LEOSTREAM™

Using RADIUS Servers for MFA with Leostream

Supporting Multi-Factor Authentication in your Leostream Environment

Version 9.0.40
February 2021

Contacting Leostream

Leostream Corporation
271 Waverley Oaks Rd.
Suite 204
Waltham, MA 02452
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. Okta is a trademark of Okta, 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 can communicate with RADIUS servers to enable multi-factor authentication (MFA) for your end-user logins. Any RADIUS server or Identity Provider with a RADIUS component or agent, such as Okta and Duo, can be used with Leostream.

RADIUS MFA is supported when users log into Leostream using any of the following client devices.

- The Leostream Web client
- Leostream Connect for Windows
- Leostream Connect for Linux and macOS
- PCoIP Zero clients
- PCoIP Software clients

Users can perform MFA by entering a one-time passcode or requesting a push notification.

Authentication Workflow and Requirements

When using a RADIUS server to provide MFA for Leostream users, the first authentication factor is always username and password. You can use Active Directory, an OpenLDAP server, a NIS server, or even your Connection Broker as the first authentication server.

You then enable MFA for groups of users in your authentication server or per-user if the user is defined locally in the Connection Broker.

The authentication workflow depends on if the user enters a one-time passcode or requests a push notification.

Entering a One-Time Passcode

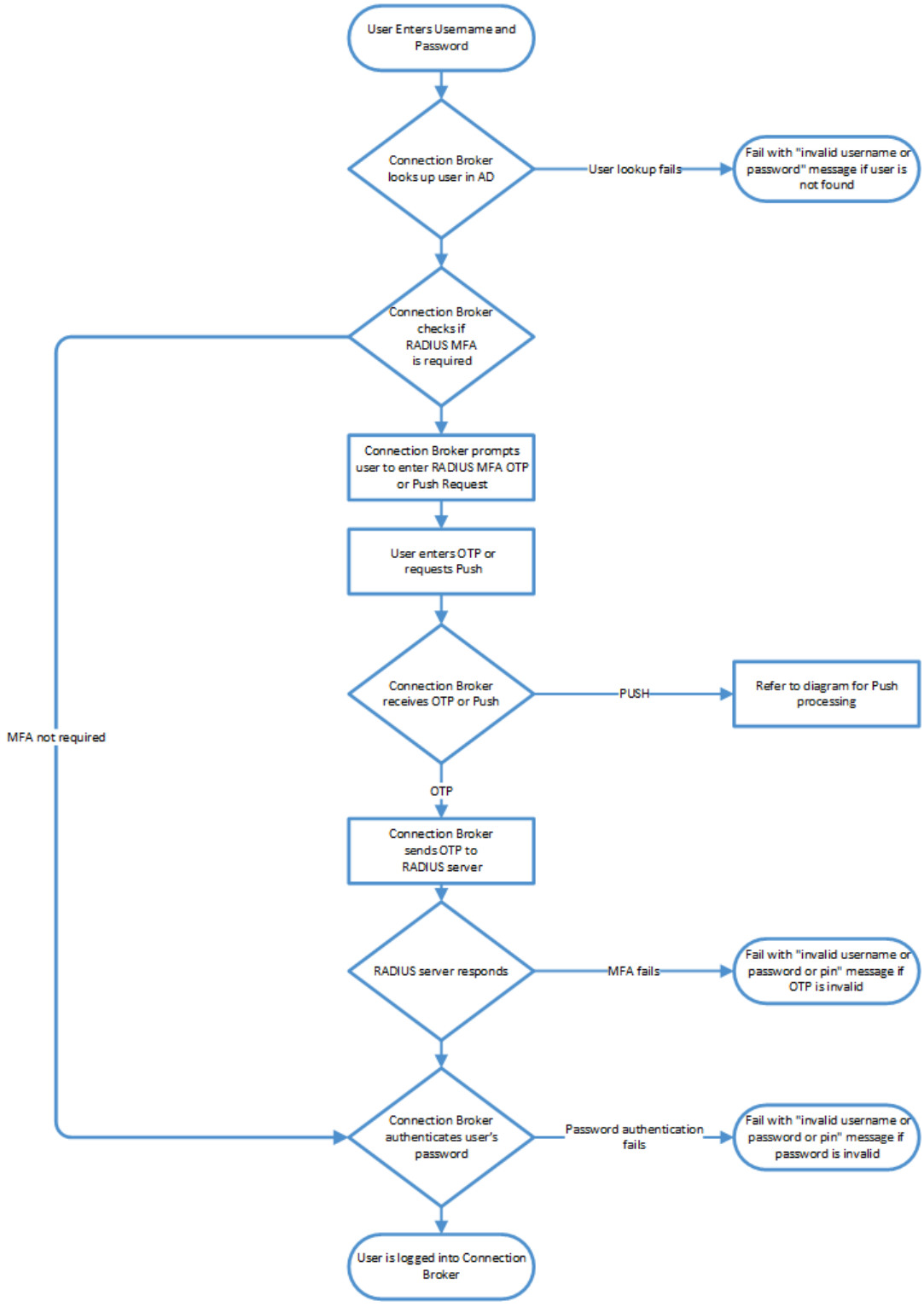
In this scenario the Connection Broker first locates the user in one of your authentication servers using the username exactly as the user typed it into the login form. This username is matched against the attribute entered in the **Match username against this field** edit field of your authentication server, typically sAMAccountName for Active Directory.

If the Connection Broker finds a matching user in your authentication server, the Connection Broker retrieves the value for the **Match username against this field** attribute as stored in your authentication server and the user's group attributes. If the user is a member of a group that requires MFA, the Connection Broker then prompts the user for the alphanumeric string to send to the RADIUS server.

The Connection Broker sends the username as returned by your authentication server and the entered alphanumeric string to the RADIUS Server. If the RADIUS server returns success *and* the authentication server password validation succeeds, the user is finally allowed to log into Leostream.

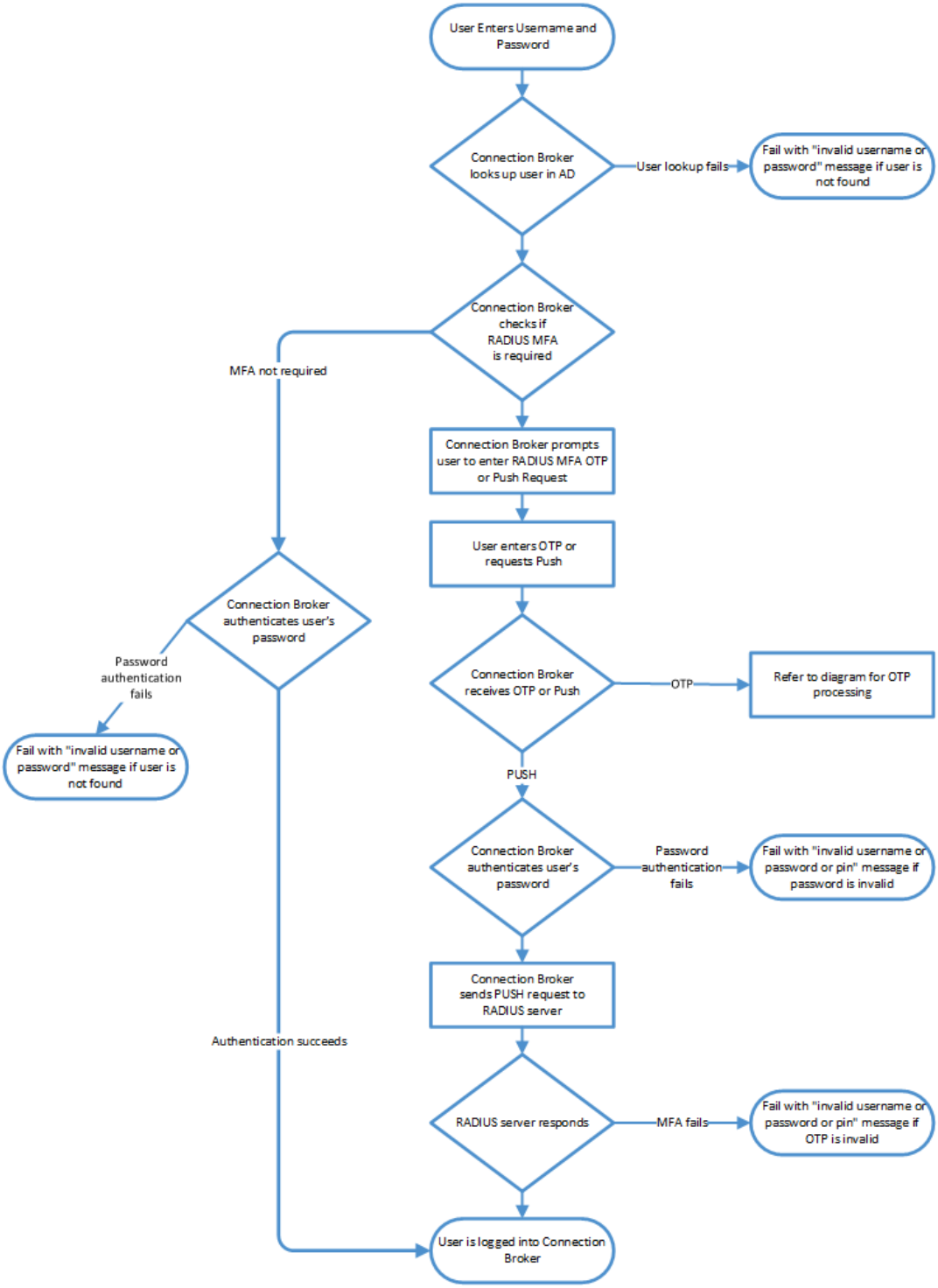

If your RADIUS server is case sensitive, ensure that the user is defined in your RADIUS server using the exact attribute value that is stored in your authentication server.

The following flow chart describes this workflow.



Requesting a Push Notification

If the user requests a push notification as the second factor of authentication, the authentication work changes slightly, as described in the following diagram. In this case, the Connection Broker validates the user's password before sending the push request to the RADIUS authentication server.

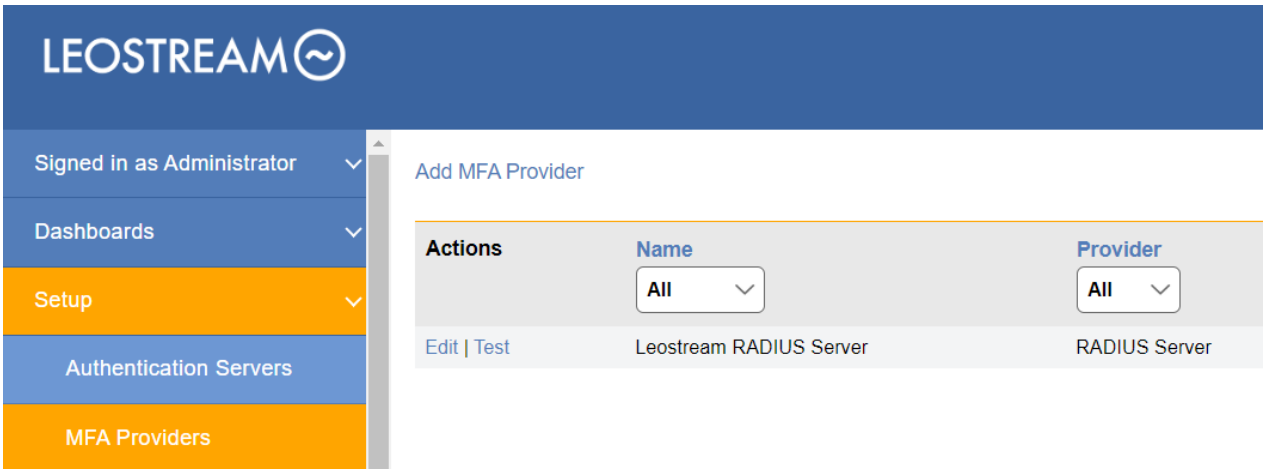


Configuring Leostream to Communicate with RADIUS Servers

The Connection Broker can integrate with multiple RADIUS servers, allowing you to use different identity providers for different groups of users. You integrate Leostream with a RADIUS server, as follows.

1. 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 **RADIUS Server** from the **Multi-factor Authentication Provider** drop-down menu.

5. Enter a display name for RADIUS Server in the **Name** field.

6. Enter the IP address or hostname of the RADIUS Server or Agent in the **Server IP or hostname** field.

7. In the **RADIUS port** edit field, enter the port used by your RADIUS server.

   ⚠ RADIUS is a UDP protocol. If your RADIUS server is behind a firewall, security group, or access control list, ensure that the RADIUS port is open for UDP traffic.

8. Specify the **RADIUS shared secret** needed to communicate with the RADIUS server or agent.

9. In the **Timeout** edit field, specify the time interval that the Connection Broker waits for the RADIUS server to reply before sending a subsequent request.

   ⚠ If you plan to allow users to request Push notifications, consider increasing the default timeout (30 seconds) to provide users with adequate time to receive and respond to the push notice.

10. In the **Retries** edit field, specify the number of times the Connection Broker tries to send the RADIUS request before concluding that the RADIUS server cannot be contacted.

    ⚠ If you plan to allow users to request Push notifications, leave this at the default value of one retry to avoid sending the user multiple push notifications.

11. Select the **Generate Message-Authenticator attributes for Access-Requests** option if you need to use the Message-Authenticator attribute to sign packets sent to your RADIUS server. This is not common, but may be necessary if your Connection Broker returns "Failed RADIUS authentication: bad response authenticator" errors when attempting to communicate with your RADIUS server.

12. Select the **This RADIUS provider can send Push notifications** options if the identity provider associated with this RADIUS server supports push notifications by sending a passcode value of `push`. The Connection Broker automatically sends the `push` passcode to the RADIUS server when the user clicks the button to request a push notification. With this option enabled, users still have the ability to enter a one-time passcode.

13. Click **Save** on the **Add MFA Provider** form.

The Connection Broker validates the hostname and port are correct, but does not validate your shared secret when you save the form. To check if you correctly entered the shared secret, perform a test for the RADIUS server. Incorrect shared secrets result in a "bad response authenticator" error.

Testing and Troubleshooting

Use the **Test** action for the Radius server to validate that your Connection Broker can communicate with your RADIUS server.

If the test fails because Leostream cannot contact the RADIUS server, double-check that your shared secret is entered correctly and that no firewall, security group, or access control list is blocking traffice from your Connection Broker to your RADIUS UDP port.

You can use the `nc` utility to scan ports and test your Connection Broker can reach your RADIUS Server, using the following command.

```
/usr/bin/nc -z -v -u RADIUS-IP 1812
```

Replace 1812 with your RADIUS server port, if you are not using the default. Note, in some cases this utility can return success even if an external firewall later blocks the traffic.

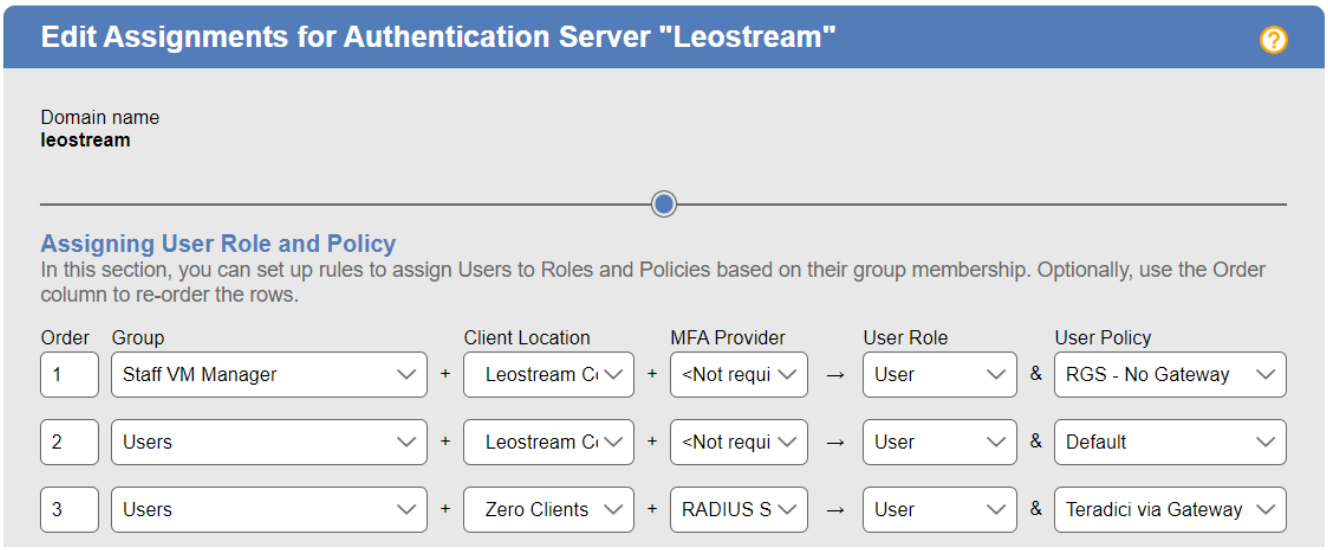
Specifying Leostream Users Who Require MFA

You use the tables on the **> Configuration > Assignments** page to control which domain users are required to pass 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 MFA.
   For example, in the following figure **Users** who log in using Leostream Connect are not required to pass MFA in order to log into Leostream. However, the same **Users** logging in from the **Zero Clients** do require MFA.

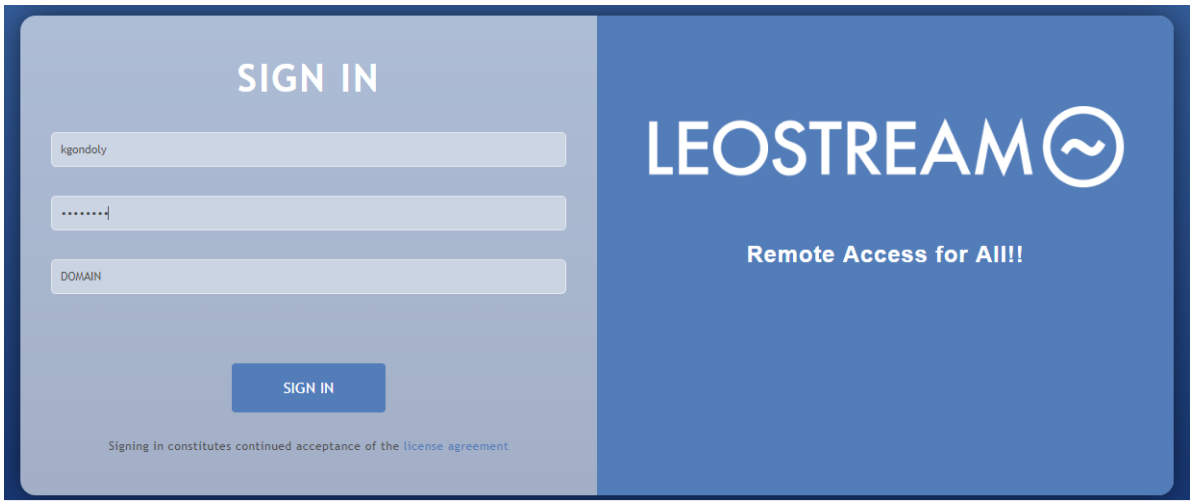


End-User Login Workflow

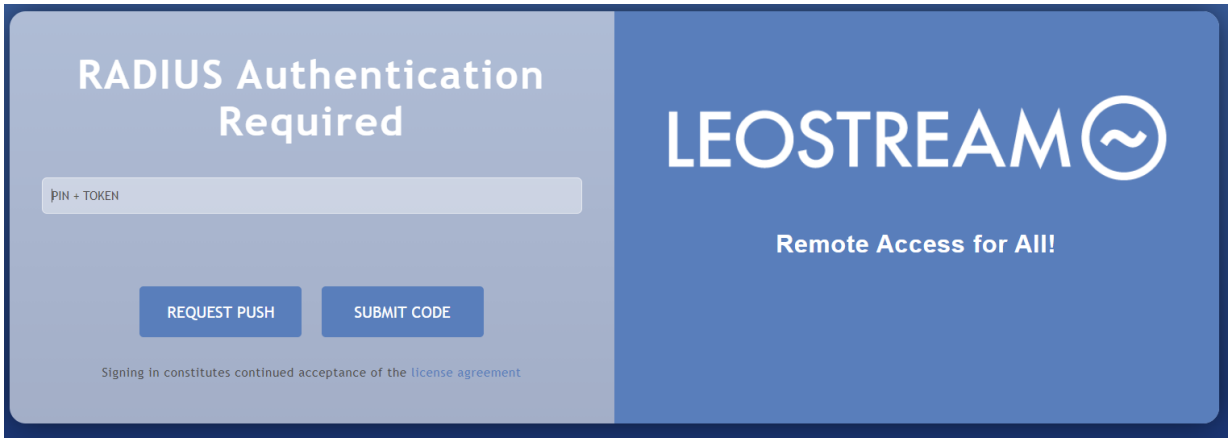
Example Using the Leostream Web Client

When logging in using the Leostream Web client, users whose logins are protected by 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 locates the user in your authentication server, for example Active Directory. If Leostream locates the user in your authentication server and determines that MFA is required, Leostream prompts the user for MFA, for example:



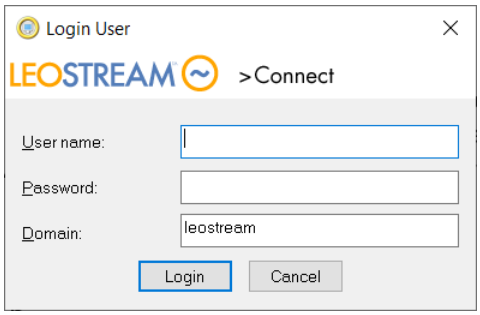
Only after the user successfully passes the MFA step will Leostream display the user's offered desktops.

Example Using Leostream Connect

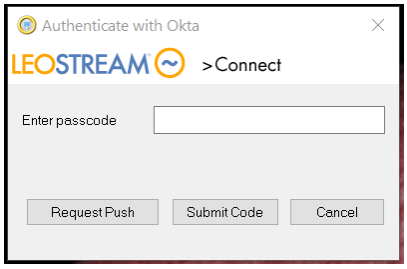
All versions of Leostream Connect support RADIUS MFA. However, older versions require users enter their username, password, and PIN/ TOTP in a single dialog and do not support Push notifications. Versions of Leostream Connect that are available with Connection Broker 9.0.40 and later support two-step authentication with Push notifications. These versions are:

- Leostream Connect for Microsoft Windows operating systems: 4.3
- Leostream Connect for Linux and macOS: 3.7

When logging in using Leostream Connect, users are first prompted for their username and password, as shows for Windows operating systems in the following figure.



If the user requires MFA, they are then prompted to enter a PIN + Token, for example:

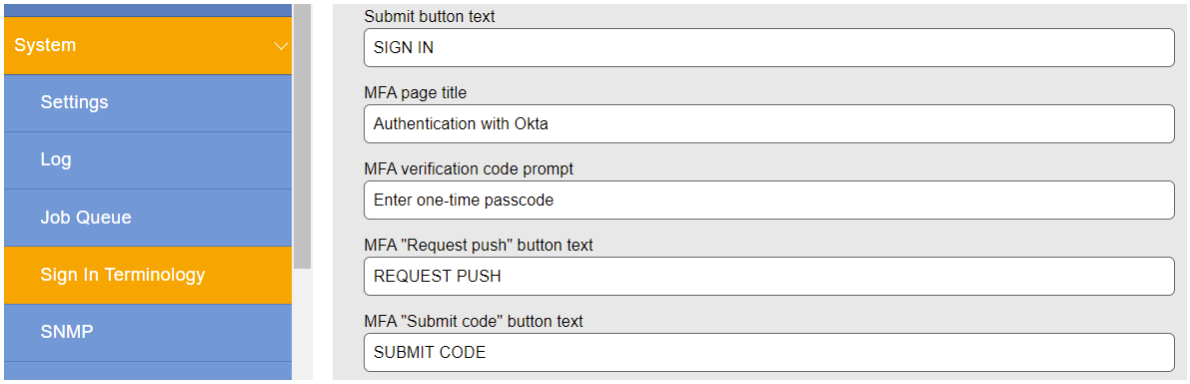


Customizing the Login Dialogs

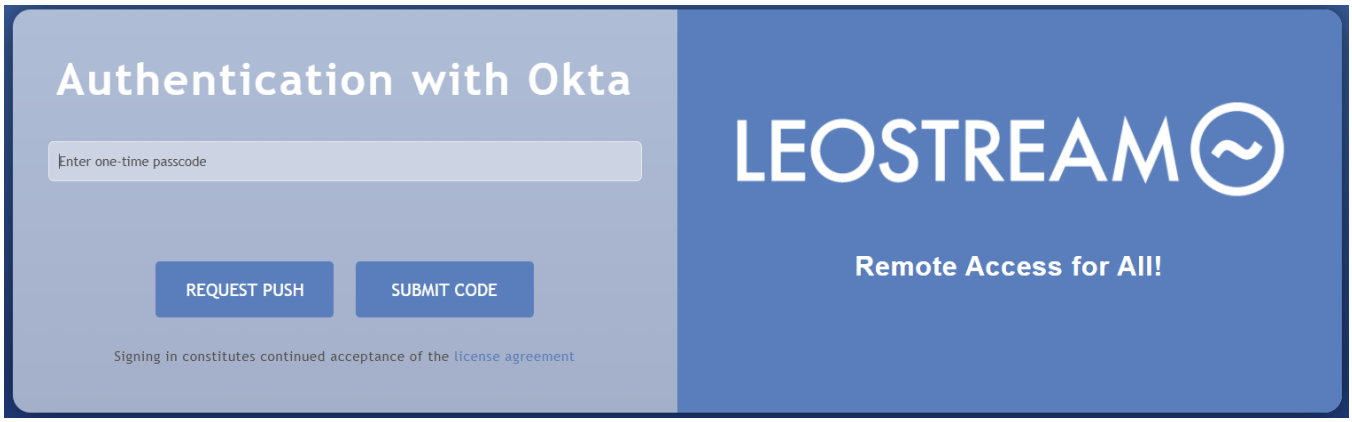
You can modify the title and prompt displayed to users that require MFA using the **Sign In Terminology** sets in your Connection Broker, as follows.

1. Go to the **> System > Sign In Terminology** page.
2. Click **Define Terminology** to start a new terminology set.
3. Enter a descriptive name in the **Name** edit field.
4. In the **Sign In Form Text Prompts** section, shown in the following figure, edit the following fields:
    a. **MFA page title:** Defines the title of the form
    b. **MFA verification code prompt:** Defines the text entered into the edit field
    c. **MFA "Request push" button text:** Defines the text on the button that requests the push notice from the RADIUS server
    d. **MFA "Submit code" button text:** Defines the text on the button that submits the OTP to the RADIUS server
5. Click **Save** to save the new terminology set.
6. Go to the **> System > Settings** page.
7. Select your new sign in terminology set from the **Sign in form terminology** drop-down menu in the **Web Browser Configuration** section.

For example, if the values entered in the following figure are set for the Sign In Terminology:



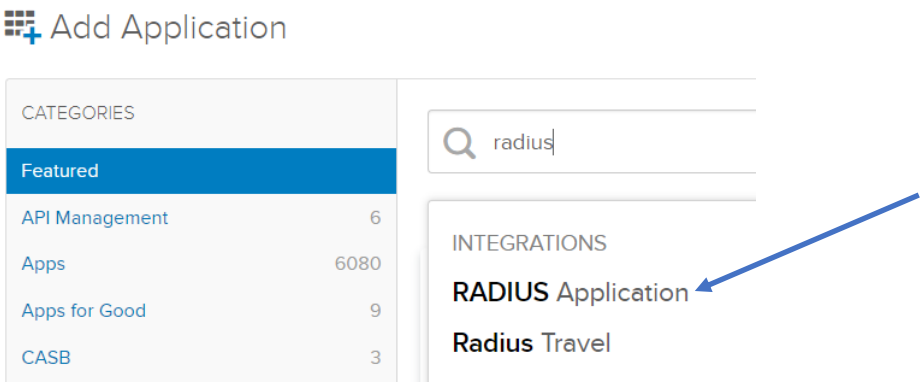
The following figure shows the example customization rendered in the Leostream Web client.



Example Configuration: Using Leostream with Okta

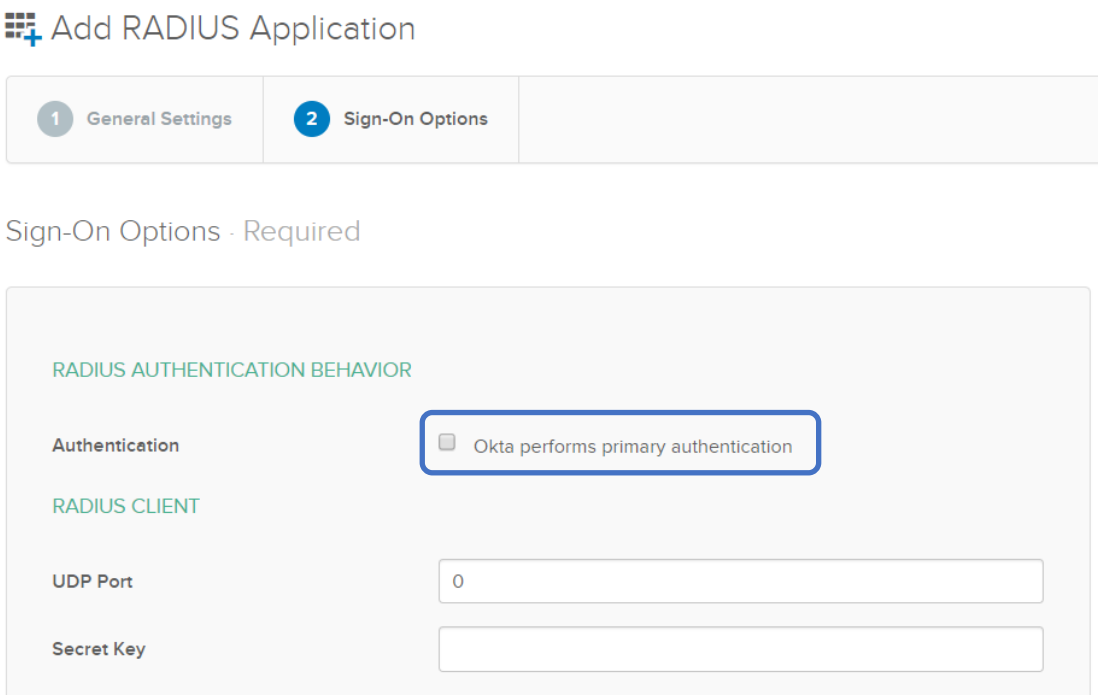
Leostream supports MFA using Okta when you deploy an Okta RADIUS Agent. For information on installing the Okta RADIUS Agent, please refer to the **Okta documentation**. When installing the Okta RADIUS Agent, if prompted for a shared secret, make note of the secret for use when configuring Okta and Leostream.

After you install the Okta RADIUS Agent, add a RADIUS Application in Okta for your Leostream Connection Broker, for example:



For a complete description of using Okta with RADIUS integrations and how to configure a RADIUS application in Okta, please consult the **Okta documentation**. When adding your RADIUS application in Okta, please ensure you configure the following settings appropriately.

1. Disable **Okta performs primary authentication**, as shown in the following figure.



2. In the RADIUS CLIENT section, shown in the previous figure, enter the port number and shared secret used for your Okta RADIUS Agent. If you did not specify a secret key when installing the Okta RADIUS Agent, enter a shared secret that you will use when configuring RADIUS integrations in Leostream.

   RADIUS is a UDP protocol. If your RADIUS Agent is behind a firewall, security group, or access control list, ensure that the RADIUS port is open for UDP traffic originating from your Connection Broker.

3. When setting the **Application username format**, ensure that the username format in Okta exactly matches the username format for your authentication server.

4. You must pre-enroll users and assign them to your Leostream application in Okta before the user can log into Leostream. Self-enrollment is not currently supported.