leostream

Remote Desktop Access Platform

Using Duo MFA with Leostream

Supporting Multi-factor Authentication for your Leostream Environment

Version 9.1 and 2023
May 2023

Contacting Leostream

Leostream Corporation
77 Sleeper St.
PMB 02-123
Boston, MA 02210
USA

http://www.leostream.com
Telephone: +1 781 890 2019

To submit an enhancement request, email **features@leostream.com**.
To request product information or inquire about our future directions, email **sales@leostream.com**.

Copyright

Trademarks

The following are trademarks of Leostream Corporation.

- Leostream™
- The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

Microsoft, Active Directory, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. The Duo logo is a registered trademark of Duo Security, Inc. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

Leostream software is protected by U.S. Patent 8,417,796.

Contents

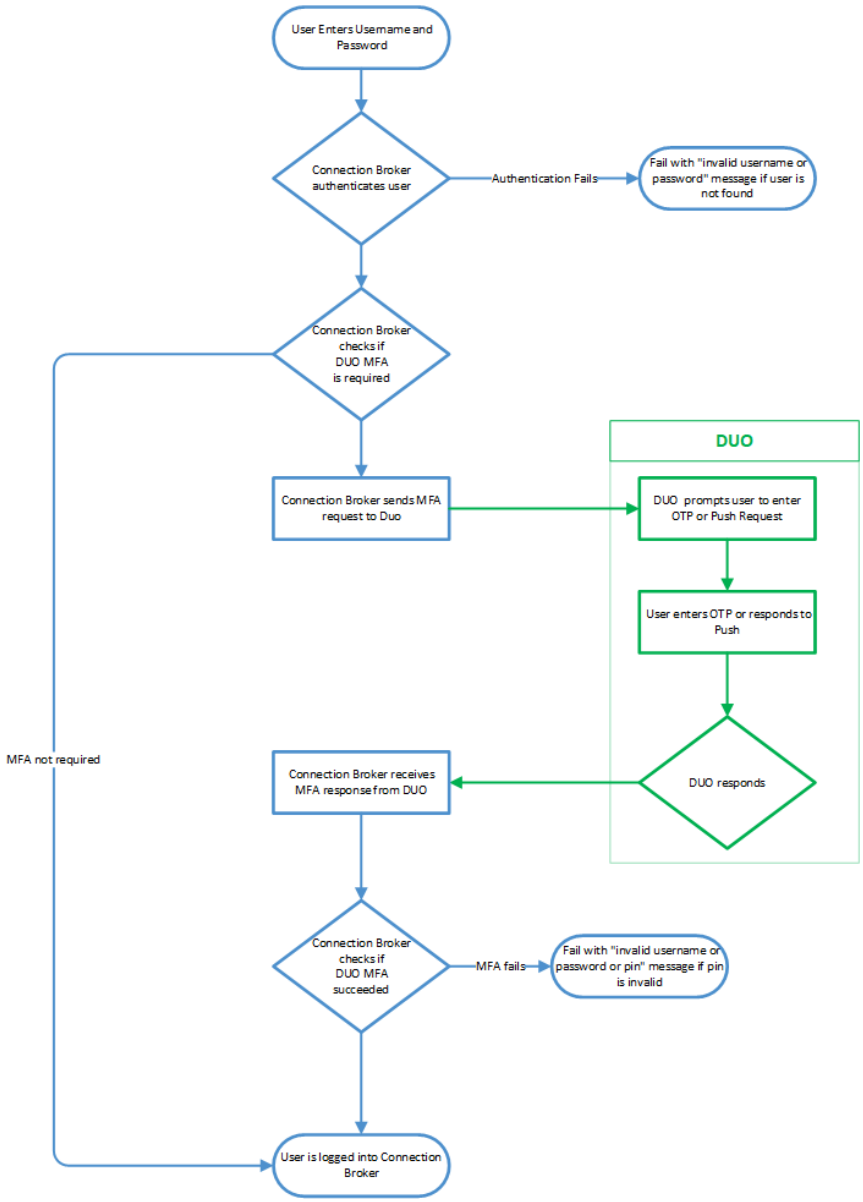
Overview

Leostream integrates with Duo Security **Duo Multi-Factor Authentication** (MFA) so you can provide a second level of security for your end-user logins.

⚠ Duo MFA is supported only for user's logging in using the Leostream Web client. If you are interested in using Duo MFA with Leostream Connect or PCoIP clients, use the Leostream support for RADIUS servers.

Authentication Workflow

The following diagram describes the when leveraging Duo Security for MFA.

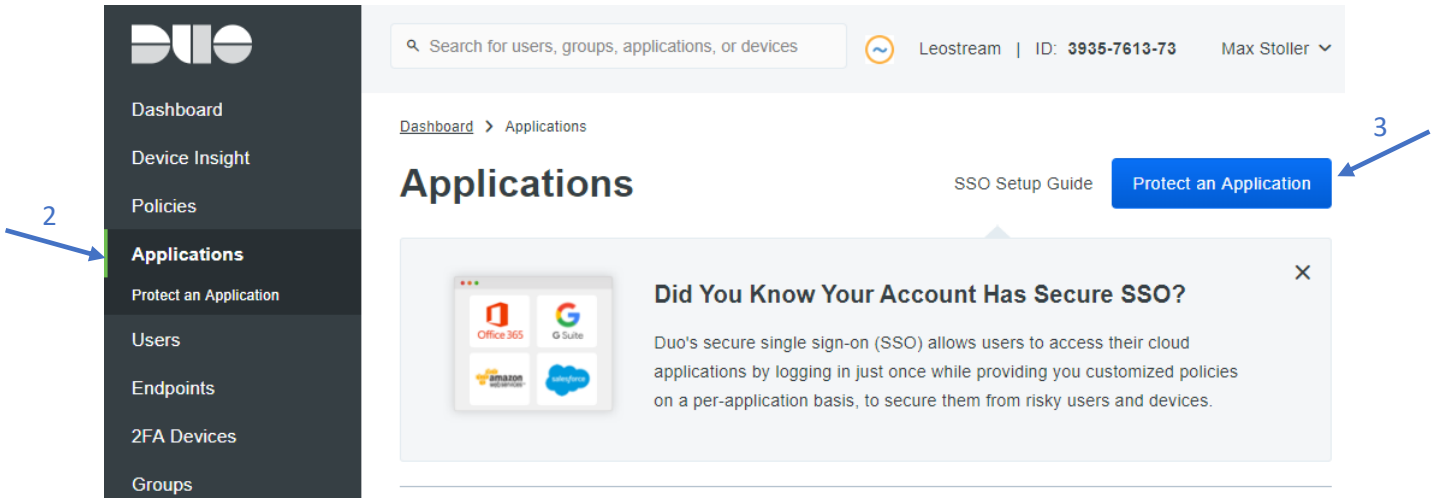


Protecting Leostream Logins in Duo

In order to protect Leostream logins with Duo MFA, add your Leostream platform as a protected Web SDK application in Duo, as follows.

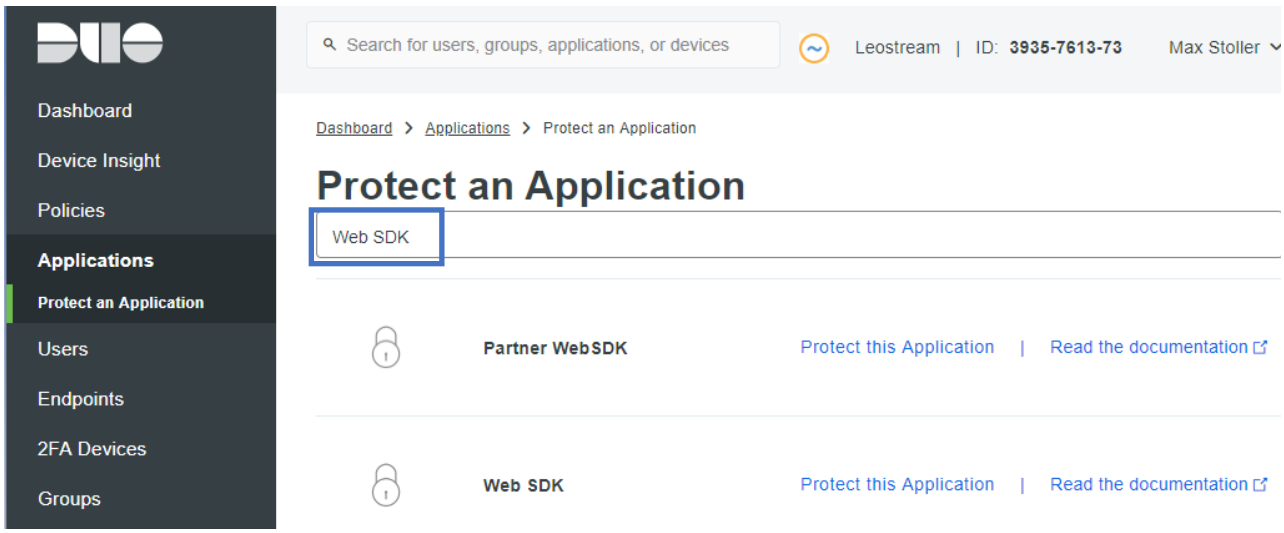
1. Go to duo.com and login as the administrator of your Duo account.

2. In the administration portal, select **Applications** from the menu, indicated with a **2** in the following figure.

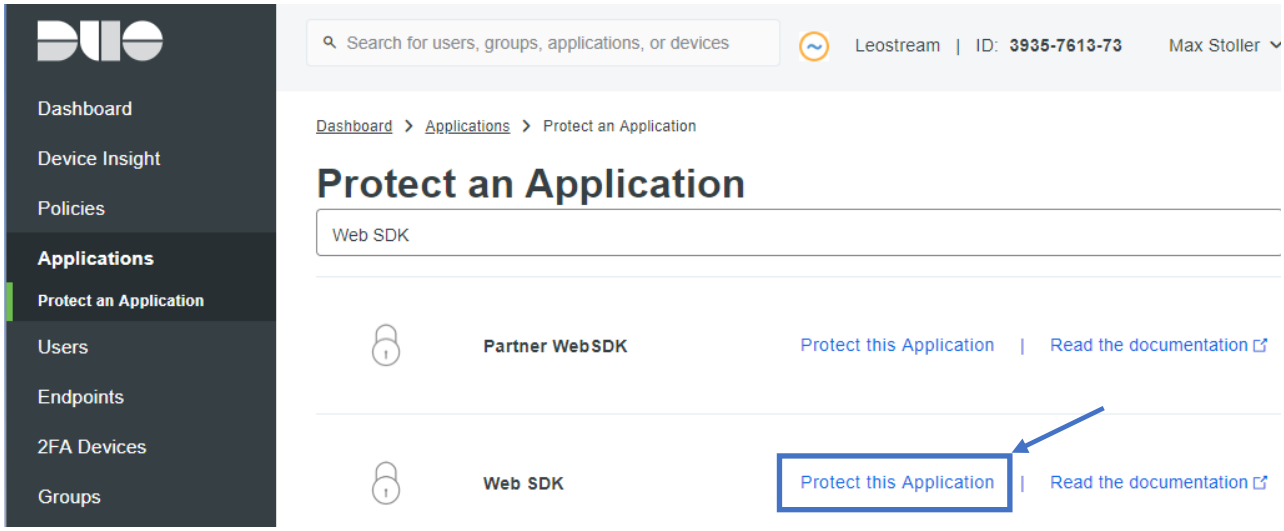


3. In the **Applications** page, click the **Protect an Application** button at the top-right, indicated with a **3** in the previous figure.

4. In the **Protect an Application** page, search for **Web SDK**, for example:

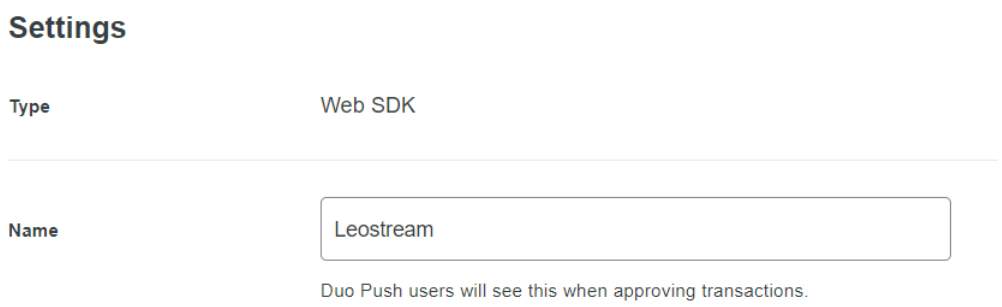


5. In the search results, click the **Protect this Application** option for the **Web SDK** application, as shown in the following figure.



6. In the **Web SDK** form that opens, modify the settings for the **Policy** section, as required by your environment. The default values are sufficient for Leostream deployments.

7. In the **Settings** section, enter in a descriptive name in the **Name** field, shown in the following figure.



8. Optionally check the **Self-service portal** option if you want to allow users to remove devices, add new devices, and reactivate Duo Mobile.

9. Modify any additional settings you require for voice greetings, notes, etc., and click **Save**.

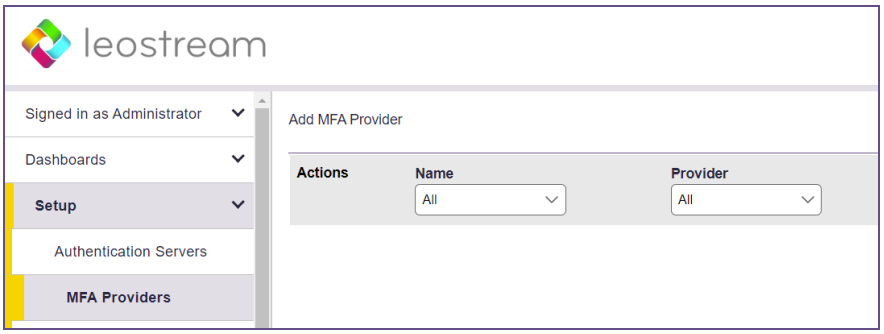
A message indicating you successfully modified your applications appears. Leave this page open in your browser window while configuring Leostream in a separate window, as described in the following section.

Configuring Leostream to Use Duo MFA

After adding Leostream as a protected Web SDK application in Duo, you must add Duo as an MFA provider in your Leostream Connection Broker.

1. In a new browser window, log into your Leostream Connection Broker Administrator web interface.

2. Go to the **> Setup > MFA Providers** page, shown in the following figure.

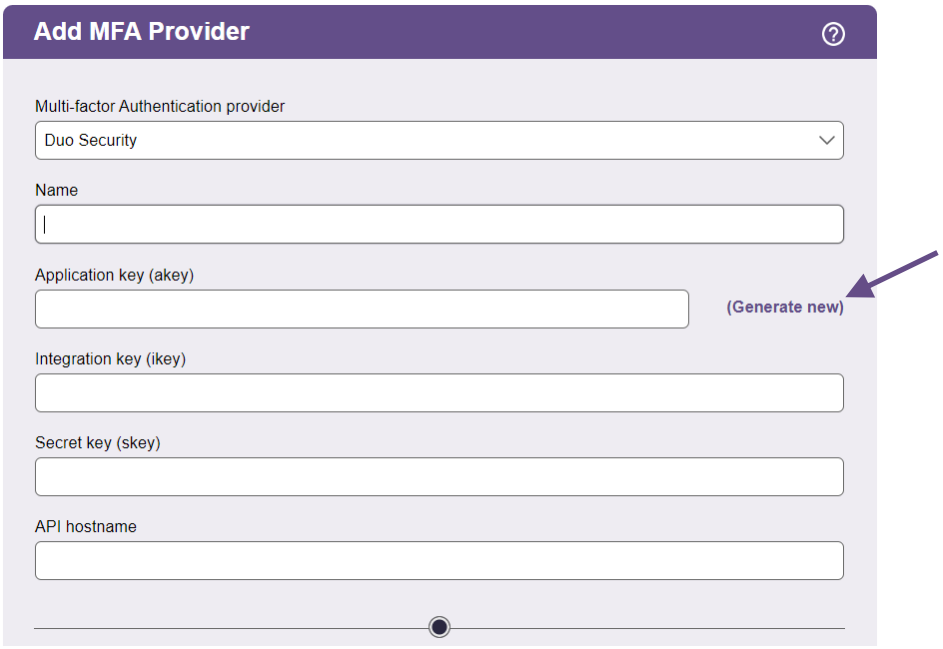


3. Click the **Add MFA Provider** link at the top of the page.

4. In the **Add MFA Provider** form, select **Duo Security** from the **Multi-factor Authentication Provider** drop-down menu.

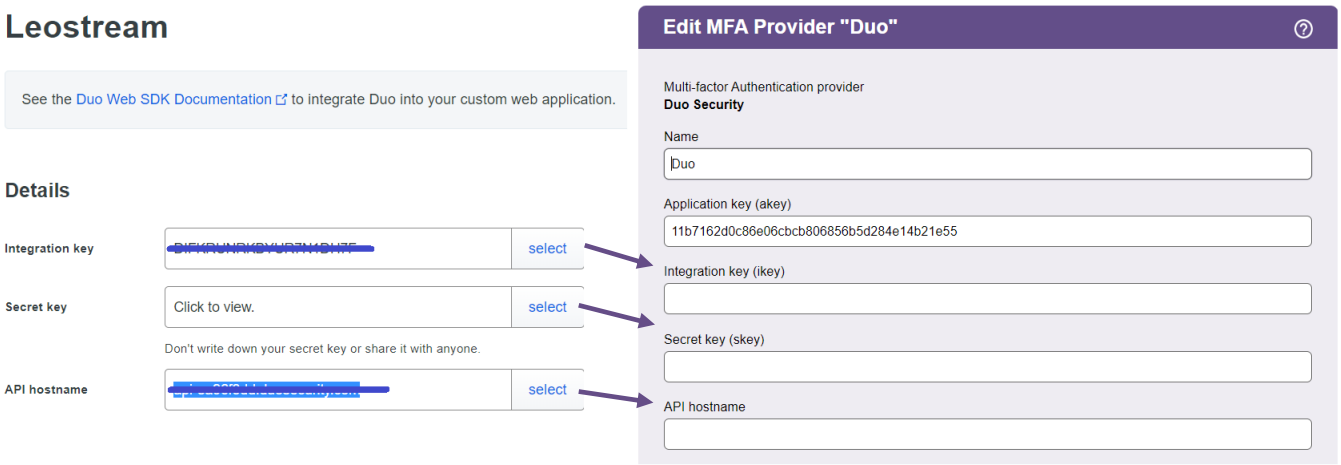
5. Enter a display name for Duo MFA in the **Name** field.

6. Click the **Generate new** link next to the **Application key** field, indicated in the following figure.



Clicking the link generates a random `akey` value and places it in the **Application key** edit field. This value is required by Duo.

Fill in values for the **Integration key**, **Secret key**, and **API hostname** fields in the **Add MFA Provider** using information from the protected Web SDK application you created in Duo. The fields in the Leostream **Add MFA Provider** form map to fields in Duo, as shown in the following figure.



7. Copy the **Integration key** value from the protected Web SDK application in Duo into the **Integration key** field in the **Add MFA Provider** form in Leostream.

8. Click in the **Secret key** field in the protected Web SDK application in Duo to view and copy the secret key. Paste the secret key value into the **Secret key** field in the **Add MFA Provider** form in Leostream.

9. Copy the **API hostname** value from the protected Web SDK application in Duo into the **API hostname** field in the **Add MFA Provider** form in Leostream.

10. Click **Save** on the **Add MFA Provider** form in Leostream.

⚠ If you set the **Web server "Cross-Origin-Embedder-Policy" HTTP header** option on your Connection Broker **> System > Settings** page to `require_corp` then you must configure Duo to return a value of `cross-origin` to ensure that Leostream has permission to use the Duo resource.

Specifying Leostream Users Who Require MFA

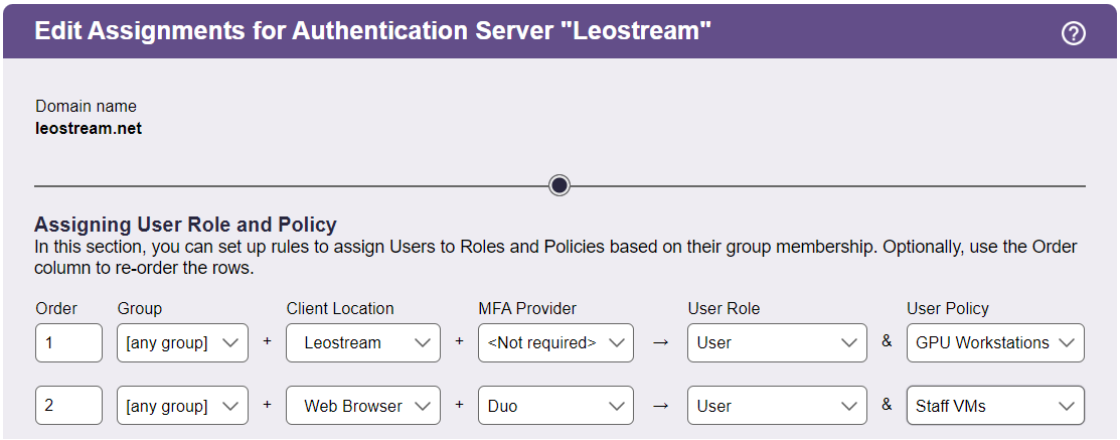
You use the tables on the **> Configuration > Assignments** page to control which users are required to pass Duo MFA based on their AD group membership and their location. By default, no users require MFA. To enable MFA:

1. Go to the **> Configuration > Assignments** page in your Leostream Connection Broker.

2. Click the **Edit** action for the assignments table associated with the authentication server whose users require MFA.

3. Use the **MFA Provider** drop-down menu to indicate which users require Duo MFA.

   For example, in the following figure, users who log in from the **Leostream** location are not required to pass Duo MFA in order to log into Leostream. However, the same users logging in from a **Web Browser** location do require Duo MFA.

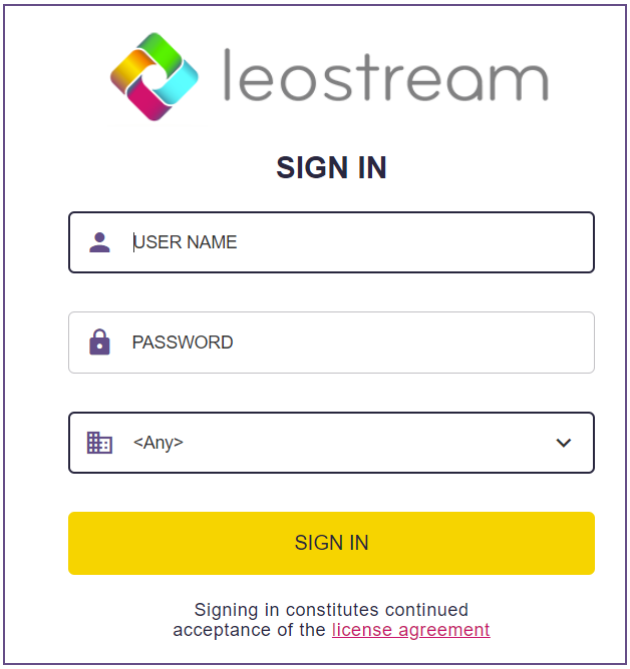


End-User Login Workflow

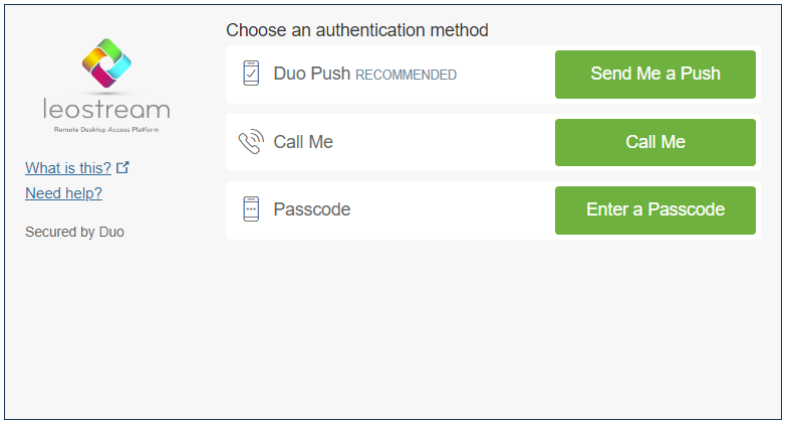
⚠ Duo MFA is currently supported only for Leostream Web client logins.

When logging in using the Leostream Web client, users whose logins are protected by Duo MFA must complete a second authentication step prior to receiving their offered resources.

To start the Leostream login process, users first go to their Leostream Web portal, for example:



After the user enters their credentials and clicks **SIGN IN**, Leostream validates the user's credentials against Active Directory. If this first authentication step passes, Leostream directs the user to Duo for a second authentication step, for example:



The page your users see may vary if you configured the properties for your protected Web SDK application differently in Duo. Only after the user successfully passes the Duo MFA step will Leostream display the user's offered desktops.

If the Duo MFA request times out or is denied, the Leostream login is blocked, for example: