



leostream[®]

Remote Desktop Access Platform

Using Duo MFA with the Leostream[®] Platform

Supporting Multi-factor Authentication for your Leostream Environment

Version 202x
March 2024

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

© Copyright 2002-2024 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

Trademarks

The following are trademarks or registered 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

CONTENTS	3
OVERVIEW	4
AUTHENTICATION WORKFLOW	4
CREATING AN APPLICATION FOR THE LEOSTREAM PLATFORM	5
CONFIGURING LEOSTREAM TO USE DUO MFA	7
UPDATING TO THE DUO UNIVERSAL PROMPT	8
SPECIFYING LEOSTREAM USERS WHO REQUIRE MFA	10
END-USER LOGIN WORKFLOW	11

Overview

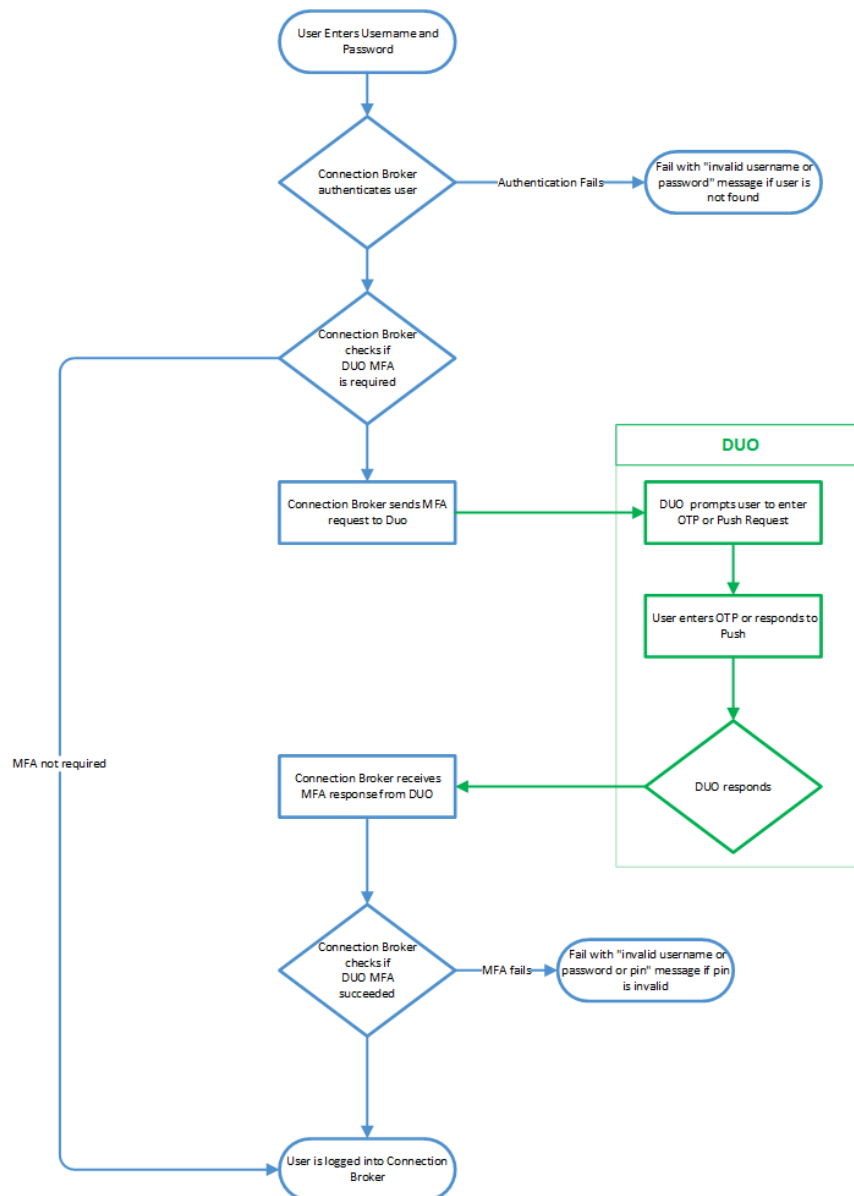
The Leostream Platform integrates with Duo Security **Duo Multi-Factor Authentication** (MFA) so you can provide a second level of security for your end-user logins.



Duo MFA is supported only for user's logging in using the Leostream Web client. To use Duo MFA with Leostream Connect or PColP clients, use the Leostream Platform support for the RADIUS protocol.

Authentication Workflow

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



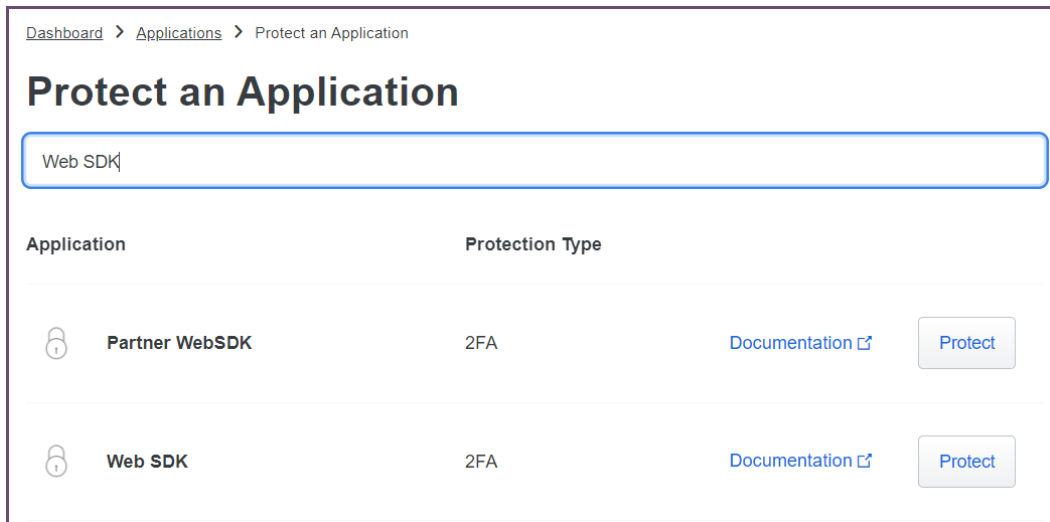
Creating an Application for the Leostream Platform

In order to protect Leostream platform 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** button for the **Web SDK** application, indicated in the following figure.

Dashboard > Applications > Protect an Application

Protect an Application

Web SDK

Application	Protection Type		
 Partner WebSDK	2FA	Documentation	<button>Protect</button>
 Web SDK	2FA	Documentation	<button>Protect</button>



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

Settings

Type Web SDK

Name

Duo Push users will see this when approving transactions.

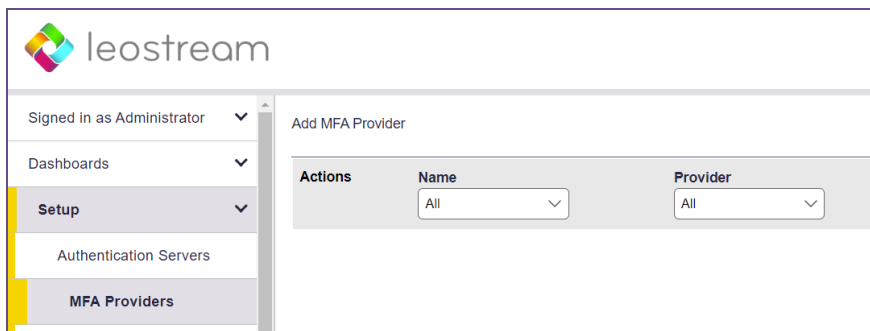
- Optionally check the **Self-service portal** option if you want to allow users to remove devices, add new devices, and reactivate Duo Mobile.
- Modify any additional settings you require for voice greetings, notes, etc., and click **Save**.

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

Configuring the Connection Broker to Use Duo MFA

After adding your Leostream platform 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.



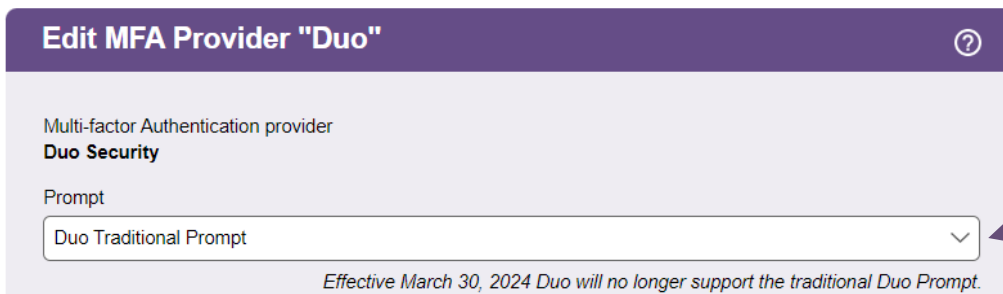
3. Click the **Add MFA Provider** link at the top of the page.
4. In the **Add MFA Provider** form, select **Duo Security** from the **Multi-factor Authentication provider** drop-down menu.
5. Enter a display name for Duo MFA in the **Name** field.
6. Fill in values for the **Client ID**, **Client secret**, and **API hostname** fields in the **Add MFA Provider** form using the associated information from the protected Web SDK application you created in Duo.
7. In the **Redirect URI** field, optionally enter the address where Duo should redirect users after they successfully authenticate. Leave the field blank to instruct the Connection Broker to select a redirect URI based on the HTTP headers of the user's browser, searching first for an HTTP Origin header. If no appropriate headers are found, the redirect URI defaults to your Connection Broker VIP.
8. Click **Save** on the **Add MFA Provider** form in the Connection Broker.

Updating to the Duo Universal Prompt

Effective March 30, 2024, Duo no longer supports the Traditional Duo Prompt. To use the preferred Duo Universal Prompt, you must upgrade to Connection Broker 2024.1 or later.

 The Duo Universal Prompt requires the use of HTTPS and a valid Hostname, not an IP address, for the Redirect URI. Currently, the Connection Broker uses the Connection Broker VIP in the Redirect URI. Ensure that the **Connection Broker Virtual IP (VIP) address or hostname** field on the **> System > Settings** page indicates the VIP is an FQDN and not an IP address. If the VIP is set to an IP address, the redirect to the Duo Universal Prompt fails with an error indicating `Invalid redirect URI`.

After you upgrade your Connection Broker, the **Edit MFA Provider** page includes an option to upgrade your Duo integration to use the new Duo Universal Prompt, as shown in the following figure. This option allows you to toggle between the Duo Traditional and Universal Prompt until your Connection Broker successfully activates your Duo Application. After that point, The **Prompt** drop-down menu no longer appears, and your Connection Broker will use the Traditional or Universal Prompt as specified in the Application for your Leostream platform in Duo.



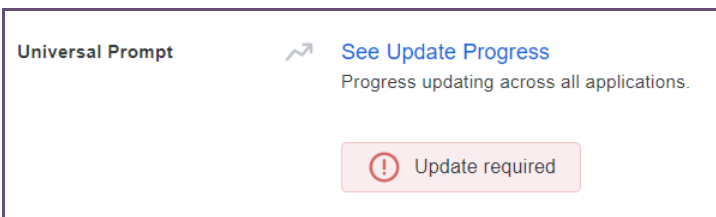
To upgrade your Connectoin Broker to use the new Duo Universal Prompt:

1. Go to your Connection Broker **> Setup > MFA Providers** page.
2. Click **Edit** for your Duo MFA provider
3. From the **Prompt** menu, select the **Duo Universal Prompt** option. The remainder of the form updates to show the configuration options required for the Duo Universal Prompt, for example:

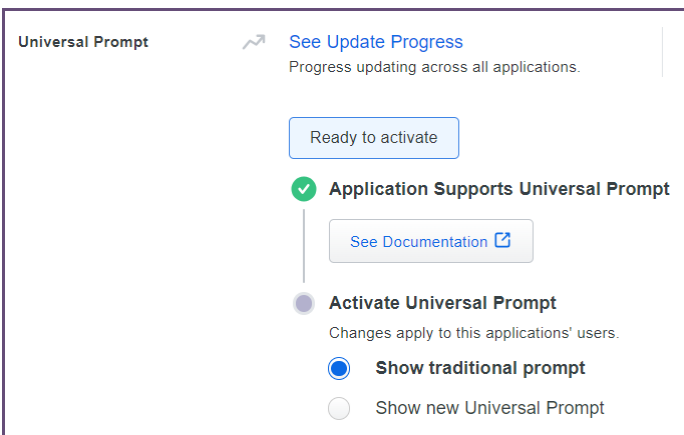
4. Click **Save**.



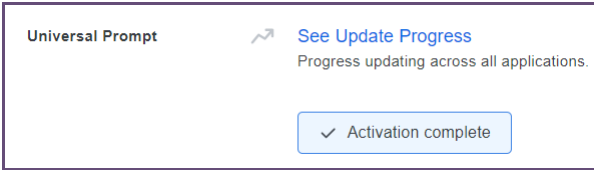
After you edit the MFA Provider settings, a user must successfully authenticate into your Leostream environment using Duo in order for Duo to recognize that your Connection Broker now supports the Universal Prompt. Until then, the Application for your Leostream environment in Duo continues to indicate it requires an update, for example:



The first user to log in after switching your Duo integration to use the Universal Prompt continues to use the Traditional Prompt. After this first successful Leostream login, your Leostream Application in Duo is ready to be Activated, for example:



To activate, select the **Show new Universal Prompt** option shown in the previous figure. Users who subsequently log into your Leostream environment are presented with the Universal Prompt. After the first user successfully logs in using the Universal Prompt, the Application for your Leostream platform in Duo shows that Activation is complete, for example:



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 the Leostream platform. However, the same users logging in from a **Web Browser** location do require Duo MFA.


Edit Assignments for Authentication Server "Leostream" ?

Domain name
leostream.net

Assigning User Role and Policy
In this section, you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally, use the Order column to re-order the rows.

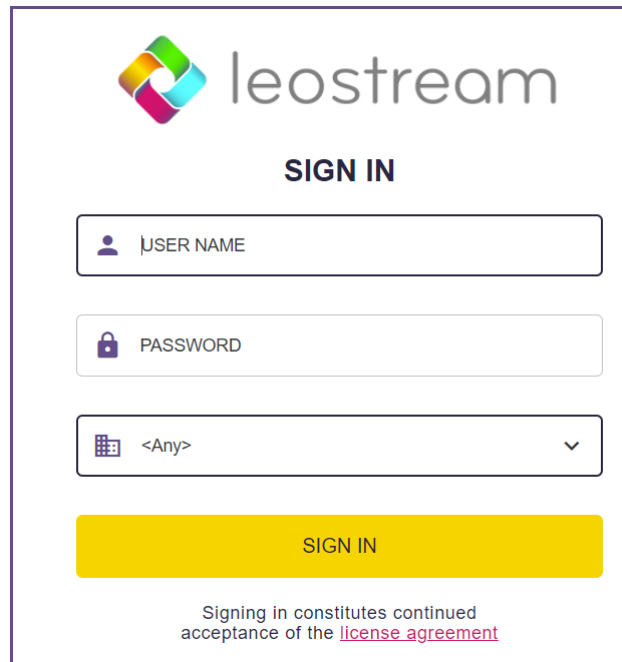
Order	Group	Client Location	MFA Provider	User Role	User Policy
1	[any group] ▼	Leostream ▼	<Not required> ▼	→ User ▼	& GPU Workstations ▼
2	[any group] ▼	Web Browser ▼	Duo ▼	→ User ▼	& Staff VMs ▼

End-User Login Workflow

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

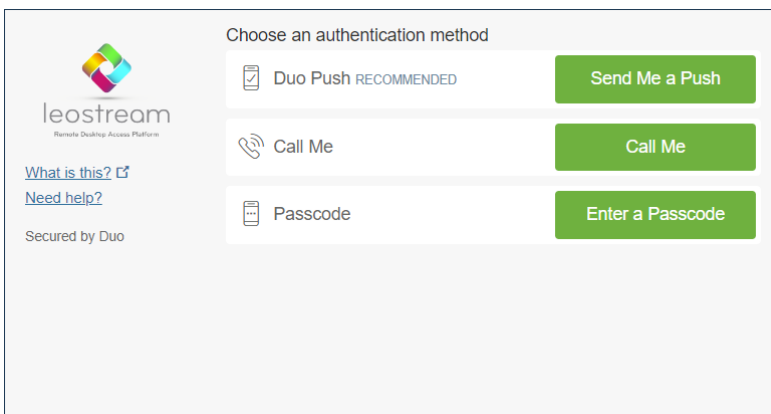
When logging in using the Leostream Web client, users whose logins are protected by Duo MFA must complete a second authentication step prior to receiving their offered resources.

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



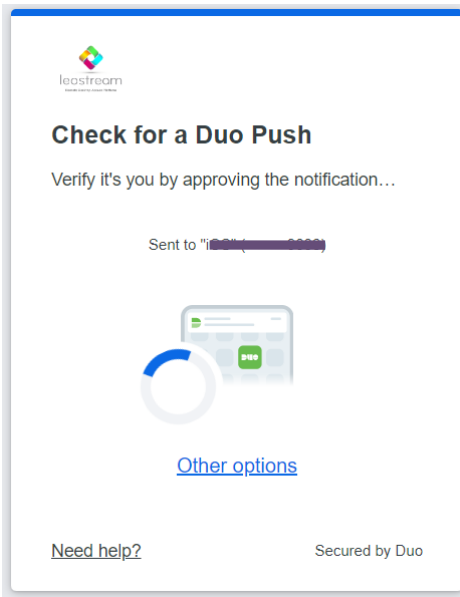
The image shows a Leostream sign-in form. At the top is the Leostream logo, which consists of a colorful geometric shape followed by the word "leostream". Below the logo is the text "SIGN IN". There are three input fields: the first is labeled "USER NAME" with a person icon, the second is labeled "PASSWORD" with a lock icon, and the third is a dropdown menu labeled "<Any>" with a grid icon and a downward arrow. Below these fields is a large yellow button labeled "SIGN IN". At the bottom, there is a line of text: "Signing in constitutes continued acceptance of the [license agreement](#)".

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



The image shows a Duo authentication prompt. On the left is the Leostream logo and the text "leostream Remote Desktop Access Platform". Below this are links for "What is this?" and "Need help?", and the text "Secured by Duo". On the right, under the heading "Choose an authentication method", there are three options: "Duo Push RECOMMENDED" with a checkmark icon and a "Send Me a Push" button, "Call Me" with a phone icon and a "Call Me" button, and "Passcode" with a passcode icon and an "Enter a Passcode" button.

Or, when using the Universal Prompt:



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.