
EDGE NEXUS



Integration with DUO Authentication Proxy to provide 2 factor Authentication

Version: 1.2
Date : 26/11/2020
Status: Draft

Index

Index	2
Overview	3
Scope	3
Introduction	3
Authentication flow	4
Prerequisites	4
Duo application and user configuration	5
Duo Authentication Proxy application installation and configuration	10
LDAP authentication proxy configuration	12
Edgenexus ADC authentication configuration with Duo LDAP	16
RADIUS authentication proxy configuration	20
Edgenexus ADC authentication configuration with Duo RADIUS	23
Duo directory synchronization	27
More information	28

Overview

When running the embedded Duo authentication proxy app, Edgenexus can provide an integrated application security and authentication platform.

Once deployed, applications and resources can be selected in a granular manner for Duo 2 factor authentication. This can be easily integrated with existing user authentication systems such as LDAP or RADIUS etc.

Rather than having to lock down all pages for all users, the ADC can choose what page should be secure and how, based on many criteria ranging from the URL, Geo location, IP or even query: in fact anything in the Request can be used.

Scope

The document aims to describe how to set up and deploy Edgenexus ADC with Duo using either Radius or LDAP.

Introduction

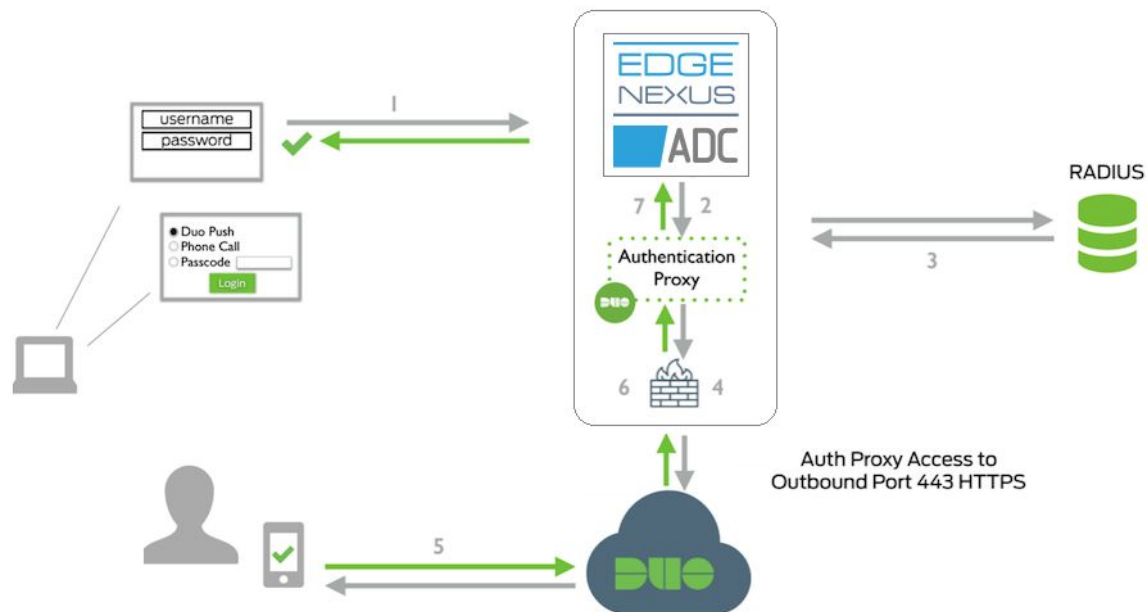
The Edgenexus ADC platform is a fully featured ADC and load balancer. In addition to providing load balancing, Proxy and SSL services, it can also provide security services by challenging users for credentials in order to allow them access to resources.

The Edgenexus ADC also has an integrated microservices container platform. This allows applications to interface with the ADC and external services such as Duo.

Duo is a 2 factor authentication platform by Cisco that also includes a proxy application that can integrate with Active Directory, OpenLDAP, RADIUS and others.

Authentication flow

The Authentication flow can be described in the following way.



1. The user initiates a request to a website protected by the Edgenexus ADC.
2. The ADC, being in the middle of communication, intercepts the user request and displays a pre-authentication page, prompting for a username and password.
3. The ADC sends an authentication request to Duo Authentication Proxy running within the ADC platform.
4. The Duo Authentication Proxy completes primary authentication using the LDAP or RADIUS server.
5. The Authentication Proxy establishes a secure connection to the Duo Security service.
6. Secondary authentication is conducted through the Duo Security service.
7. The Authentication Proxy receives a secondary authentication result from the Duo Security service.
8. Edgenexus ADC grants the user access.

Prerequisites

Before you begin you should have a working Edgenexus ADC, LDAP or RADIUS server for primary authentication and a [Duo account](#). Please ensure that the system time is in sync on all of the above servers by either enabling NTP or manual setting.

Duo application and user configuration

1. First we are going to create a LDAP or RADIUS application and a test user in Duo. Log in to the [Duo Admin Panel](#) and navigate to the **Applications** page.

[Dashboard](#) > Applications

Applications

Protect an Application

Manage your update to the new
Universal Prompt experience, all in
one place.

Get Started

Get More Information [↗](#)

Export [▼](#)

[🔍](#) Search

2. Click the **Protect an Application** button and locate LDAP or RADIUS in the applications list, depending on what protocol is supported by your user authentication system.

Protect an Application

Add an application that you'd like to protect with Duo two-factor authentication.

You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#) [↗](#)

Choose an application below to get started.

ldap

Application

Protection Type



LDAP Proxy

2FA

[Documentation](#) [↗](#)

Protect

3. Click the **Protect** button to get your integration key, secret key, and API hostname. You will need this information later for configuring the Duo Authentication Proxy.

[Dashboard](#) > [Applications](#) > LDAP Proxy

LDAP Proxy

[Authentication Log](#) | [Remove Application](#)

See the [LDAP proxy documentation](#) to integrate Duo into your LDAP-enabled platform.

Details [Reset Secret Key](#)

Integration key	<input type="text" value="DIRCQJJIJHNCN9XWP78E"/> select
Secret key	<input type="text" value="Click to view."/> select
Don't write down your secret key or share it with anyone.	
API hostname	<input type="text" value="api-1db74fb0.duosecurity.com"/> select

4. Scroll the page down to the **Settings** section and enable **Username normalization** by selecting the **Simple** option.

Username normalization

☐ None
☒ Simple

"DOMAIN\username", "username@example.com", and "username" are treated as the same user.

Controls if a username should be altered before trying to match them with a Duo user account.

5. Navigate to the **Users** page of the Duo Admin Panel and click the **Add User** button to create a test user which we will use to check the Duo two factor authentication with Edgenexus ADC.

[Dashboard](#) > [Users](#)

Users

[Directory Sync](#) | [Import Users](#) | [Bulk Enroll Users](#)[Add User](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#) .

3

Total Users

0

Not Enrolled

1

Inactive Users

0

Trash

0

Bypass Users


0

Locked Out

Select (0) ▾

...

Export ▾

 Search

Username ▲

Name

Email

Phones

Tokens

Status

Last Login

6. Fill in the user details and click the **Save Changes** button.

[Dashboard](#) > [Users](#) > testuser

testuser

[Logs](#) | [Send Enrollment Email](#) |  [Send to Trash](#)

This user has not enrolled yet. See our [enrollment documentation](#)  to learn more about enrolling users.

Username

testuser

Username aliases

[+ Add a username alias](#)

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

Email

7. Prior to adding a phone number to the Duo user, please install the **Duo Mobile** app on your iPhone or Android device from the app store, as it will be needed to confirm the phone number with Duo.

8. Next click the **Add Phone** button in the Duo Admin Panel.

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#).

[Add Phone](#)

This user has no phones. [Add one.](#)

9. Enter your phone number and click the **Add Phone** button.

Add Phone

[Learn more about Activating Duo Mobile](#).

Type

☒ Phone
☐ Tablet

Phone number

 +44 7400 123456

[Show extension field](#)

Optional. Example: "+44 7400 123456"

[Add Phone](#)

10. In the **Device Info** section click the **Activate Duo Mobile** link.

[Dashboard](#) > [Phones](#) > Phone: +44 7400 123456

+44 7400 123456

[Send SMS Passcodes...](#) | [Delete Phone](#)



testuser

+44 7400 123456

[Attach a user](#)

Authentication devices
can share multiple
users

Device Info

[Learn more about Activating Duo Mobile](#).



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone

Settings

Number

 +44 7400 123456

[Show extension settings](#)

Optional. Example: "+44 7400 123456"

11. On the Activate Duo Mobile page click the **Generate Duo Mobile Activation Code** button.

[Dashboard](#) > [Phone: +44 7400 123456](#) > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone +44 7400 123456

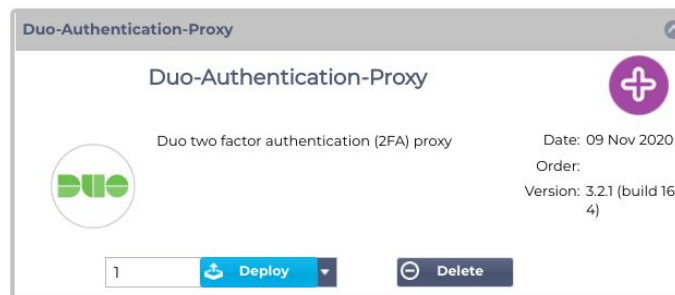
Expiration

[Generate Duo Mobile Activation Code](#)

12. Then click the **Send Instructions by SMS** button. You should shortly get a text message with an activation link on the phone you added to the Duo user. Follow the link, and the Duo test user account should be added to the Duo Mobile App on your phone. Should you get the activation link expired message, simply repeat the last two steps.

Duo Authentication Proxy application installation and configuration

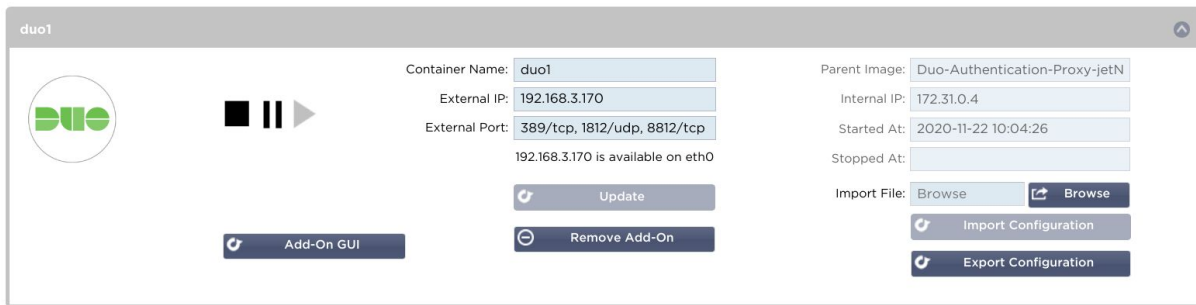
1. Now we are going to install and configure the Duo Authentication Proxy on the Edgenexus ADC. Download Duo Authentication Proxy App from the Edgenexus App Store.
2. Deploy Duo Authentication Proxy App in the **Library -> Apps** page of Edgenexus ADC.



3. Navigate to the **Library -> Add-Ons** page of Edgenexus ADC. Fill in the **Add-On Name**, **External IP** and **External Ports** parameters of the Duo Authentication Proxy Add-On, then click the **Play** button to start the Add-On. Port 389/tcp is used by the LDAP proxy server, port 1812/udp is used by the RADIUS proxy server, port 8812/tcp is used by the Duo Authentication Proxy Add-On GUI.



4. After the Add-On has started, click the **Add-On GUI** button.



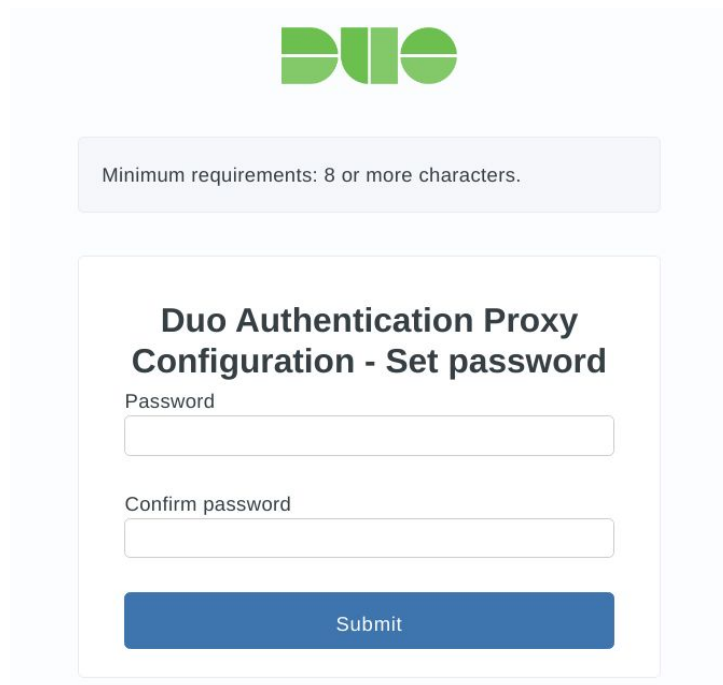
The screenshot shows the Duo Authentication Proxy GUI for a container named 'duo1'. It displays various configuration fields and control buttons.

Field	Value
Container Name	duo1
External IP	192.168.3.170
External Port	389/tcp, 1812/udp, 8812/tcp
Parent Image	Duo-Authentication-Proxy-jetN
Internal IP	172.31.0.4
Started At	2020-11-22 10:04:26
Stopped At	

Additional information: 192.168.3.170 is available on eth0

Buttons: Add-On GUI, Update, Remove Add-On, Import File (Browse), Import Configuration, Export Configuration

5. When you visit the Duo Authentication Proxy GUI for the first time, you are asked to set the administrator's password that you will use to access the App. Please specify a strong password which is at least 8 characters long. After having entered a password and a password confirmation please click the **Submit** button. The Duo Authentication Proxy configuration page will be loaded automatically.



The screenshot shows the 'Duo Authentication Proxy Configuration - Set password' page. It includes a password input field, a confirm password input field, and a submit button.

Minimum requirements: 8 or more characters.

Duo Authentication Proxy Configuration - Set password

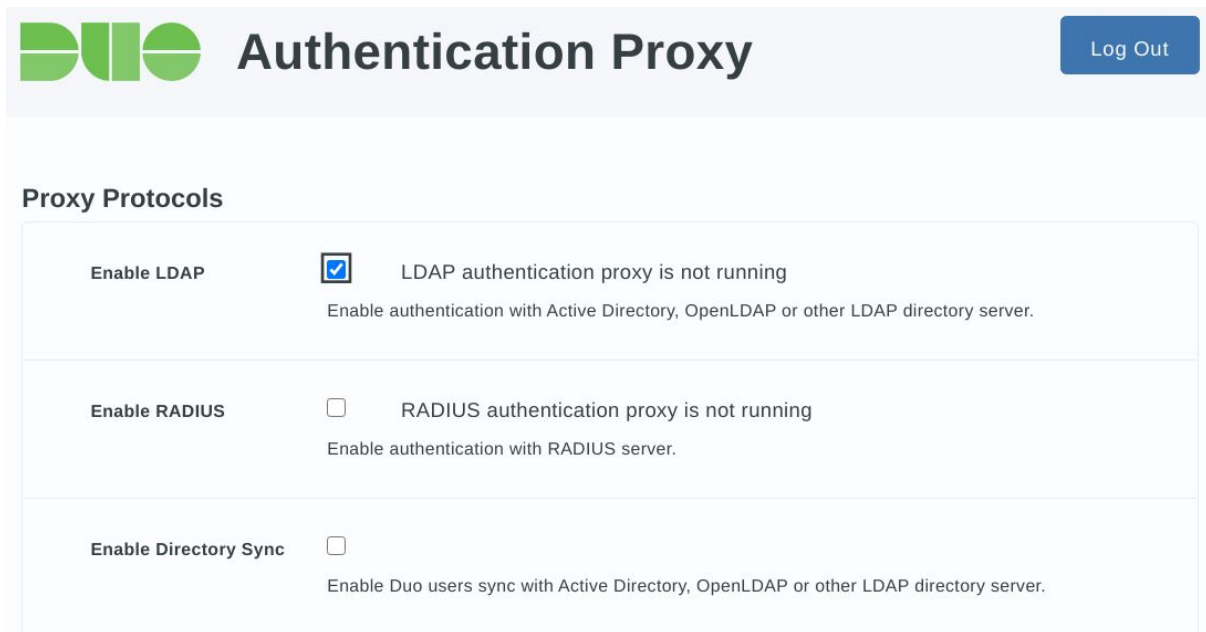
Password

Confirm password

Submit

LDAP authentication proxy configuration

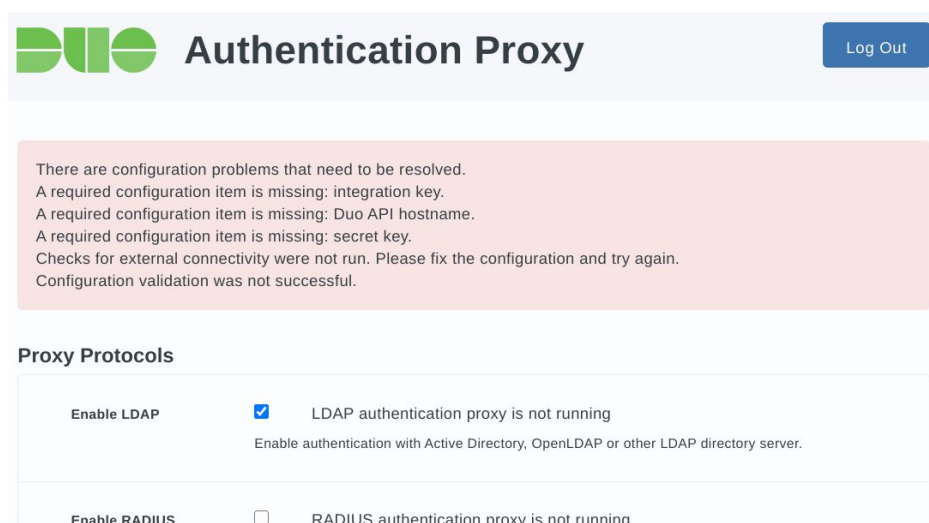
1. Let's see how to configure the LDAP authentication proxy, which can use your existing Active Directory, OpenLDAP or other LDAP server as a source of primary authentication. In the **Proxy Protocols** section tick the **Enable LDAP** checkbox and click the **Save Settings** button.



The screenshot shows the Duo Authentication Proxy configuration interface. At the top, there is a header with the Duo logo and the text "Authentication Proxy", and a "Log Out" button. Below the header, the "Proxy Protocols" section is visible. It contains three rows of configuration options:

Option	Checkbox	Status	Description
Enable LDAP	<input checked="" type="checkbox"/>	LDAP authentication proxy is not running	Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.
Enable RADIUS	<input type="checkbox"/>	RADIUS authentication proxy is not running	Enable authentication with RADIUS server.
Enable Directory Sync	<input type="checkbox"/>		Enable Duo users sync with Active Directory, OpenLDAP or other LDAP directory server.

Every change in the Duo Authentication proxy settings triggers a configuration check. As long as LDAP configuration is incomplete, the application GUI will show a list of errors as shown in the next figure. Don't worry, this is normal, you will see the list of errors shrinking with more configuration detail supplied.



The screenshot shows the Duo Authentication Proxy configuration interface with a red error message box at the top. The error message reads:

There are configuration problems that need to be resolved.
A required configuration item is missing: integration key.
A required configuration item is missing: Duo API hostname.
A required configuration item is missing: secret key.
Checks for external connectivity were not run. Please fix the configuration and try again.
Configuration validation was not successful.

Below the error message, the "Proxy Protocols" section is visible, showing the same configuration options as the previous screenshot:

Option	Checkbox	Status	Description
Enable LDAP	<input checked="" type="checkbox"/>	LDAP authentication proxy is not running	Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.
Enable RADIUS	<input type="checkbox"/>	RADIUS authentication proxy is not running	

2. In the **Primary LDAP Server** section fill in the server hostname or IP address and port. Typically the port number is 389 for cleartext LDAP and STARTTLS and 636 for LDAPS.

Primary LDAP Server

Server	<input type="text" value="ad-server.example.org"/>	<input type="text" value="Port"/>
Hostname and port of your directory server. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS.		
Transport type	<input type="radio"/> CLEAR <input type="radio"/> LDAPS <input checked="" type="radio"/> STARTTLS	
This setting controls whether communication between the directory server and the Duo Authentication Proxy is encrypted.		
SSL certificate	<input type="button" value="Выберите файл"/> <input type="text" value="ad-server.example.org.pem"/>	
Upload PEM-formatted full chain SSL certificate for the directory server. All certificates needed to validate the directory server's certificate must be present here. The hostname domain suffix specified above MUST match the common name for the certificate.		
Verify hostname	<input checked="" type="checkbox"/>	
With LDAPS and STARTTLS transport types the common name in the server certificate is matched against the value of the server hostname parameter specified above. If your LDAP server uses a certificate with a mismatched common name, or you specified the host as an IP address, disable this option.		

Please upload an SSL certificate of your LDAP server if it is using STARTTLS or LDAPS encrypted network communication. The certificate must be in PEM format and must contain the full chain of certification, including the CA and all intermediate certificates if there are any. Please see [this article](#) on how to export the certificate chain from Active Directory.

If you specified the LDAP server by its IP address, or the hostname of the LDAP server does not match the common name in the SSL certificate, you have to untick the **Verify hostname** checkbox. However, this will somewhat reduce the security guarantees otherwise provided by the use of TLS/SSL. Disabling hostname verification may also be required when **Transport type** is set to **CLEAR**.

3. We recommend creating a dedicated account with read-only access to the LDAP server which will be used by the Duo authentication proxy for searching the users directory. Please specify the search username, password and the base DN of your directory server in the respective input fields.

Search username	<input type="text" value="duobinduser@example.com"/>
The username of an account that has permission to read from your directory server. We recommend creating a service account that has read-only access.	
Search password	<input type="password" value="*****"/>
The password corresponding to the search username specified above.	
Search base DN	<input type="text" value="DC=example,DC=com"/>
The DN which will be used as a base for the search.	

4. Set the **Authentication type** parameter to **Plain LDAP** - this is the authentication type compatible with Edgenexus ADC. If for some reason this is not working for you, try selecting other authentication types.

Authentication type

☐ Microsoft NTLM, version 2

☐ Microsoft NTLM, version 1

☒ **Plain LDAP authentication**

NTLMv1 and Plain options should not be used without enabling transport level encryption. In addition Plain authentication requires that you specify a Bind DN.

Bind DN

The full LDAP distinguished name of an account permitted to read from the directory. Typically, this would be the distinguished name of the user specified in Search username parameter above.

Username attributes

Specify attributes the username should match against.
For example: sAMAccountName,mail.
Typical for Active Directory: sAMAccountName.
Typical for OpenLDAP: uid.

[Save Settings](#)

Please also specify the **Bind DN** parameter when authentication type is set to **Plain LDAP**. Bind DN is the full LDAP distinguished name of the account permitted to read from the directory. Typically, this is the distinguished name of the account you have specified in the **Search username** parameter above.

You may specify the **Username attribute** parameter if your LDAP server's username attribute name is different from the commonly used sAMAccountName and uid username attribute names.

Click the **Save Settings** button after having specified the LDAP server parameters. You will see an error message again as some configuration parameters are still missing.

5. The **Failmode** setting controls whether access should be allowed or denied shall the Duo cloud become unavailable.

LDAP Proxy Server

Failmode

☒ **Secure**
Deny access

☐ **Safe**
Allow access

This setting controls what happens if the Duo cloud service is unavailable.

[Save Settings](#)

6. Enter your Duo LDAP application connection details in the **Duo LDAP Application Details** section. You may find them in the **Applications** page of the Duo Admin Panel.

Duo LDAP Application Details

Create a Duo LDAP application in the Duo Admin Panel and enter its details here.

Integration key	<input type="text" value="DIRCQJJJHNCN9XWP78E"/>
Secret key	<input type="text" value="*****"/>
Duo API hostname	<input type="text" value="api-1db74fb0.duosecurity.com"/>

When you click the **Save Settings** button, you should see a message saying that settings were successfully updated. If you get an error message instead, please review your configuration.

Edgenexus ADC authentication configuration with Duo LDAP

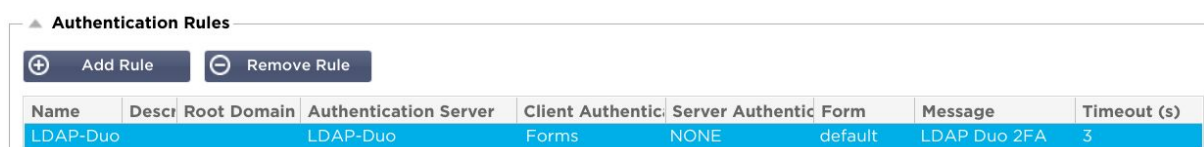
1. Once the Duo LDAP authentication proxy is configured, let's configure the Edgenexus ADC to use Duo for two factor authentication. Open Edgenexus ADC GUI in a web browser and navigate to the **Library -> Authentication** tab.

2. Add an authentication server as shown in the next figure. Give it a name you like, we'll call it LDAP-Duo in this example. In the **Authentication Method** column please select **LDAP**. In the **Domain** column please specify the name of your domain, eg., example.com. In the **Server Address** column please supply the name of the Duo Authentication proxy Add-On you have deployed at one of the previous steps. Set port number to 389 in the **Port** column. Enter the search base DN in the **Search Base** column. Select **Username and Domain** in the **Login Format** column.



Name	Descr	Authentication	Domain	Server	Port	Search	Search Base	Login Format	Passph	Dead Time
LDAP-Duo		LDAP	example.com	duo1	389		dc=example.dc=com	Username and Domain		

3. Then add an authentication rule as shown in the next figure. In the **Authentication Server** drop-down list select the value matching the **Name** of the authentication server you added at the previous step.



Name	Descr	Root Domain	Authentication Server	Client Authentic	Server Authentic	Form	Message	Timeout (s)
LDAP-Duo			LDAP-Duo	Forms	NONE	default	LDAP Duo 2FA	3

4. Navigate to the **Library -> flightPATH** tab of the Edgenexus ADC GUI and create an authentication flightPATH as shown in the next figure. In the **Target** drop-down list of the **Action** table select the value matching the **Name** of the authentication rule you defined at the previous step.

The screenshot shows the 'flightPATH' configuration page. It has a 'Details' section with a table containing one entry: 'LDAP-Duo' with 'Applied To VS' set to 'Not in use'. Below this are sections for 'Condition' and 'Evaluation'. The 'Action' section contains a table with one entry: 'Authentication' with 'Target' set to 'LDAP-Duo'.

flightPATH Name	Applied To VS	Description
LDAP-Duo	Not in use	

Action	Target	Data
Authentication	LDAP-Duo	

In this example there are no conditions, meaning that the rule will fire all the time. If you do not wish this you can add some conditions. For example you could configure it to only challenge users that want to access a certain path e.g. “/secure” or only if they are not from a certain source IP. For more details on flightPATH please refer to the Edgenexus ADC user guide.

5. Navigate to the **Services -> IP-Services** tab of the Edgenexus ADC GUI and create a virtual service. In the **IP Address**, **Subnet Mask** and **Port** columns of the **Virtual Services** table set the networking details describing how clients will be connecting to the virtual service. Set the **Service Type** to HTTP.

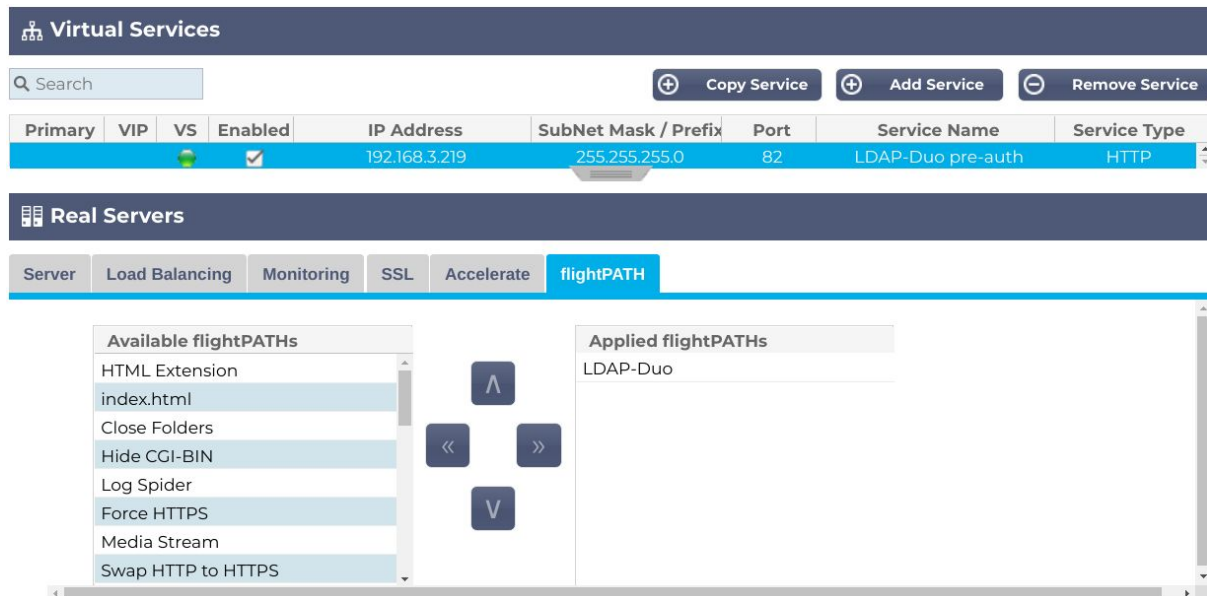
The screenshot shows the 'Virtual Services' and 'Real Servers' configuration pages. The 'Virtual Services' table has one entry: 'LDAP-Duo pre-auth' with IP Address '192.168.3.219', SubNet Mask / Prefix '255.255.255.0', Port '82', and Service Type 'HTTP'. The 'Real Servers' section shows a table with one entry: '192.168.3.250' with Port '8001' and Weight '100'.

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
			<input checked="" type="checkbox"/>	192.168.3.219	255.255.255.0	82	LDAP-Duo pre-auth	HTTP

Status	Activity	Address	Port	Weight	Calculated Weig	Notes	ID
	Online	192.168.3.250	8001	100	100		

In the **Server** tab under the **Real Servers** section set the **Address** and **Port** of the real server you are protecting with the two factor authentication.

6. Next open the **flightPATH** tab in the **Real Servers** section and apply the authentication flightPATH you have recently created.



The screenshot shows the EdgeNexus management console. At the top, there's a 'Virtual Services' section with a table listing services. Below it, the 'Real Servers' section is active, with the 'flightPATH' tab selected. The 'flightPATH' configuration page shows a list of 'Available flightPATHs' on the left, including 'HTML Extension', 'index.html', 'Close Folders', 'Hide CGI-BIN', 'Log Spider', 'Force HTTPS', 'Media Stream', and 'Swap HTTP to HTTPS'. In the center, there are navigation buttons: a left arrow, a right arrow, and a 'V' button. On the right, the 'Applied flightPATHs' section shows 'LDAP-Duo' is applied.

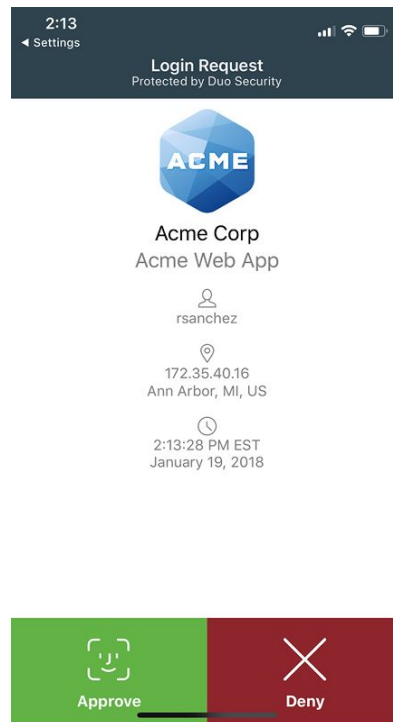
7. The configuration is done - let's check how it works. Open a new tab in the web browser and type the address of the virtual service protected with the two factor authentication. In our example it is "http://192.168.3.219:82", most likely that yours is different. After hitting **Enter** you should see a page similar to the one below.



The screenshot shows a login page titled 'LDAP Duo 2FA'. It features a username input field with a user icon, a password input field with a key icon, and a green 'Login' button with a right arrow icon. Below the login button, it says 'Secured by edgeADC'.

8. Enter the username and password of the test user you created in your LDAP server and in the Duo Admin Panel.

9. If the username and password pass validation on your LDAP server, you should soon get a confirmation request in the Duo Mobile App on the phone associated with the Duo test user.

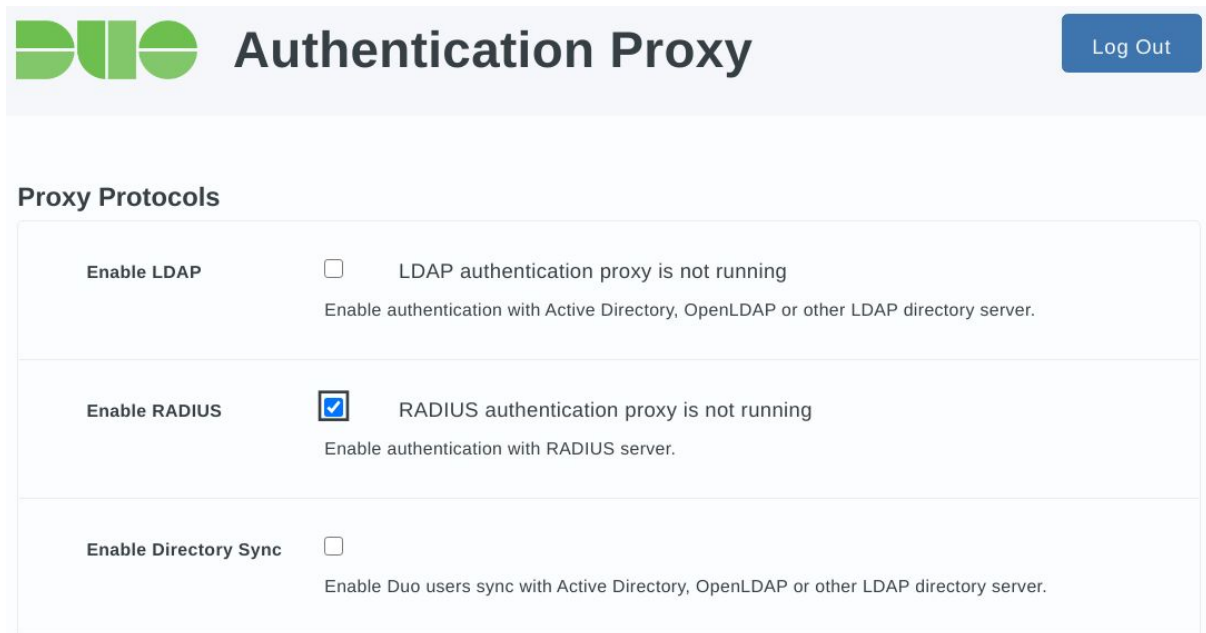


If you approve access in Duo Mobile, you should see a page served by the real server in your web browser. If you choose to deny access, the pre-authentication login page should appear again in your web browser with an error message saying that username or password is incorrect.

See the [Duo Mobile on iPhone](#) and the [Duo Mobile on Android](#) articles for more information on the Duo Mobile App. See the [Enroll Users](#) article for the information on how to add users to the Duo system.

RADIUS authentication proxy configuration

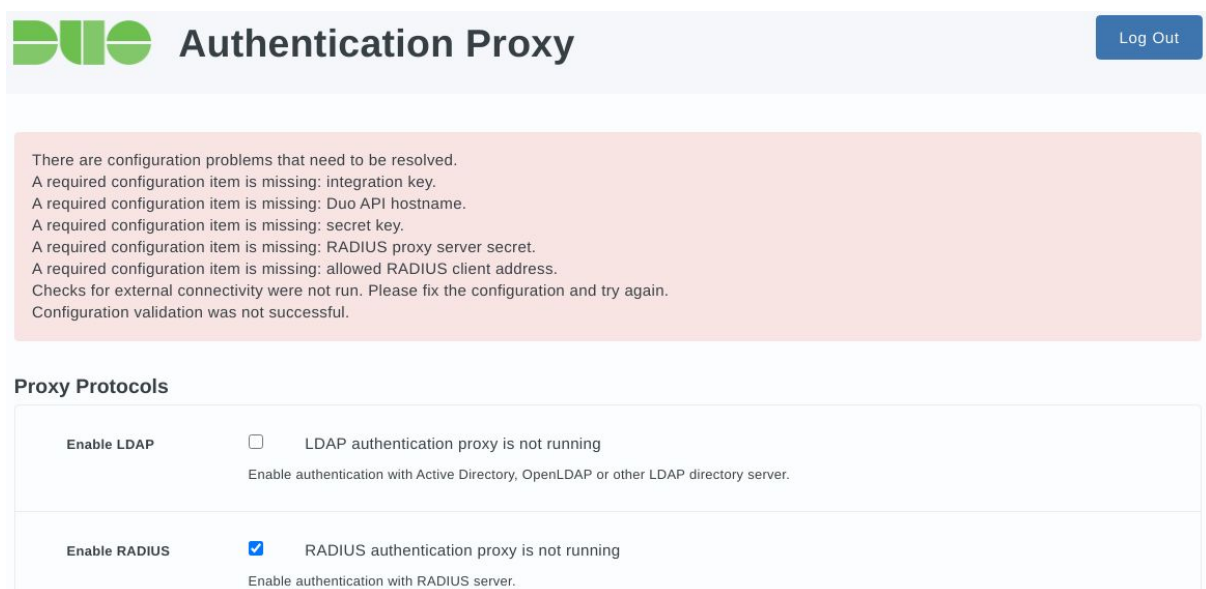
1. Let's see how to configure the RADIUS authentication proxy, which can use your existing RADIUS server as a source of primary authentication. In the **Proxy Protocols** section tick the **Enable RADIUS** checkbox and click the **Save Settings** button.



The screenshot shows the Duo Authentication Proxy configuration interface. At the top, there is a header with the Duo logo and the text "Authentication Proxy", and a "Log Out" button. Below the header is the "Proxy Protocols" section, which contains three rows of configuration options:

Option	Checkbox	Status	Description
Enable LDAP	<input type="checkbox"/>	LDAP authentication proxy is not running	Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.
Enable RADIUS	<input checked="" type="checkbox"/>	RADIUS authentication proxy is not running	Enable authentication with RADIUS server.
Enable Directory Sync	<input type="checkbox"/>		Enable Duo users sync with Active Directory, OpenLDAP or other LDAP directory server.

Every change in the Duo Authentication proxy settings triggers a configuration check. As long as RADIUS configuration is incomplete, the application GUI will show a list of errors as shown in the next figure. Don't worry, this is normal, you will see the list of errors shrinking with more configuration detail supplied.



The screenshot shows the Duo Authentication Proxy configuration interface with error messages displayed. At the top, there is a header with the Duo logo and the text "Authentication Proxy", and a "Log Out" button. Below the header is a red box containing the following error messages:

There are configuration problems that need to be resolved.
A required configuration item is missing: integration key.
A required configuration item is missing: Duo API hostname.
A required configuration item is missing: secret key.
A required configuration item is missing: RADIUS proxy server secret.
A required configuration item is missing: allowed RADIUS client address.
Checks for external connectivity were not run. Please fix the configuration and try again.
Configuration validation was not successful.

Below the error messages is the "Proxy Protocols" section, which contains two rows of configuration options:

Option	Checkbox	Status	Description
Enable LDAP	<input type="checkbox"/>	LDAP authentication proxy is not running	Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.
Enable RADIUS	<input checked="" type="checkbox"/>	RADIUS authentication proxy is not running	Enable authentication with RADIUS server.

2. In the **Primary RADIUS Server** section of the Duo Authentication Proxy GUI you have to specify the connection details of your RADIUS server: the hostname or IP address, the port number and the secret. Click the **Save Settings** button after you enter the RADIUS server parameters.

Primary RADIUS Server

Server	<input type="text" value="Hostname or IP address"/>	<input type="text" value="Port"/>
Hostname and port of your RADIUS server. The port is typically 1812.		
Secret	<input type="text"/>	
The shared secret of your RADIUS server.		
<input type="button" value="Save Settings"/>		

As soon as you click the **Save Settings** button, you will see an error message again as some configuration parameters are still missing.

3. The **RADIUS Proxy Server** section of the Duo Authentication proxy GUI defines how RADIUS clients access the authentication proxy and what should be done if the Duo cloud service is unavailable.

RADIUS Proxy Server

Allowed RADIUS Clients	<input type="text" value="172.31.42.1"/>
IP address or IP address range for RADIUS clients. Only clients with configured addresses and shared secrets will be allowed to send requests to the Authentication Proxy. This can be a single IP address, a specification in CIDR notation (e.g. 1.2.3.0/24), or an IP address range (e.g. 3.3.3.3 - 3.3.3.6). To allow access to the Authentication Proxy only from Edgenexus ADC set this to 172.31.42.1.	
Secret	<input type="text"/>
The shared secret of Duo RADIUS proxy server.	
Failmode	<input checked="" type="radio"/> Secure Deny access <input type="radio"/> Safe Allow access This setting controls what happens if the Duo cloud service is unavailable.
<input type="button" value="Save Settings"/>	

In the **Allowed RADIUS Clients** input field please specify an IP address or a range of IP addresses of RADIUS clients which are allowed to connect to your Duo Authentication proxy App. In the simplest case you would like to allow access to the RADIUS proxy only for

the Edgenexus ADC. Communications between the ADC and the add-ons are held over a virtual Docker network. The ADC IP address on the Docker network is displayed as a hint in the **Allowed RADIUS Clients** input field when there is no user input. Please enter this IP address.

In the **Secret** input field please enter a password which RADIUS clients must use when connecting to the Duo Authentication proxy. We will supply this RADIUS secret later when we will be configuring RADIUS authentication in the Edgenexus ADC.

The **Failmode** setting controls whether access should be allowed or denied shall the Duo cloud become unavailable.

After configuring all settings in this section please click the **Save Settings** button. You will see an error message again as some configuration parameters are still missing.

4. Enter your Duo RADIUS application connection details in the **Duo RADIUS Application Details** section. You may find them in the **Applications** page of the Duo Admin Panel.

Duo RADIUS Application Details

Create a Duo RADIUS application in the Duo Admin Panel and enter its details here.

Integration key	DI4WMDG3TDQWM3YGRKFZ
Secret key	*****
Duo API hostname	api-1db74fb0.duosecurity.com

Save Settings

When you click the **Save Settings** button, you should see a message saying that settings were successfully updated. If you get an error message instead, please review your configuration.

Edgenexus ADC authentication configuration with Duo RADIUS

10. Once the Duo RADIUS authentication proxy is configured, let's configure the Edgenexus ADC to use Duo for two factor authentication. Open Edgenexus ADC GUI in a web browser and navigate to the **Library -> Authentication** tab.

11. Add an authentication server as shown in the next figure. Give it a name you like, we'll call it RADIUS-Duo in this example. In the **Server Address** column please supply the name of the Duo Authentication proxy Add-On you have deployed at one of the previous steps. Set port number to 1812 in the **Port** column. Enter the RADIUS secret of the Duo RADIUS proxy server in the **Password** input field below the **Authentication Servers** table.

The screenshot shows the 'Authentication' tab in the Edgenexus ADC GUI. Under the 'Authentication Servers' section, there is a table with one entry: 'RADIUS-Duo' with domain 'edgenexus', login format 'Username Only', authentication type 'RADIUS', server address 'duo1', and port '1812'. Below the table are input fields for 'Description', 'Search Base', 'Search Condition', 'Search Account', and 'Password'. The 'Password' field is masked with dots. An 'Update' button is at the bottom.

Name	Domain	Login Format	Authentication	Server Address	Port
RADIUS-Duo	edgenexus	Username Only	RADIUS	duo1	1812

Description:

Search Base:

Search Condition:

Search Account:

Password:

12. Then add an authentication rule as shown in the next figure. In the **Authentication Server** drop-down list select the value matching the **Name** of the authentication server you added at the previous step.

The screenshot shows the 'Authentication Rules' section in the Edgenexus ADC GUI. There is a table with one entry: 'RADIUS-Duo' with description 'RADIUS-Duo', root domain 'RADIUS-Duo', client auth 'Forms', server auth 'NONE', form 'default', message 'RADIUS Duo 2FA', and timeout '60'. Below the table is an 'Add Rule' button.

Name	Description	Root Domain	Authentication Server	Client Auth	Server Auth	Form	Message	Timeout (s)
RADIUS-Duo	RADIUS-Duo	RADIUS-Duo	RADIUS-Duo	Forms	NONE	default	RADIUS Duo 2FA	60

13. Navigate to the **Library -> flightPATH** tab of the Edgenexus ADC GUI and create an authentication flightPATH as shown in the next figure. In the **Target** drop-down list

of the **Action** table select the value matching the **Name** of the authentication rule you defined at the previous step.

flightPATH

Details

Copy Rule Filter Keyword flightPATH Name Create jetPACK Add Rule Remove Ru...

flightPATH Name	Applied To VS	Description
RADIUS-Duo	Not in use	

Condition

Evaluation

Action

Add Action Remove Action Move Up Move Down

Action	Target	Data
Authentication	RADIUS-Duo	

In this example there are no conditions, meaning that the rule will fire all the time. If you do not wish this you can add some conditions. For example you could configure it to only challenge users that want to access a certain path e.g. “/secure” or only if they are not from a certain source IP. For more details on flightPATH please refer to the Edgenexus ADC user guide.

14. Navigate to the **Services -> IP-Services** tab of the Edgenexus ADC GUI and create a virtual service. In the **IP Address**, **Subnet Mask** and **Port** columns of the **Virtual Services** table set the networking details describing how clients will be connecting to the virtual service. Set the **Service Type** to HTTP.

Virtual Services

Search Copy Service Add Service Remove Service

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
			<input checked="" type="checkbox"/>	192.168.3.219	255.255.255.0	81	RADIUS-Duo pre-auth	HTTP

Real Servers

Server Load Balancing Monitoring SSL Accelerate flightPATH

Group Name: Server Group Copy Server Add Server Remove Server

Status	Activity	Address	Port	Weight	Calculated Weig	Notes	ID
	Online	192.168.3.250	8001	100	100		

In the **Server** tab under the **Real Servers** section set the **Address** and **Port** of the real server you are protecting with the two factor authentication.

15. Next open the **flightPATH** tab in the **Real Servers** section and apply the authentication flightPATH you have recently created.

Virtual Services

Search Copy Service Add Service Remove Service

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
			<input checked="" type="checkbox"/>	192.168.3.219	255.255.255.0	81	RADIUS-Duo pre-auth	HTTP

Real Servers

Server Load Balancing Monitoring SSL Accelerate **flightPATH**

Available flightPATHs

- HTML Extension
- index.html
- Close Folders
- Hide CGI-BIN
- Log Spider
- Force HTTPS
- Media Stream
- Swap HTTP to HTTPS

Applied flightPATHs

- RADIUS-Duo

16. The configuration is done - let's check how it works. Open a new tab in the web browser and type the address of the virtual service protected with the two factor authentication. In our example it is "http://192.168.3.219:81", most likely that yours is different. After hitting **Enter** you should see a page similar to the one below.

EDGE NEXUS

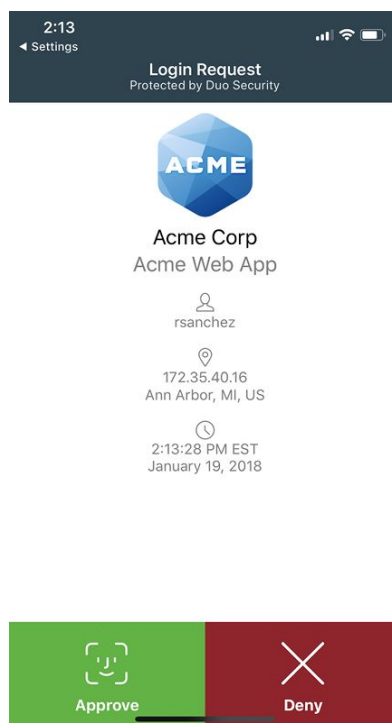
RADIUS Duo 2FA

Login

Secured by edgeADC

17. Enter the username and password of the test user you created in your RADIUS server and in the Duo Admin Panel.

18. If the username and password pass validation on your RADIUS server, you should soon get a confirmation request in the Duo Mobile App on the phone associated with the Duo test user.



If you approve access in Duo Mobile, you should see a page served by the real server in your web browser. If you choose to deny access, the pre-authentication login page should appear again in your web browser with an error message saying that username or password is incorrect.

See the [Duo Mobile on iPhone](#) and the [Duo Mobile on Android](#) articles for more information on the Duo Mobile App. See the [Enroll Users](#) article for the information on how to add users to the Duo system.

Duo directory synchronization

1. Please first read the Duo [Synchronizing Users from Active Directory](#) article to understand how the users synchronization works and how it can be configured.
2. Then start setting up the synchronization as per the above article until it comes to the Duo Authentication Proxy installation and configuration.
3. After completing the initial configuration in the Duo Admin Panel and obtaining your integration key, secret key and API hostname details for the Duo directory synchronization, please fill in these data in the **Duo Directory Sync** section of the Duo Authentication Proxy Add-On GUI and click the **Save Settings** button.

Duo Directory Sync

Enable Directory sync in the Duo Admin Panel and enter the details here.

Integration key	<input type="text" value="DIWQXRJFR1TPPRRAYJ30"/>
Secret key	<input type="password" value="....."/>
Duo API hostname	<input type="text" value="api-46e4474c.duosecurity.com"/>
Search username	<input type="text" value="duobinduser@example.com"/> <small>The username of an account that has permission to read from your directory server. We recommend creating a service account that has read-only access.</small>
Search password	<input type="password" value="....."/> <small>The password corresponding to the search username specified above.</small>
<input type="button" value="Save Settings"/>	

After saving the settings you should see a message saying that the settings were successfully updated.

4. Please continue the configuration process following the Duo article from the place where it describes how to test the connection.

More information

For more information or help please contact Edgenexus

hello@edgenexus.io or call us on:

0808 1645876 (866) 376-0175

Or refer to the Duo website

www.duo.com