encryption on store's PrismCore (customer must grant PrismRBS team access)	PrismRBS	During cutover
Adjust DNS	PrismRBS	During cutover
Test new production site	PrismRBS	During cutover
Email verification that site is live and operational	PrismRBS	After cutover
Set up FileCloud 2FA	Customer	After cutover

**We will inform you if this action applies to your PrismCore system.

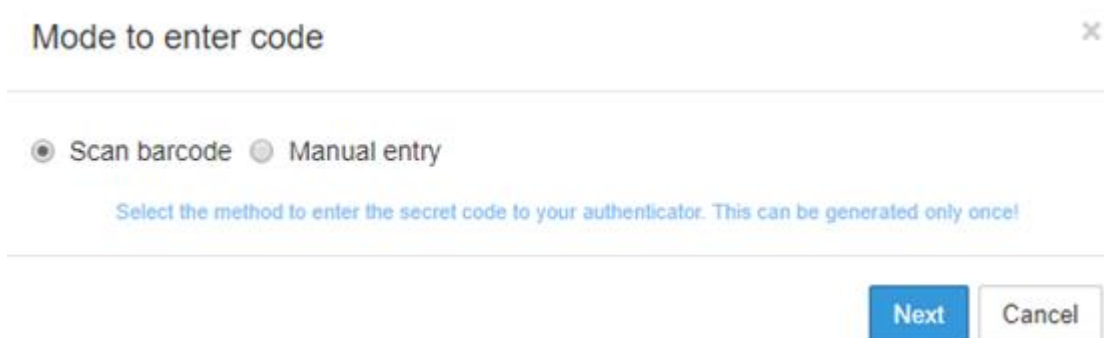
2FA Setup and Installing FileCloud Drive

1. Upon receiving the confirmation email that your cutover is complete, you will receive a one-time encrypted link to reset your FileCloud password.
2. Download and install Google Authenticator on your smart phone.
3. Open an internet browser and go to the following URL:
 - a. <https://webstage.prismservices.net:1443>
4. Login to the portal using the domain credentials provided by PrismRBS.
5. When prompted to enter your Google Authenticator code, click the “Setup Google Authenticator” button.



The screenshot shows the Prism|rbs login interface. At the top is the Prism|rbs logo. Below it, the text 'Google Authenticator Code' is displayed above a text input field with the placeholder 'Enter security code'. Below the input field are two buttons: 'Confirm' and 'Setup Google Authenticator'. Below the buttons, a message states: 'For additional security, your administrator requires you to setup Google Authenticator and enter the code to login.' At the bottom right of the message area, it says 'Powered by FileCloud'.

6. Select “Scan Barcode” and click next.



The screenshot shows a dialog box titled 'Mode to enter code' with a close button (X) in the top right corner. Below the title bar, there are two radio button options: 'Scan barcode' (which is selected) and 'Manual entry'. Below these options, a message states: 'Select the method to enter the secret code to your authenticator. This can be generated only once!'. At the bottom right of the dialog box are two buttons: 'Next' and 'Cancel'.

7. You will then be shown a QR code that can be scanned from within the Google Authenticator App on your phone.
8. After the authenticator code has been setup on your phone, you may close the QR code and enter the code from your phone into the screen from Step 4 and click "Confirm."
9. You may now close your internet browser.
10. Launch the FileCloud Client installed on your computer.
11. Update the following dialog box:

FileCloudDrive2

FileCloudDrive2 Settings

Server URL:

Account:

Password:

[Use Device Authorization Code](#)

[Use SSO](#)

Options

Mount Point:

Language:

[Proxy Settings](#)

- Server URL: <https://webstage.prismservices.net:1443/>
- Account: Your Existing Username
- Password: The securely sent password from the above email
- Mount Point: Any letter not currently assigned

12. Click "Map Drive"