

ARC 6418

GSS Sign In Two Factor Authentication with Duo

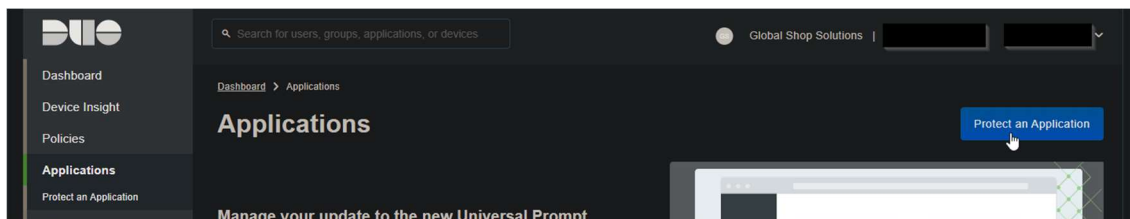
ARC 6418 is a project to enable the use of two factor authentication when signing into GSS using the Duo Auth API. When this project is enabled, and a proper Duo API account is connected, users will have push notifications sent to their mobile device when logging in to Global Shop to verify their identity. Currently, only Duo Push notification authentication, SMS authentication, and hardware token authentication is supported.

Setting up the Duo API

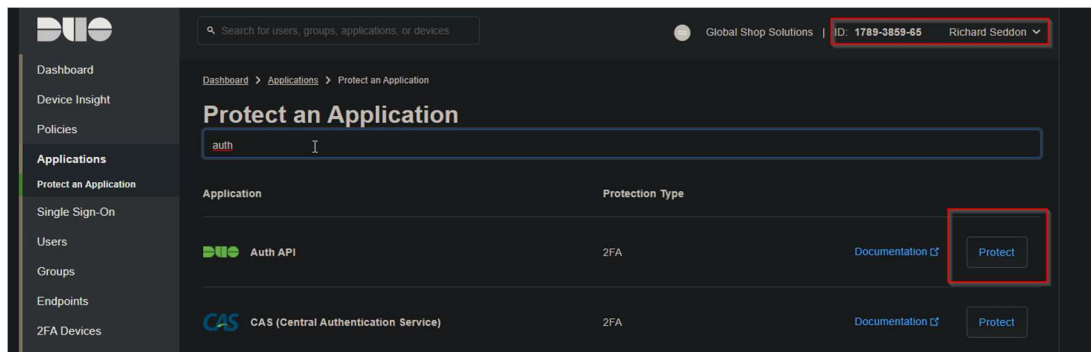
To set up the project, a Duo Auth API account needs to be created and set up. Documentation on the Duo API and setting up an application can be found here: <https://duo.com/docs/authapi>

An account needs to be created and logged into through at the following link: <https://duo.com/>

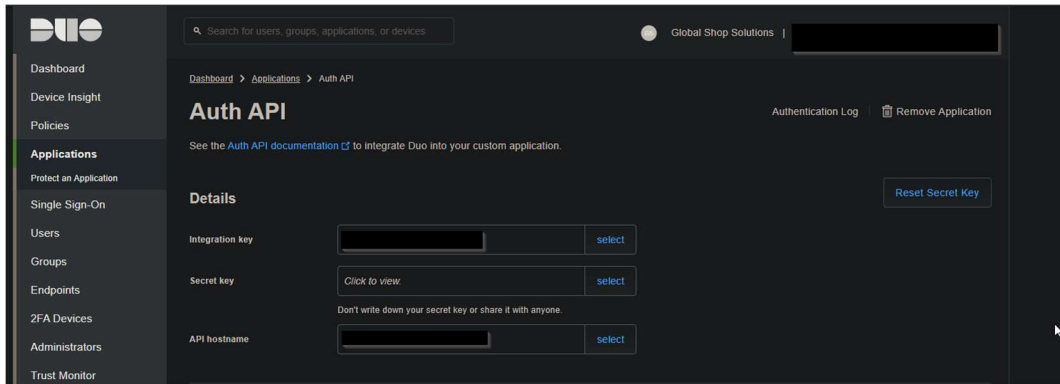
Once logged in, navigate to the Application section and click “Protect an Application” to add a new application.



Find the Duo Auth API option and click “Protect”.



At this point, you should be given a 20 character Integration Key, a 40 character Secret Key, and an API hostname in the format **api-XXXXXXXX-duosecurity.com**. These are required for the integration.



Here you can also edit the Duo policies. Make sure the authentication methods required are enabled.

Adding Users

Lastly, users will need to be added to the account. Users can be added through the Users section of the Duo website. Documentation on adding users can be found here: <https://duo.com/docs/enrolling-users>

For users, their username needs to be their email address, and their email address also needs to be entered in the Email field.

A screenshot of the Duo Admin console's 'Users' page for a specific user named 'rseddon'. The breadcrumb trail is Dashboard > Users > rseddon. At the top right, there are links for 'Logs', 'Send Enrollment Email', and 'Send to Trash'. Below this is a message: 'This user has not enrolled yet. See our enrollment documentation to learn more about enrolling users.' The form contains several fields: 'Username' (a text input), 'Username aliases' (a section with a '+ Add a username alias' link and explanatory text: 'Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).'), 'Full name' (a text input), 'Email' (a text input), and 'Status' (a radio button set with 'Active' selected and a note 'Require two-factor authentication (default)').

The email address entered will need to match the email address for the GSS user in System Support > File > User Security Maintenance.

Once the user is added, their devices can be set up.

- For Hardware tokens, go to Add Hardware Token towards the bottom of the user menu, add the tokens, and assign them to the user.
- For SMS authentication, go to Add Phone and set up their phone.
- For Duo Push authentication, add the phone the same as the SMS set up, then click “Activate Duo Mobile” in the Device Info section of the phone menu to send the user a link to download and set up the Duo Mobile app. Once they do that, they will be enabled for push authentication.

Setting up Dup API Authorization with ARC 6418

Now that the API is set up, only the Global Shop side needs to be set up. A maintenance menu for the project will be created by the ARC at System Support > Administration > Duo API Authorization Maintenance [6418]. Here, enter the Integration Key, Secret Key, and API Hostname from the Duo Auth API.

Once the API values are entered, to turn on 2FA, check the “Enable 2FA” checkbox and save. **Warning:** Only turn this one once all users are enrolled and set up for 2FA. Any users not enrolled or without proper email addresses set up in GSS will not be allowed into GSS once 2FA is turned on.

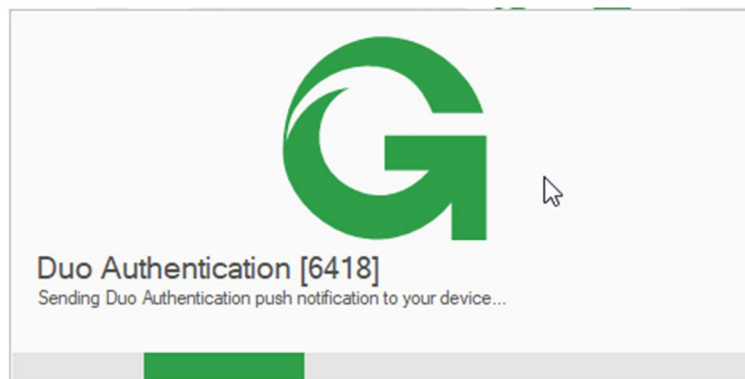
Authentication

Once 2FA has been enabled, users will be prompted for authentication once they log in to GSS. Authorization will be skipped for Online Update users, Wirepoll users, and the SUPERVSR user.

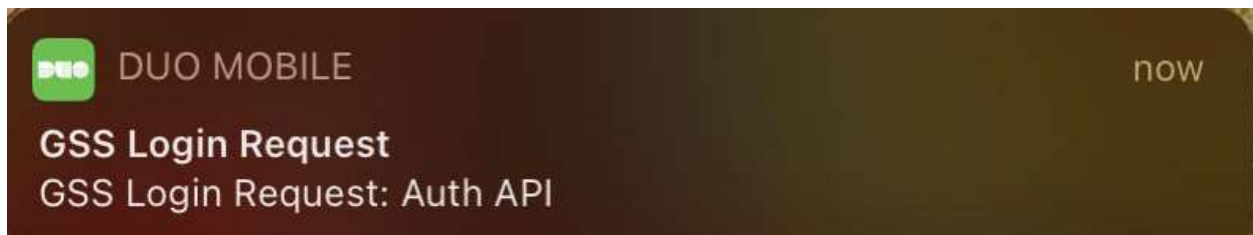


When authentication, the project will use a hierarchy. If the user has Duo Push enabled it will use that. If not, and SMS is enabled, it will use that. If not, and a hardware token is set up, it will use that.

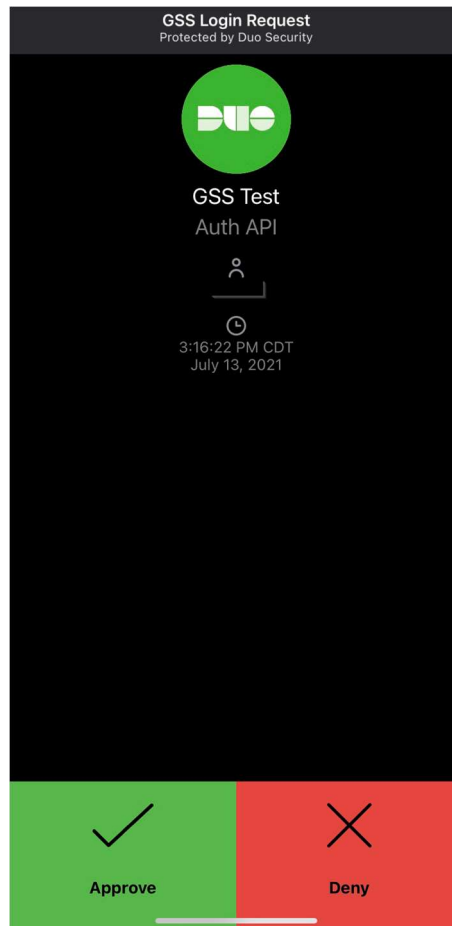
For Duo Push, the following screen will be displayed:



A Duo Push notification will be sent to their device.



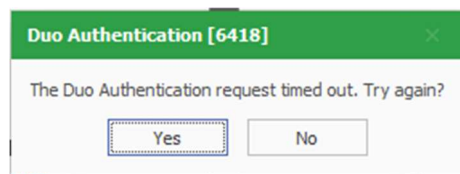
The notification can be approved or denied from the Duo App.



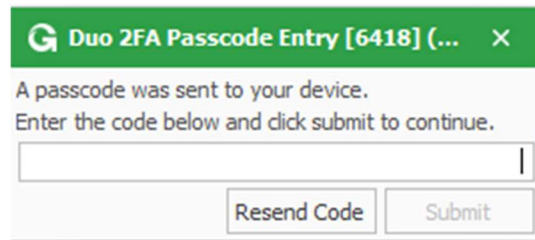
If the prompt is approved, the user will be let into GSS. If the prompt is denied, the GSS Login will be canceled.



If the request times out without a response, the user will be prompted to try again.



For SMS, the following screen will be displayed, and a code will be sent to their device:



A screenshot of a Duo 2FA Passcode Entry dialog box. The title bar is green with a white 'G' icon and the text 'Duo 2FA Passcode Entry [6418] (... X'. The main content area is white and contains the text 'A passcode was sent to your device. Enter the code below and click submit to continue.' Below this text is a text input field. At the bottom right of the dialog are two buttons: 'Resend Code' and 'Submit'.

The user can enter the code and click Submit to log in or click resend code to send the code again. If the code is entered incorrectly, the user will be prompted to try again.

For Hardware token authentication, the same screen will be displayed, and the user will need to enter the code from their hardware device.