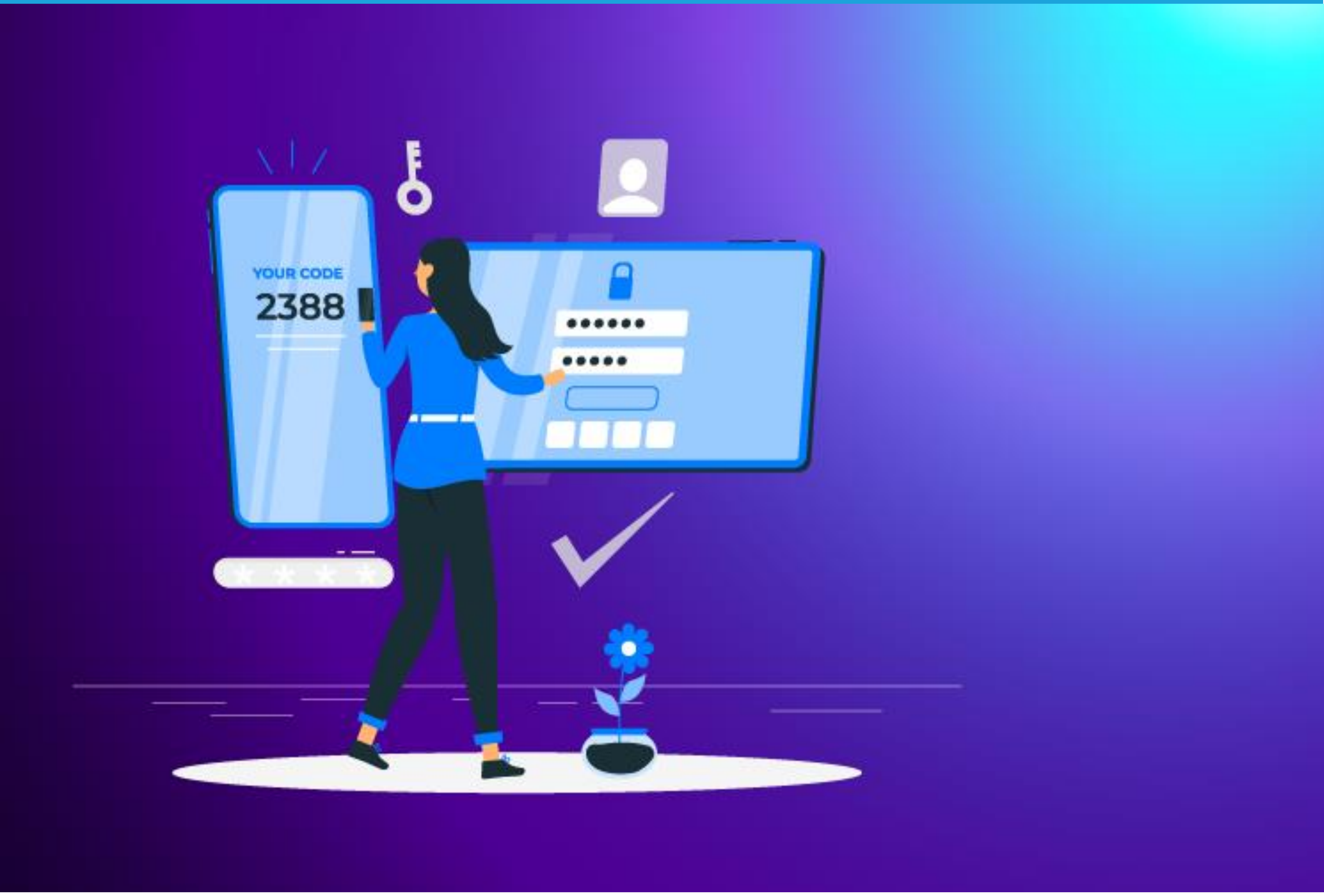


CISCO DUO 2FA PROXY

AN EDGENEXUS APP USER GUIDE

EDGE NEXUS

Contents

Document Properties

Document Number: 2.0.9.30.21.10.09

Document Creation Date: May 8, 2021

Document Last Edited: September 30, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: Cisco Duo - Version: General

Document Disclaimer

Screenshots and graphics in this manual may differ slightly from your product due to differences in your product release version. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

Trademarks

The Edgenexus logo, Edgenexus, EdgeADC, EdgWAF, EdgeGSLB, EdgeDNS are all trademarks or registered trademarks of Edgenexus Limited. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Introduction

The use of two-factor authentication, commonly referred to as 2FA has increased dramatically over the years. This rise in 2FA usage has mainly been due to the stealth capabilities of hackers improving and consequently affecting general and corporate users alike.

Cisco Duo is one of the leading 2FA solutions on the market and has increased its footprint within the enterprise space by leaps and bounds.

Unlike its competition, the Edgenexus ADC (EdgeADC) is the perfect vehicle for providing the corporate enterprise to introduce Cisco Duo authentication capabilities even before the user enters the corporate network.

The Cisco Duo authentication request engine resides within the EdgeADC's container technology and talks directly to the Cisco Duo servers to generate authentication requests and submissions. Once authenticated, the user is passed through to the real servers defined in the load balancing rules.

Document Intention

This document is aimed at administrators who need to deploy Cisco Duo within the organization's network and desire to incorporate the solution within the EdgeADC.

Assumptions

We are going to make the following assumptions for this guide.

a. The person reading this guide is familiar with the configuration and operation of LDAP and RADIUS servers.
b. The person is familiar with the configuring of Cisco Duo and its management UI.

Installation Prerequisites

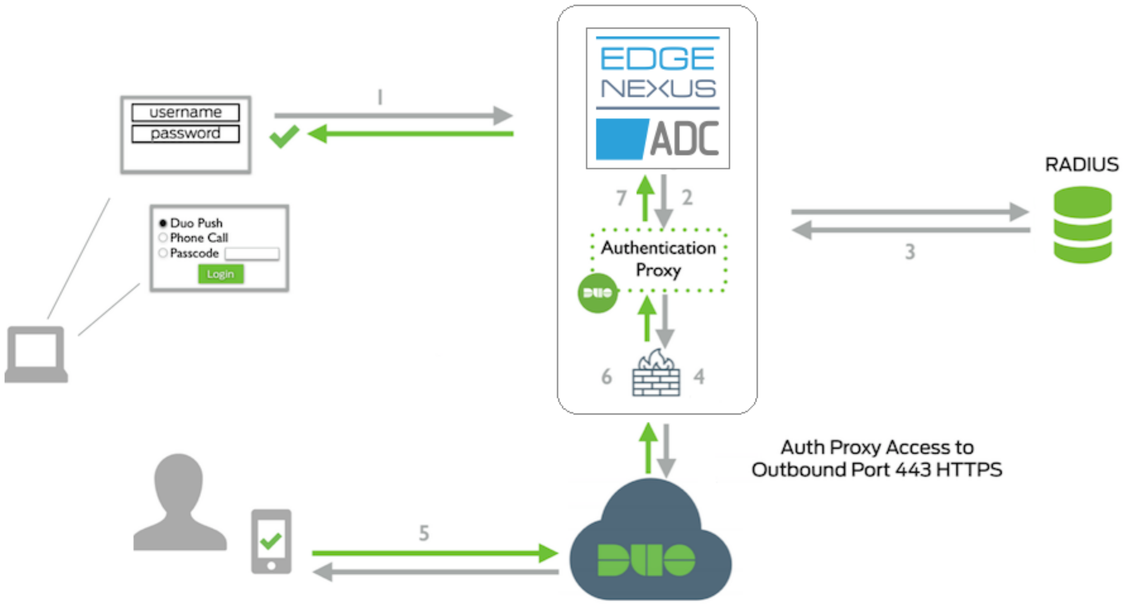
The Cisco Duo integration for the Edgenexus ADC is provided as a Jetpack, an installable containerized application module especially created by Edgenexus.

Installation and operation of the Cisco Duo Jetpack require some prerequisites to be in place and operational. These are:

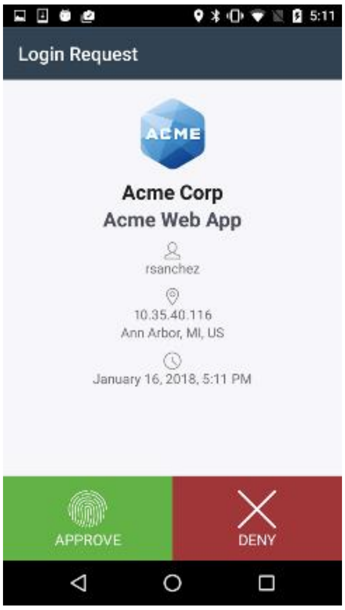
- Edgenexus ADC (single or HA pair)
- LDAP or RADIUS Authentication Server
- A Cisco Duo account

Authentication Workflow

The workflow described below shows the flow of information and subsequent authentication through the ADC and the Cisco Duo system.



1. The user initiates a connection to the target server protected by Duo via the ADC.
2. The ADC essentially acts as middleware and intercepts the user's connection request.
3. The ADC then displays a pre-authentication page to the end-user, similar to the one below, prompting the user for their Radius or LDAP credentials.
4. The ADC then sends an authentication request to the Cisco Duo Authentication Proxy (CDAP) – running in the ADC as a container application.
5. The CDAP completes pre-authentication against LDAP or Radius.
6. The CDAP establishes a secure connection to the Cisco Duo Security Service (CDSS)
7. The CDSS then requests the 2FA from the end-user through the Cisco Duo app.


5:11

Login Request

Acme Corp
Acme Web App
rsanchez
10.35.40.116
Ann Arbor, MI, US
January 16, 2018, 5:11 PM

8. Once the user confirms the result, the result is sent back to the CDAP, which approves the authentication.
9. The user is granted access to the target application by the ADC.

Cisco Duo Initialization

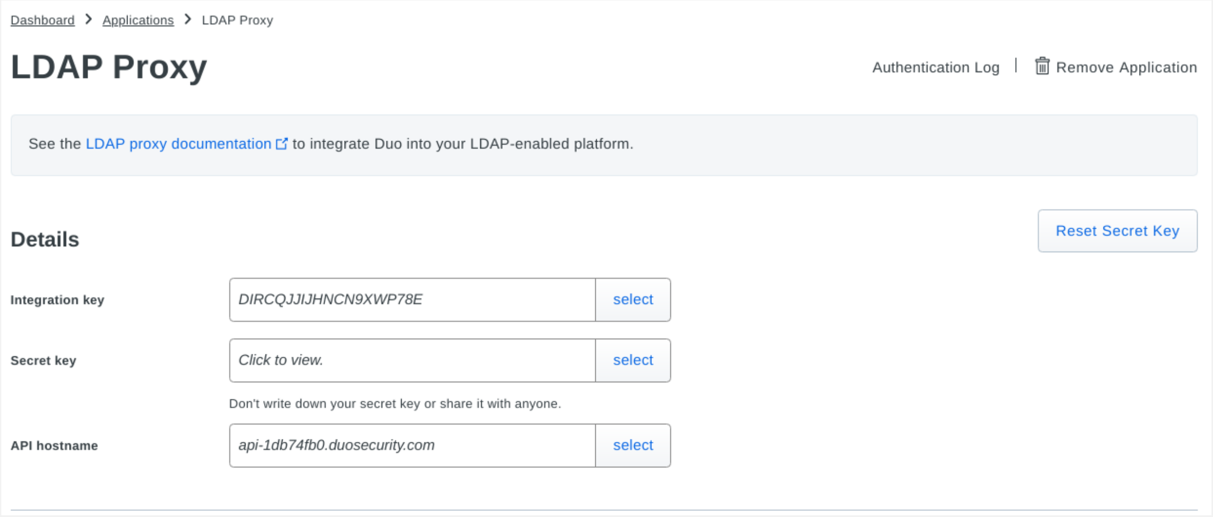
Before installing the Cisco Duo Authentication Proxy into the ADC, we first need to choose an application to protect and obtain the integration and secret keys and the API hostname.

For this exercise, we are going to be configuring using LDAP. The operation is similar for RADIUS.

Our first task is to create a test user to make sure everything works. You do not need to do this if you have a working Duo installation.

You will need access to the Cisco Duo Admin Panel to proceed.

1. Log in to the Duo admin panel and navigate to the Applications page.
2. Click the Protect an Application button and select LDAP from the applications list.
3. Click the Protect button in the application listing line
4. You will see a page with information similar to the one below:



Dashboard > Applications > LDAP Proxy

LDAP Proxy

See the LDAP proxy documentation to integrate Duo into your LDAP-enabled platform.

Details

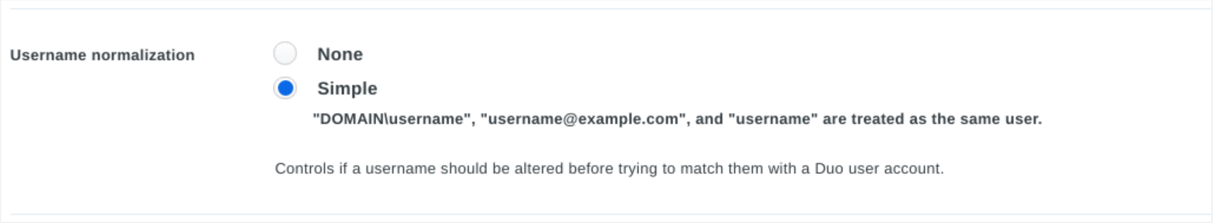
Integration key: DIRCQJJIJHNCN9XWP78E

Secret key: Click to view.

Don't write down your secret key or share it with anyone.

API hostname: api-1db74fb0.duosecurity.com

5. Scroll down the same page until you see the Settings section.
6. There is an option called Username Normalization.



Username normalization

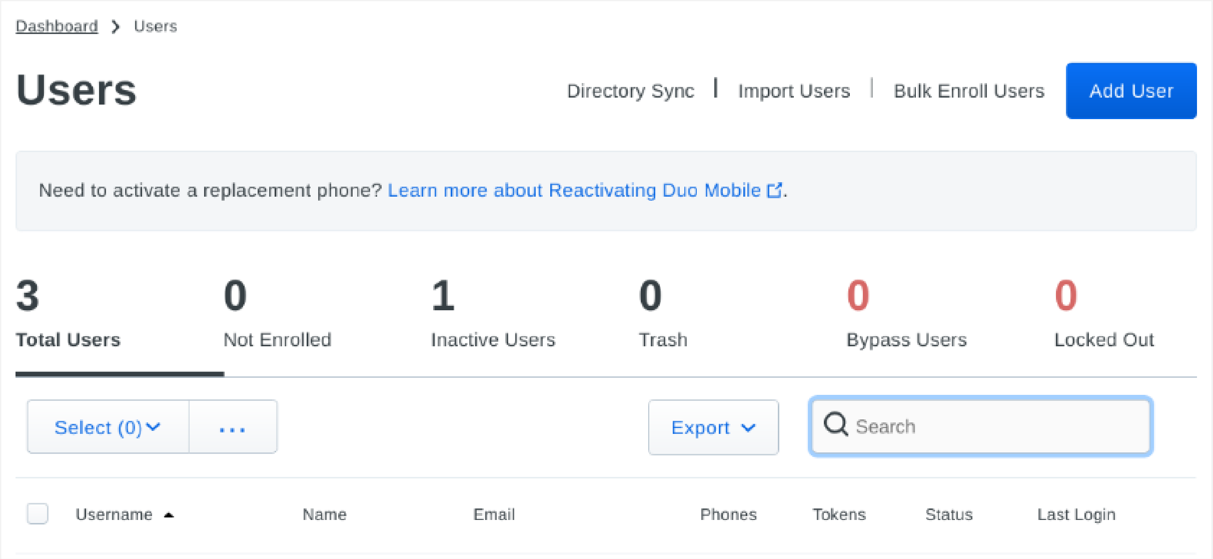
○ None

● 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.

7. Select the Simple option.
8. From the navigation panel, find and the option Users.
9. Click on Users to display the Users section on the main page.



Dashboard > Users

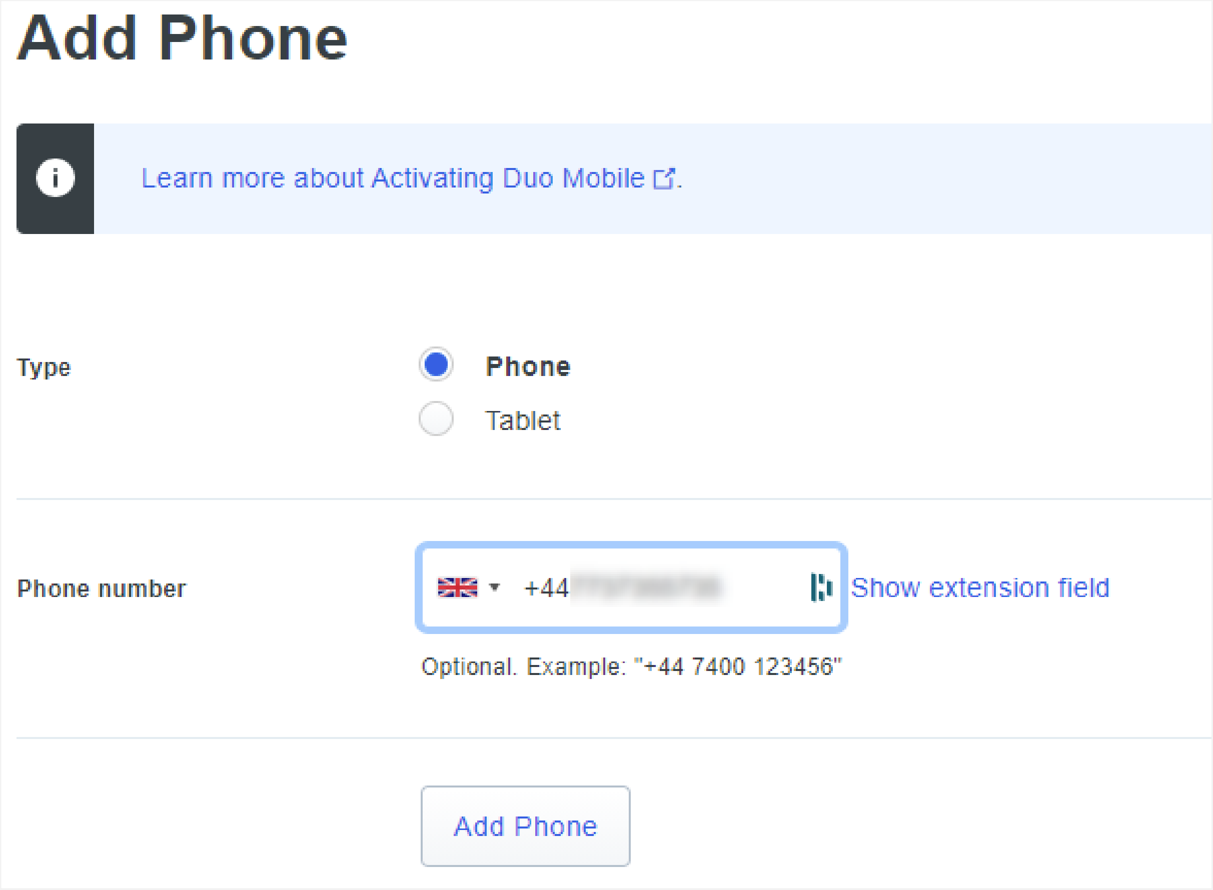
Users

Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.

3	0	1	0	0	0
Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out

□	Username ▲	Name	Email	Phones	Tokens	Status	Last Login

10. Click the Add User button
11. Fill in the fields for Username, Full Name, and Email. We also advise you to select the Add a username alias and create an alias.
12. Install the Cisco Duo mobile application on your phone unless you have already done so. The App will be needed for confirmation.
13. Scroll down the page until you see the Phones section.
14. Click the Add Phone button and fill in the details.



Add Phone

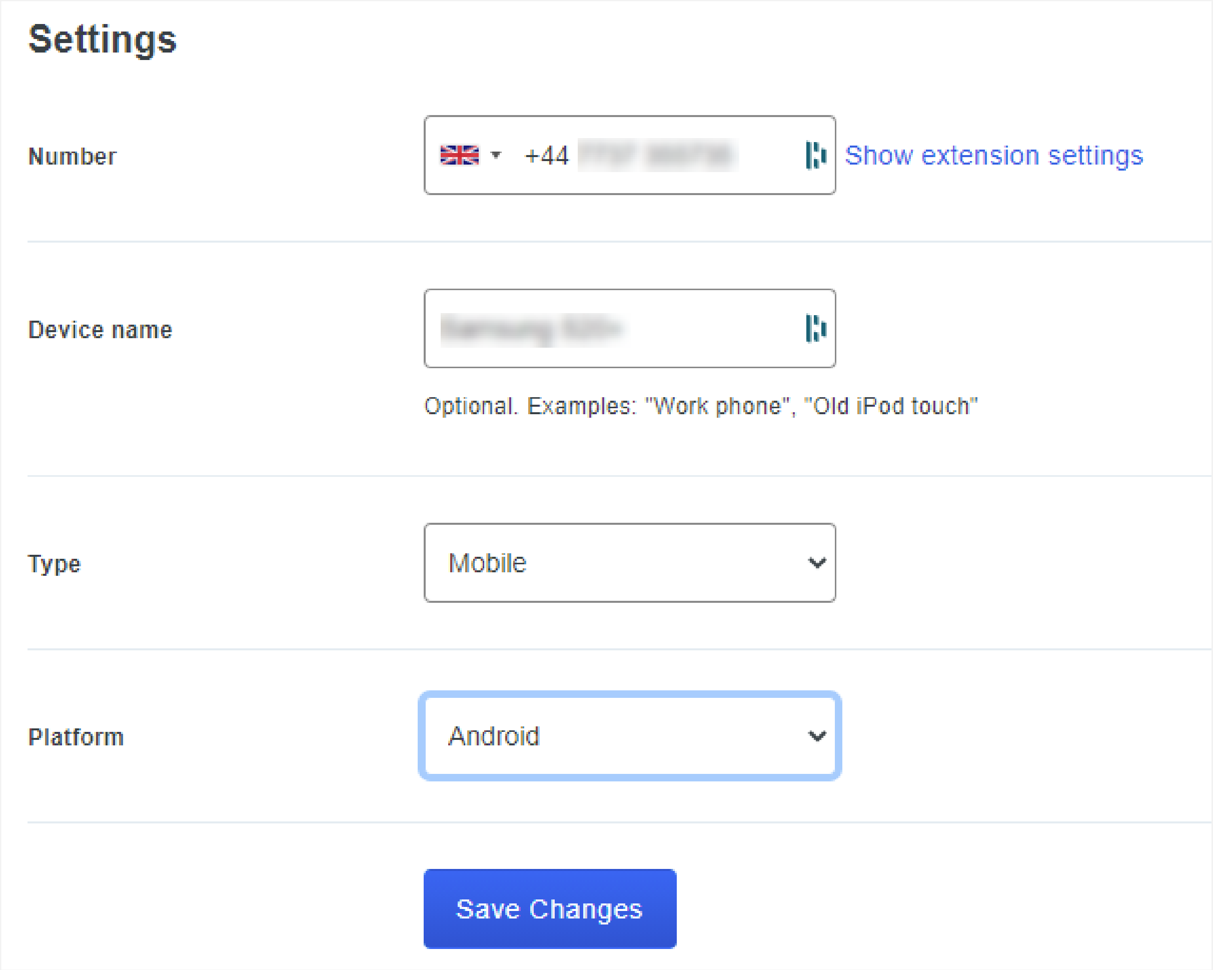
Learn more about Activating Duo Mobile.

Type ● Phone ○ Tablet

Phone number +44 [redacted] Show extension field

Optional. Example: "+44 7400 123456"

15. Fill in the details and click the Add Phone button
16. You will now need to add further information as below.



Settings

Number: +44 [redacted] Show extension settings

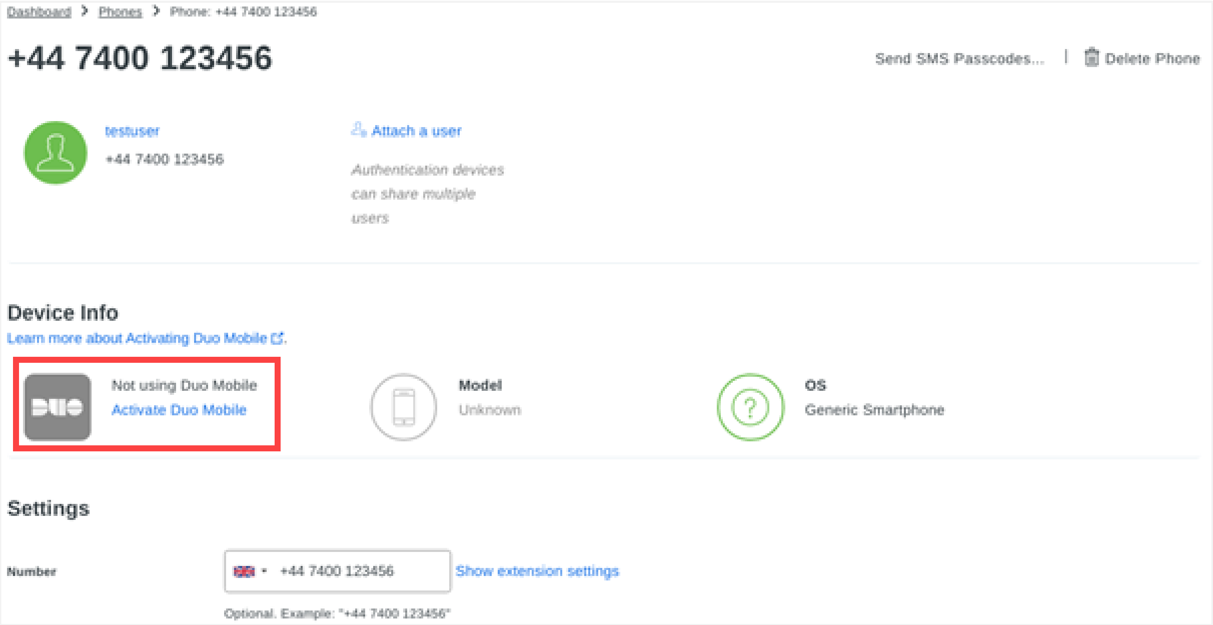
Device name: [redacted]

Optional. Examples: "Work phone", "Old iPod touch"

Type: Mobile

Platform: Android

17. You will now need to click Activate Duo Mobile, shown in the example below.



Dashboard > Phones > Phone: +44 7400 123456

+44 7400 123456

testuser
+44 7400 123456

Authentication devices can share multiple users

Device Info

Learn more about Activating Duo Mobile

Not using Duo Mobile
Activate Duo Mobile

Model: Unknown

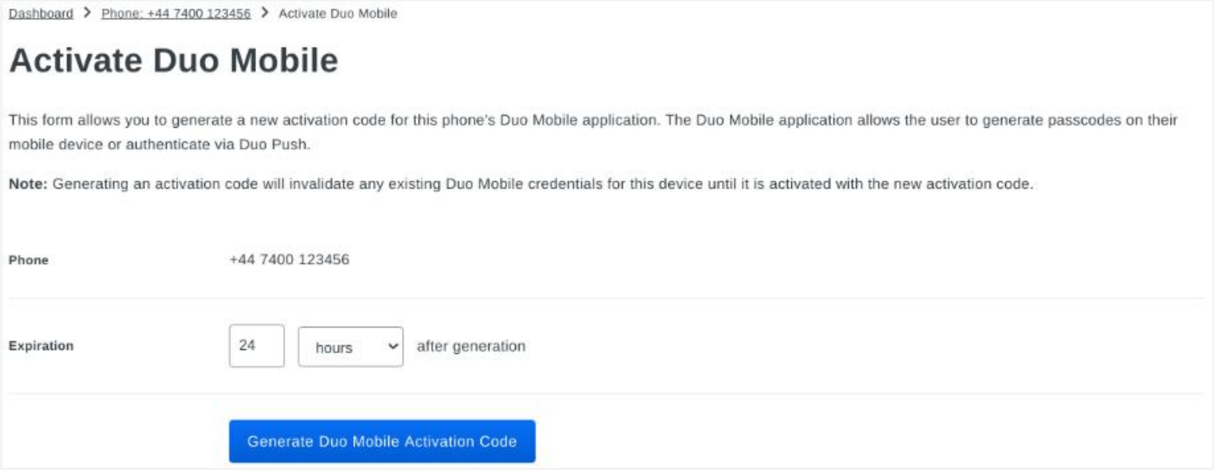
OS: Generic Smartphone

Settings

Number: +44 7400 123456 Show extension settings

Optional. Example: "+44 7400 123456"

18. This action will take you to a new screen, as shown below. Click the Generate Duo Mobile Activation Code, and then click the Send Instructions by SMS 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 24 hours after generation

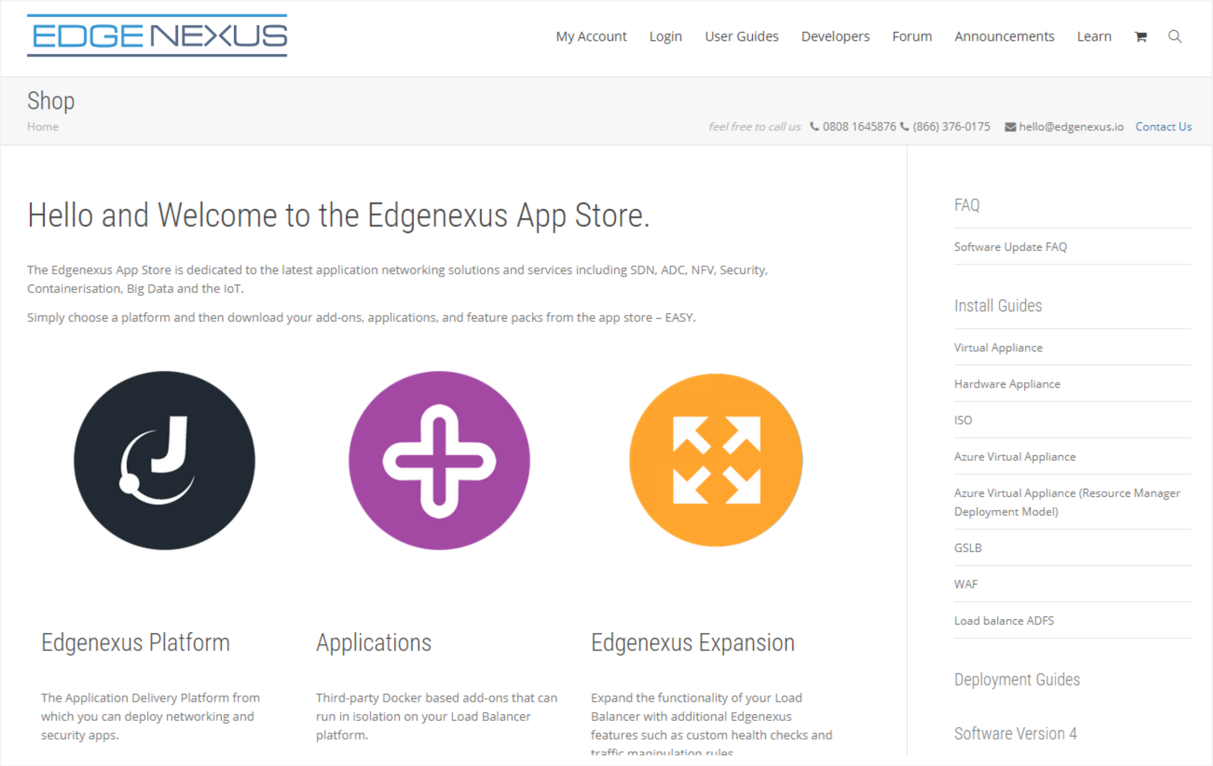
19. You will get an SMS message with an activation link. Click the link, and the user we created will be activated and added to the Cisco Duo App.

Installing the Cisco Duo Authentication Proxy (CDAP)

The next stage is to install the Cisco Duo Authentication Proxy, also referred to as CDAP.

The CDAP product is available as a Jetpack, a containerized application developed by Edgenexus in collaboration with Cisco. The CDAP Jetpack installs directly into the ADC using the Dockers container technology.

1. Log into the ADC using administrator credentials.
2. First, we will navigate to the App Store and download the Cisco Duo Authentication Proxy app. We will assume that you have created your App Store account (https://appstore.edgenexus.io) and associated this with your ADC.
3. Navigate to Services > App store



Hello and Welcome to the Edgenexus App Store.

The Edgenexus App Store is dedicated to the latest application networking solutions and services including SDN, ADC, NFV, Security, Containerisation, Big Data and the IoT.

Simply choose a platform and then download your add-ons, applications, and feature packs from the app store – EASY.

Edgenexus Platform

The Application Delivery Platform from which you can deploy networking and security apps.

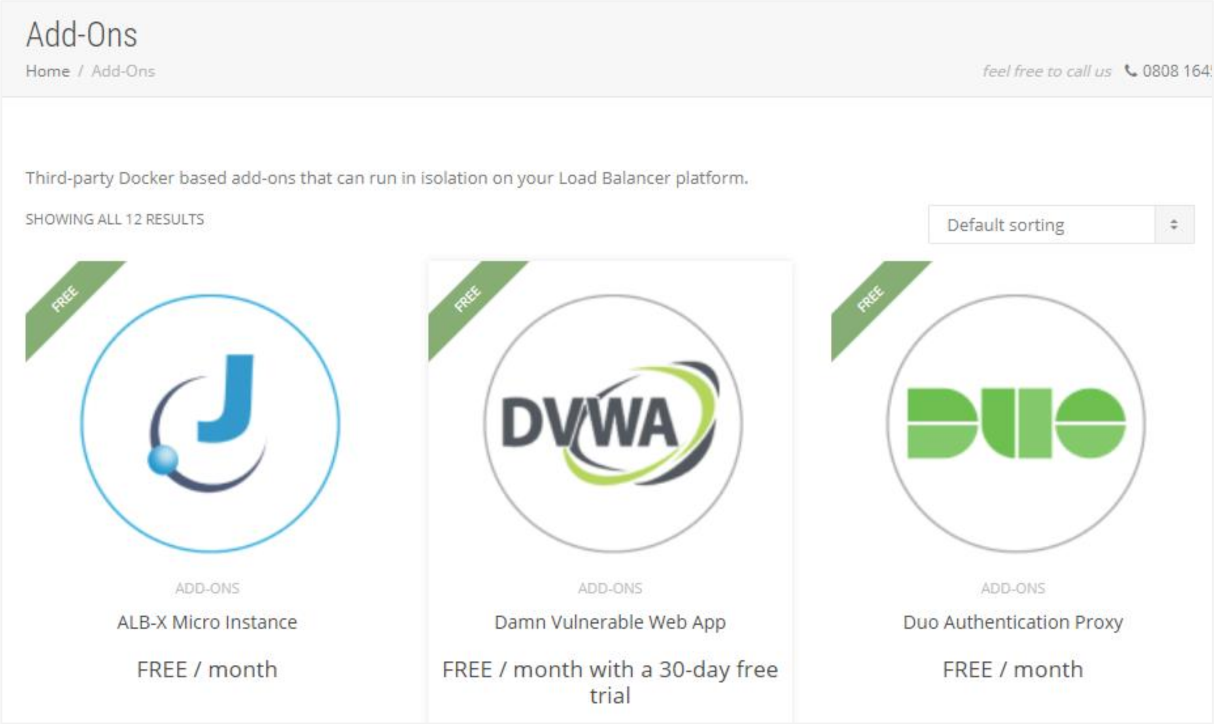
Applications

Third-party Docker based add-ons that can run in isolation on your Load Balancer platform.

Edgenexus Expansion

Expand the functionality of your Load Balancer with additional Edgenexus features such as custom health checks and traffic manipulation rules

4. Click on the Applications icon and click on the Duo application icon



Add-Ons

Home / Add-Ons

feel free to call us ☎ 0808 164

Third-party Docker based add-ons that can run in isolation on your Load Balancer platform.

SHOWING ALL 12 RESULTS

Default sorting

FREE

ADD-ONS

ALB-X Micro Instance

FREE / month

FREE

ADD-ONS

Damn Vulnerable Web App

FREE / month with a 30-day free trial

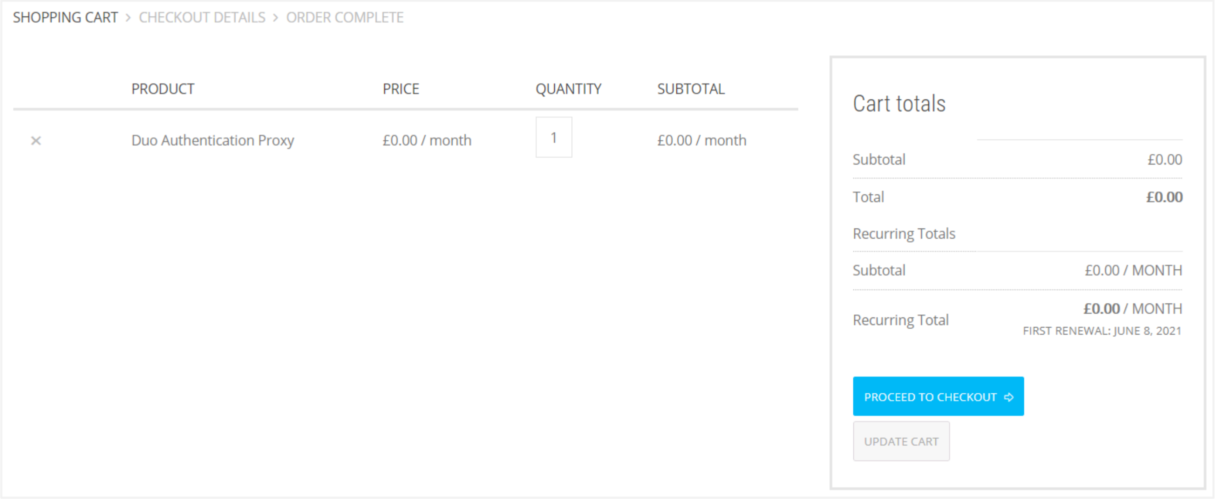
FREE

ADD-ONS

Duo Authentication Proxy

FREE / month

5. The application is free, and you can click the Sign Up Now button. This action will add the application to the shopping cart, as shown below.



SHOPPING CART > CHECKOUT DETAILS > ORDER COMPLETE

	PRODUCT	PRICE	QUANTITY	SUBTOTAL
×	Duo Authentication Proxy	£0.00 / month	1	£0.00 / month

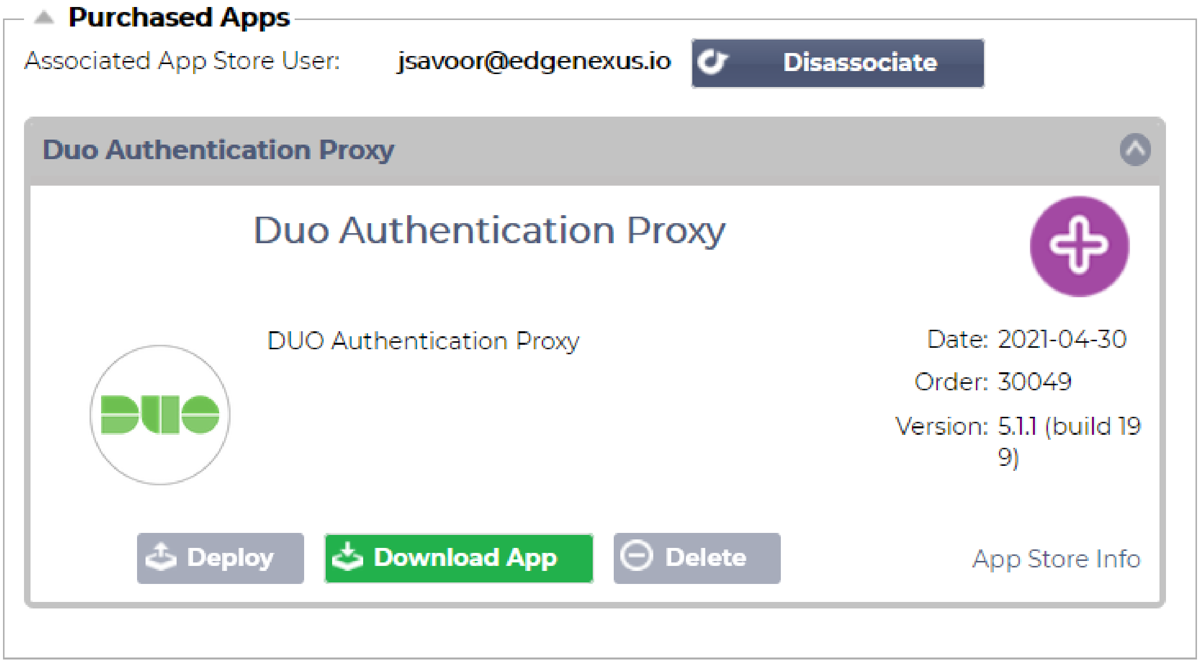
Cart totals

Subtotal	£0.00
Total	**£0.00**
Recurring Totals	
Subtotal	£0.00 / MONTH
Recurring Total	**£0.00** / MONTH FIRST RENEWAL: JUNE 8, 2021

PROCEED TO CHECKOUT

UPDATE CART

6. Click checkout, and the CDAP app will appear in your purchased items within the Services > App Store section.



Purchased Apps

Associated App Store User: jsavoor@edgenexus.io

Duo Authentication Proxy

Duo Authentication Proxy

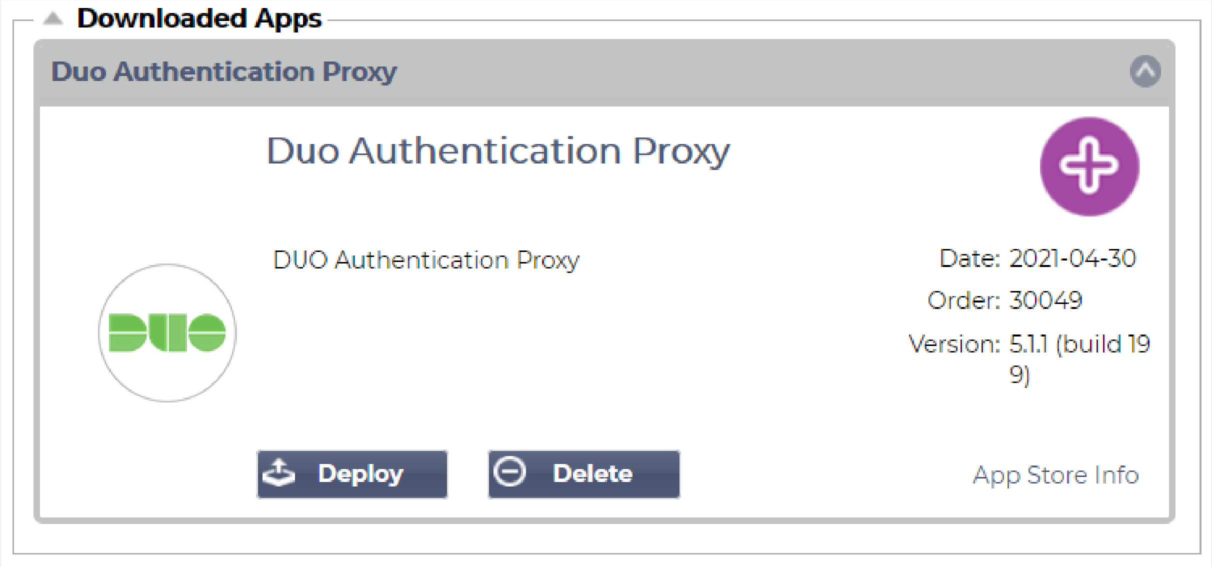
DUO Authentication Proxy

Date: 2021-04-30

Order: 30049

Version: 5.1.1 (build 19 9)

7. Click the Download button to download the App to the ADC appliance.
8. Once downloaded, the App will then appear in the Downloaded Apps section on the same page.



Downloaded Apps

Duo Authentication Proxy

Duo Authentication Proxy

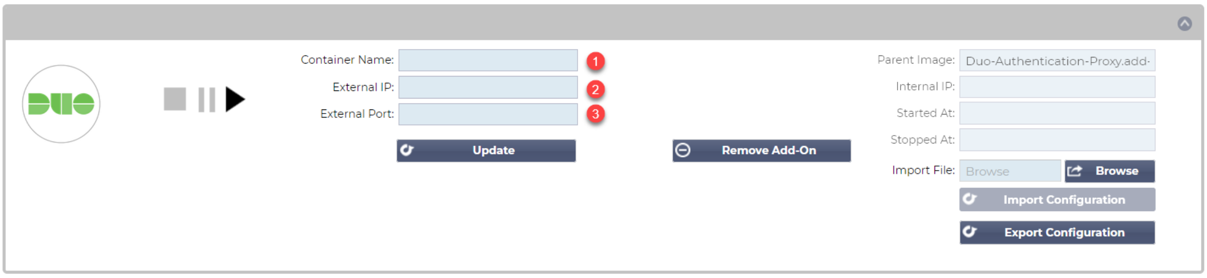
DUO Authentication Proxy

Date: 2021-04-30

Order: 30049

Version: 5.1.1 (build 19 9)

9. Now click on the Deploy button to deploy it into a container, ready for configuration.
10. Navigate to Library > Add-Ons once the deployment process is complete.
11. You will now need to fill in the details highlighted using the table below the image.



Container Name: 1

External IP: 2

External Port: 3

Parent Image: Duo-Authentication-Proxy.add-

Internal IP:

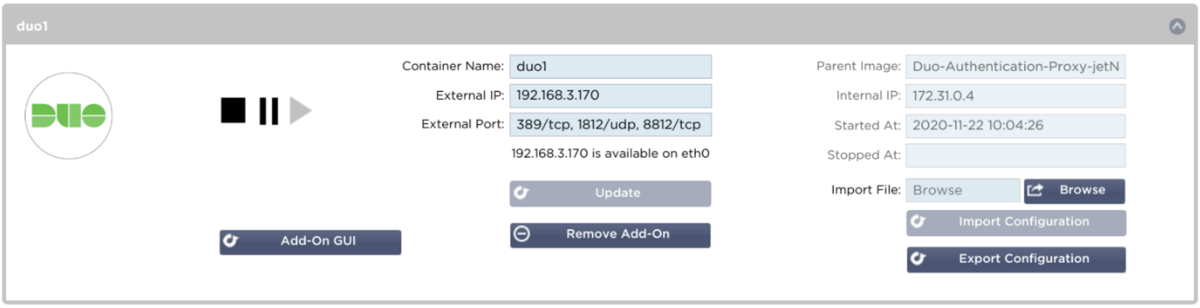
Started At:

Stopped At:

Import File: Browse

Field	Data
Container Name	A name you will give for the CDAP application. The name you provide will be referenced later within the flightPATH rules you will create for Duo to work.
External IP	The external IP value can be anything within the subnet in which the ADC sits.
External Ports	The value to be entered here is: as follows: **389/TCP, 1812/UDP, 8812/TCP** LDAP uses 389/TCP, Radius uses 1812/UDP, and the Cisco Duo Authentication Proxy (CDAP) uses 8812/TCP.

12. Click the PLAY or START button to activate the CDAP App. The screen should show something similar to the image below.



duo1

Container Name: duo1

External IP: 192.168.3.170

External Port: 389/tcp, 1812/udp, 8812/tcp

192.168.3.170 is available on eth0

Parent Image: Duo-Authentication-Proxy-jetN

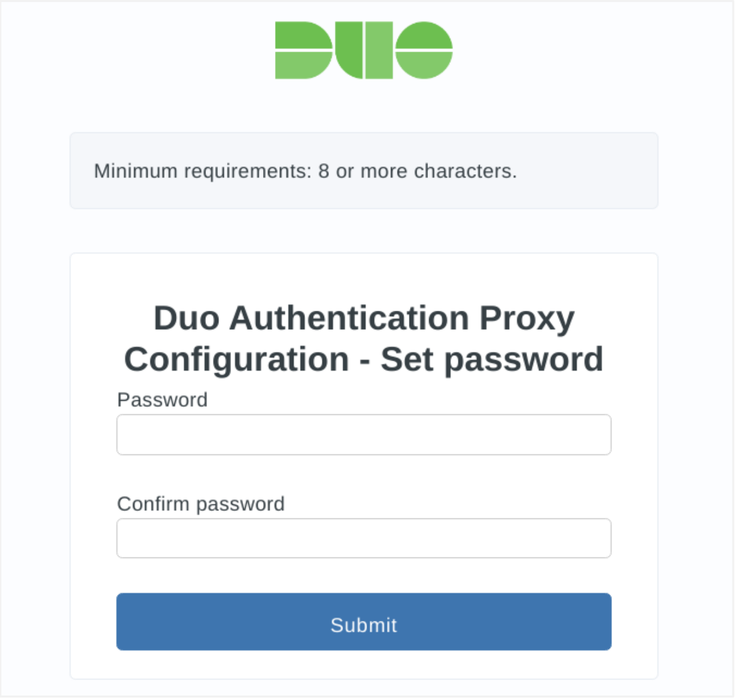
Internal IP: 172.31.0.4

Started At: 2020-11-22 10:04:26

Stopped At:

Import File: Browse

13. Click the Add-On GUI button.
14. The first time you visit the CDAP App's user interface, you will be asked to create the admin password for the App.



Minimum requirements: 8 or more characters.

Duo Authentication Proxy Configuration - Set password

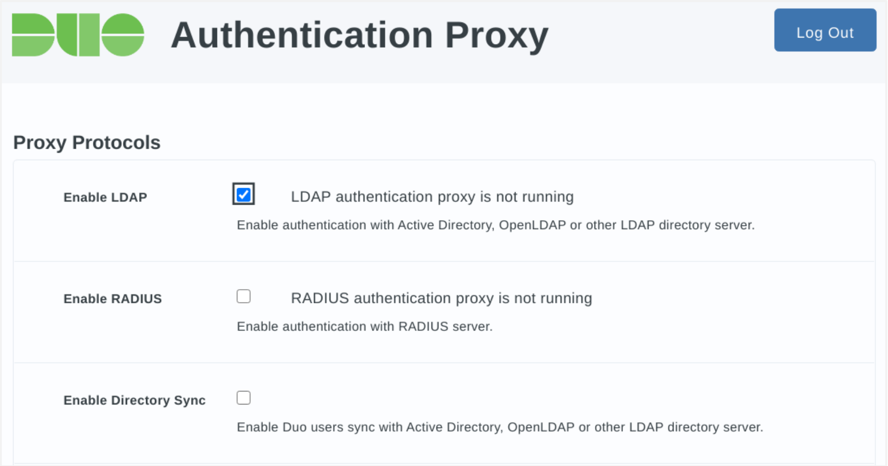
Password

Confirm password

Configuring for LDAP Authentication

To use the Cisco Duo Authentication Proxy (CDAP) with LDAP, we need to make some configuration changes to the CDAP App. This configuration change will allow you to use Active Directory, OpenLDAP, or any other LDAP server as the primary authentication source.

Proxy Protocols



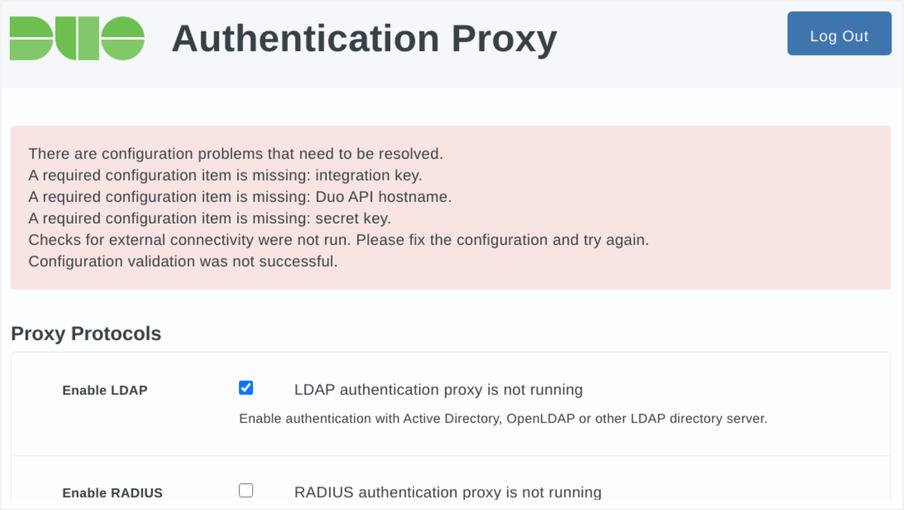
Proxy Protocols

Enable LDAP ☑ LDAP authentication proxy is not running
Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.

Enable RADIUS □ RADIUS authentication proxy is not running
Enable authentication with RADIUS server.

Enable Directory Sync □
Enable Duo users sync with Active Directory, OpenLDAP or other LDAP directory server.

1. When you are presented with the UI as shown above, please tick the Enable LDAP checkbox
2. Click Save Settings.
3. Whenever you change the Duo Authentication settings, CDAP will initiate a configuration check to ensure there are no errors. If the LDAP configuration is correct and operational, you should not see any errors. However, on the first run, you may see errors, as seen in the image below. There is nothing to worry about when such errors are displayed.



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.

Proxy Protocols

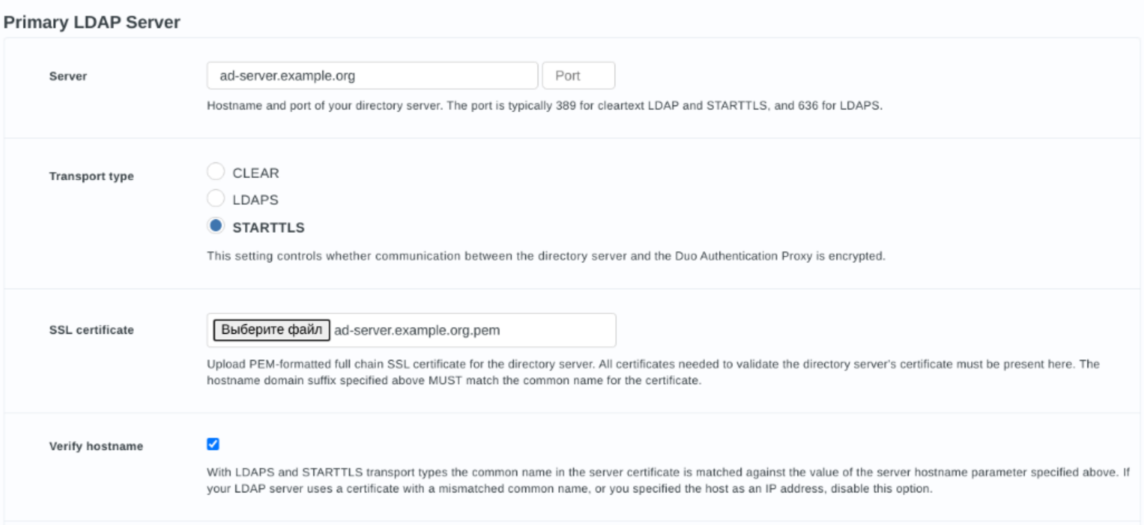
Enable LDAP ☑ LDAP authentication proxy is not running
Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.

Enable RADIUS □ RADIUS authentication proxy is not running

4. The 'required configuration' errors you see are due to required data not being configured as yet – we will get to that later on.

Primary LDAP Server

5. In the Primary LDAP Server section shown below, fill in the LDAP server hostname or IP address, together with the Port. Typically the port number is 389 for clear text LDAP and STARTTLS, and 636 for LDAPS.



Primary LDAP Server

Server: ad-server.example.org | Port

Hostname and port of your directory server. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS.

Transport type:
○ CLEAR
○ LDAPS
● STARTTLS

This setting controls whether communication between the directory server and the Duo Authentication Proxy is encrypted.

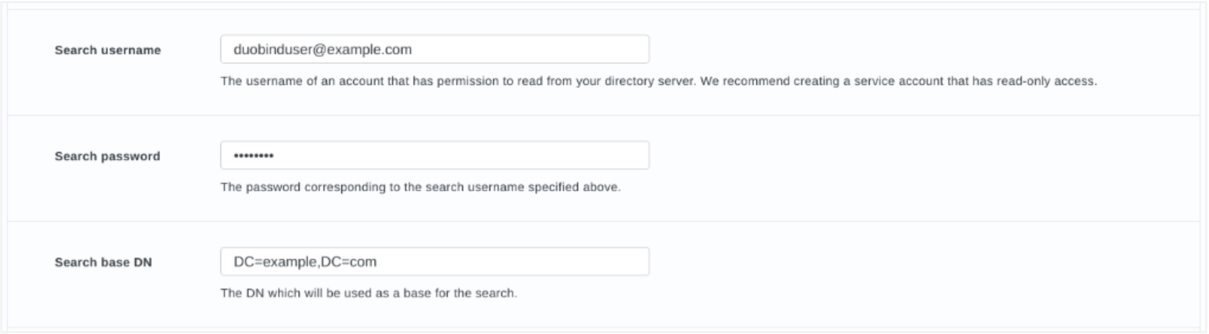
SSL certificate: Выберите файл ad-server.example.org.pem

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: ☑

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.

6. Select the Transport Type according to your network infrastructure.
7. Click on the Add Certificate button in the SSL Certificate section, and upload your LDAP server certificate if you use STARTTLS or LDAPS encrypted access. The certificate must be in PEM format and contain the FULL chain of certification, including the CA ROOT and all intermediate certificates. Please see "How do I export a complete issuing certificate chain for LDAPS authentication with Active Directory?" linked here for further information.
8. In cases where you have specified the LDAP server using its IP address or the hostname used does not match the name used in the SSL certificate, you will have to uncheck the Verify Hostname checkbox. Note, however, that this will reduce the security guarantees provided by SSL/TLS. Disabling the Verify Hostname check may also be required when the Transport Type is set to Clear.
9. We recommend creating a dedicated read-only access account on the LDAP server to use the CDAP when searching for users listed in the Directory.
10. Once done, or if a suitable username is present, provide the username, password, and the base DN as shown in the example below.



Search username: 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: ••••••••

The password corresponding to the search username specified above.

Search base DN: DC=example,DC=com

The DN which will be used as a base for the search.

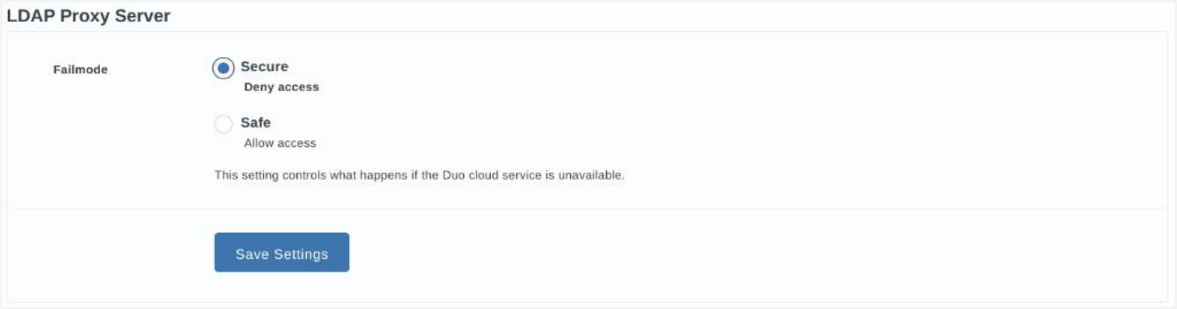
11. Next, set the Authentication type to Plain LDAP as this is the type compatible with the EdgeADC. If this does not work for you, please try the other types before contacting Support. Please also specify the BIND DN parameter. This value is typically the full LDAP

distinguished name of the account permitted to read from the Directory and the name you specified in the Search Username field.

12. You can also specify the Username Attribute value if your LDAP server's username attribute name is different from the commonly used sAMAccountName and UID user attribute names.

LDAP Proxy server

13. The Failmode setting controls whether access should be allowed or denied should Duo Cloud connections become unavailable.



LDAP Proxy Server

Failmode

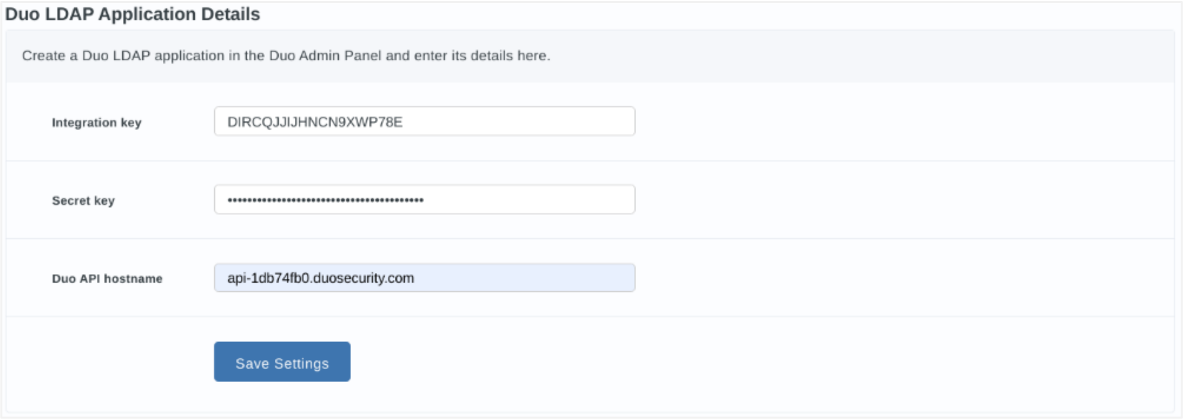
● Secure
Deny access

○ Safe
Allow access

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

14. In the Duo LDAP Application Details section, you must add the Integration Key, Secret Key, and Duo API Hostname values. These are found on the Applications page of the Dup Admin panel.

Duo LDAP Application Details



Duo LDAP Application Details

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

Integration key: DIRCQJJIJHNCN9XWP78E

Secret key: ••

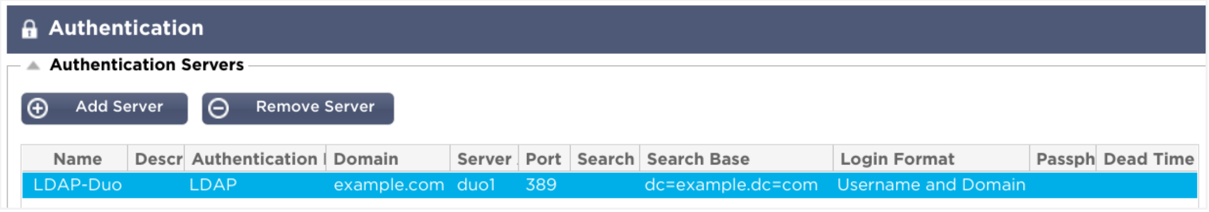
Duo API hostname: api-1db74fb0.duosecurity.com

15. Once done, click the Save Settings button, after which you will get a message showing success or get an error if any of the settings were incorrect.

Configuring the ADC for Duo with LDAP Authentication

Now come the steps to configure the ADC so that users can authenticate using LDAP and Cisco Duo. The guide will now assume that you are familiar with the ADC and its configuration methods and features.

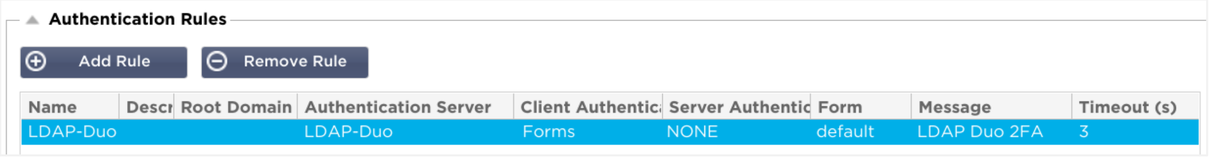
1. Proceed to Library > Authentication using the navigation panel of the ADC
2. You will now see the Authentication Servers section on the right panel.
3. Click Add Server
4. A new line will appear, showing some fields that you will need to fill in. An example of the filled-in fields is shown below.



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		

Field Name	Example and description
Name	The name can be any alphanumeric value, but for ease of understanding, let's use LDAP-Duo
Description	Optional, this value describes this entry
Authentication	Select LDAP from the drop-down
Domain	The value here should be your LDAP domain
Server	The value you provide here should be the same as the name you gave your Cisco Duo Authentication Proxy – this is important.
Port	389 is the standard Port used
Search	Optional and can be left blank
Search Base	Enter the search Base DN
Login format	Select 'Username and Password' from the drop-down
Passphrase	Optional
Dead Time	Optional

5. The next step is to create an authentication rule to handle the requests for Duo authentication. See the example below. Fill in the fields as explained in the table below the image.



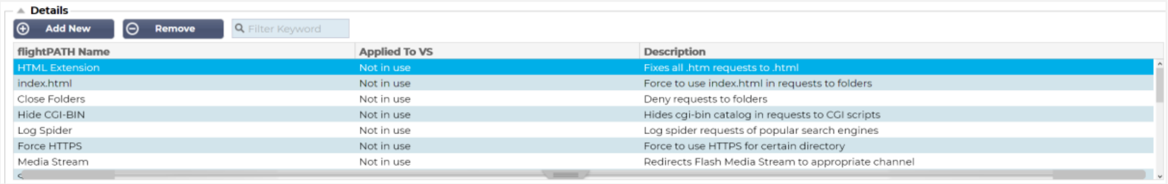
Name	Descr	Root Domain	Authentication Server	Client Authentic	Server Authentic	Form	Message	Timeout (s)
LDAP-Duo			LDAP-Duo	Forms	NONE	default	LDAP Duo 2FA	3

Field Name	Explanation
Name	Add a suitable name for the rule – it could be something like LDAP-Duo-Rule.
Description	Optional, this is the description for the rule.
Root Domain	Optional, unless you wish to use single-sign-on across sub-domains.
Authentication Server	A drop-down field – select the name of the Authentication Server you created in the previous steps.
Client Authentication	A drop-down field – select Forms
Server Authentication	A drop-down field – select None
Form	A drop-down field – select Default
Message	We will use the value to display a message on the form shown to the user. An example may be "LDAP-Duo 2FA."
Timeout	The value is specified in seconds, after which the user will need to authenticate again.

Creating the flightPATH rule

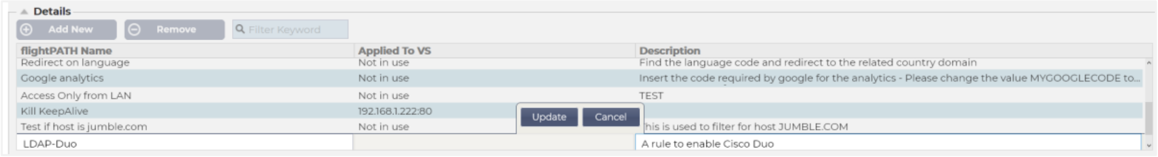
For the Cisco Duo authentication to work correctly through the CDAP, we need to create a traffic management rule using fightPATH. The ADC will redirect the data received into the Virtual Service to the CDAP engine for action.

1. Navigate to Library > flightPATH using the left-side navigation pane.
2. You will see the flightpath configuration panel on the right of the navigation pane. There are some predefined rules in the Details section, but for Duo, we will be creating a new and straightforward rule.



flightPATH Name	Applied To VS	Description
HTML Extension	Not in use	Fixes all .htm requests to .html
index.html	Not in use	Force to use index.html in requests to folders
Close Folders	Not in use	Deny requests to folders
Hide CGI-BIN	Not in use	Hides cgi-bin catalog in requests to CGI scripts
Log Spider	Not in use	Log spider requests of popular search engines
Force HTTPS	Not in use	Force to use HTTPS for certain directory
Media Stream	Not in use	Redirects Flash Media Stream to appropriate channel

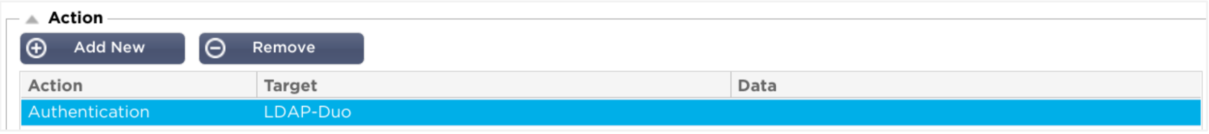
3. Click the Add New button located at the top left of the Details section.
4. A new line for adding the flightPATH detail line will be shown.



flightPATH Name	Applied To VS	Description
Redirect on language	Not in use	Find the language code and redirect to the related country domain
Google analytics	Not in use	Insert the code required by google for the analytics - Please change the value MYGOOGLECODE to...
Access Only from LAN	Not in use	TEST
Kill KeepAlive	192.168.1.222:80	
Test if host is jumble.com	Not in use	his is used to filter for host JUMBLE.COM
LDAP-Duo		A rule to enable Cisco Duo

Field	Description
flightPATH Name	This field represents the name you will give the flightPATH rule, and it is referred to within drop-down menus elsewhere in the GUI.
Applied to VS	Auto populated when you apply the rule to a Virtual Service
Description	The description is a plain language description to allow you to remember what the flightPATH rule was designed for

5. For this exercise, we have named the flightPATH rule as LDAP-Duo
6. In this guide, we are not going to use any Conditions or Evaluations. You could, for example, configure a Condition that only allows access to the authentication form from a specific IP or subnet, or if you only want to challenge users that access a specific path such as '/secure.' More information on flightPATH can be found in the EdgeADC administrator guide.
7. Next, we will configure what will happen next in the Actions section.



Action	Target	Data
Authentication	LDAP-Duo	

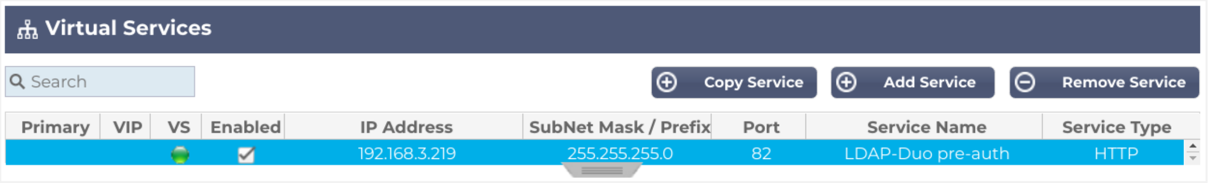
Field	Description
Action	This field informs what to do what the rule condition is met. In this case, the Action is Authentication.
Target	A drop-down field and the value you select here must be the Authentication Server you created, in this case, LDAP-Duo.
Data	Leave blank

8.

Creating the Cisco Duo Virtual Service

To make use of the Cisco Dup Authentication Proxy (CDAP), we need to create the Virtual IP (VIP) and Virtual Service (VS). It is this VIP that users will aim their browsers to access the software.

1. Navigate to Services > IP Services using the left-side navigation panel.
2. The IP Services panel will be shown on the right side.
3. The IP Services panel consists of 2 main sections: Virtual Services and Real Servers.

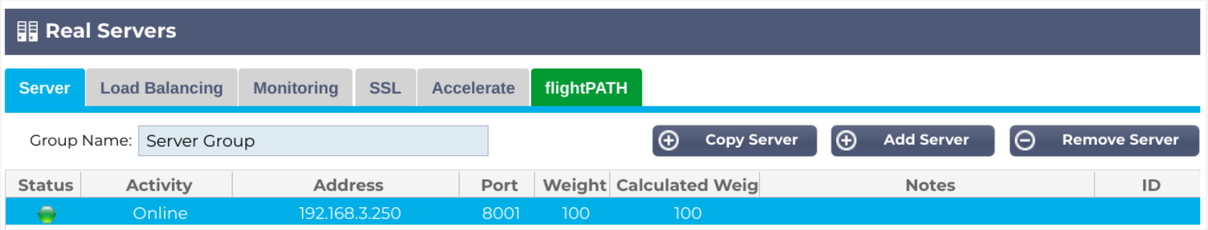


Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
		●	☑	192.168.3.219	255.255.255.0	82	LDAP-Duo pre-auth	HTTP

4. Click the Add Service button in the Virtual Services section. Fill in the details that are relevant to your network infrastructure. We have highlighted the areas you need to specify in **GREEN**. Remember to set the Service Type as HTTP.

Field	Description
Primary/Mode	An auto-populated field that indicates whether the VIP is Active, In Drain, or Disabled
VIP	A visual indicator that displays in a variety of colors to show the status of the VIP. See Admin Guide.
VS	A visual indicator that displays in a variety of colors to show the status of the VS. See Admin Guide.
Enabled	A checkbox used to enable or disable the VIP/VS
IP Address	The IP address that users will use to access the software – Please add the IP address you are going to use
Subnet Mask/Prefix	The relevant and applicable subnet mask for your network segment
Port	The Port that the users will specify in the URL (in our example, we are using 82)
Service Name	A short name for the VIP/VS
Service Type	This drop-down should be set to **HTTP** as we are going to use a flightPATH rule

5. Now we will start configuring the Real Servers section.



Group Name: Server Group

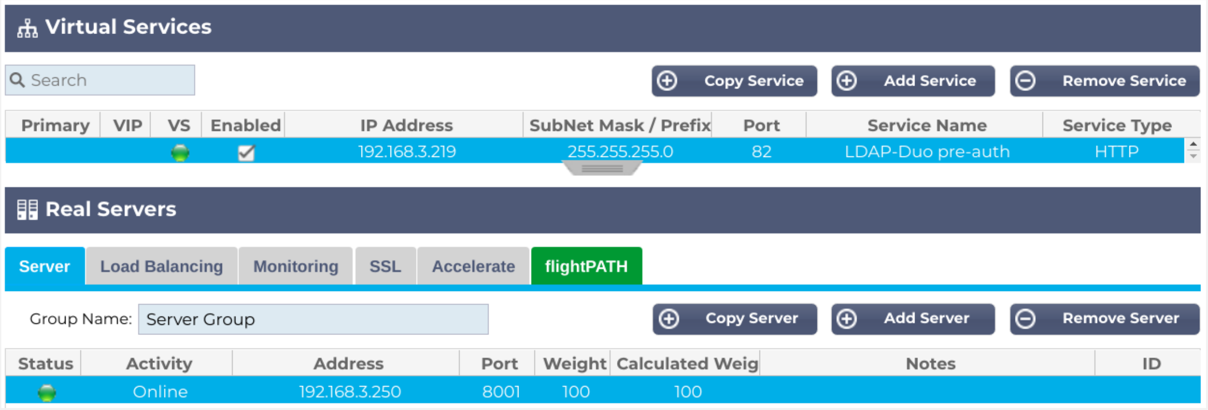
Status	Activity	Address	Port	Weight	Calculated Weig	Notes	ID
●	Online	192.168.3.250	8001	100	100		

The Server Tab

The Server Tab is used to specify the Real Server or load-balanced set of Real Servers you are trying to protect with Cisco Duo 2FA. In our example, there is only a single server.

Field	Description
Status	This indicator will display the current status of the connection to the Real Server. See the administration guide for the meaning of status colors.
Activity	Will show whether the Real Server is online or not
Address	The IP Address of the Real Server
Port	The Port configured for accessing the Real Server and its software
Weighting	This field can be configured if required, but we recommend that you let the ADC handle this.
Notes	This field describes Real Server and any relevant notes.

6. Fill in the details shown in GREEN per your requirements.
7. Once you have done that, the Status indicator should light up Green, and the VIP and VS lights on the Virtual Services section. If they are not Green, this indicates there may be an issue with connectivity or configuration. An example of this is shown below.

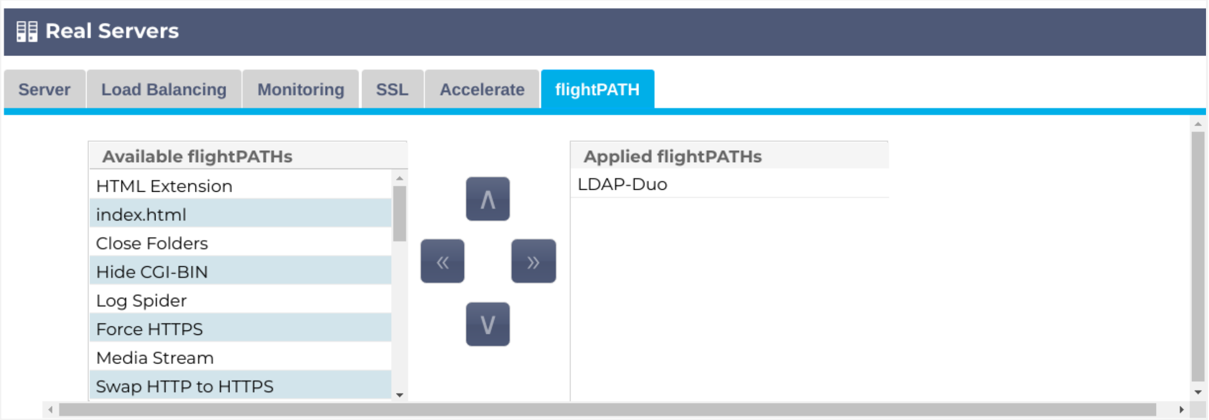


Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
		●	☑	192.168.3.219	255.255.255.0	82	LDAP-Duo pre-auth	HTTP

Group Name: Server Group

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

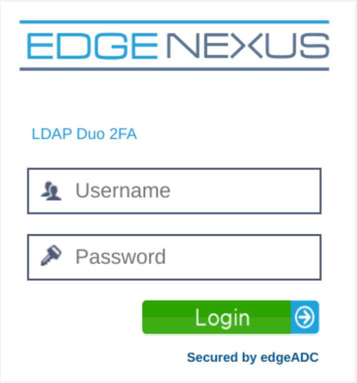
8. Now click the flightPATH tab. You will see the flightPATH details as shown below.



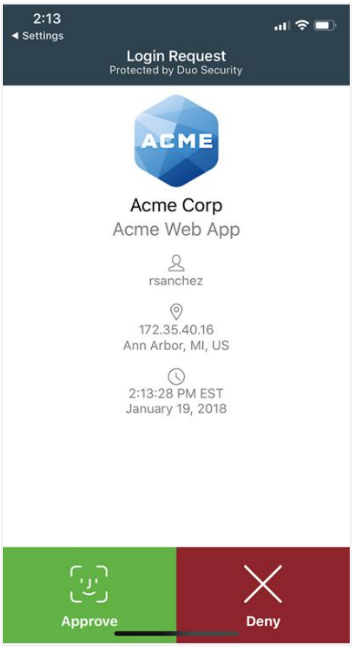
9. Please scroll down the Available flightPATHs until you see the LDAP-Duo rule we created.
10. Select the rule and click the right arrow button in the central area.
11. The flightPATH rule will be moved to the Applied flightPATH segment on the right of the arrow buttons.
12. The rule is immediately applied and is operational.

The Cisco Duo Authentication Proxy has now been installed and is fully operational. The Real Server(s) specified in the Real Servers section are now protected using Cisco Duo authentication using the CDAP engine.

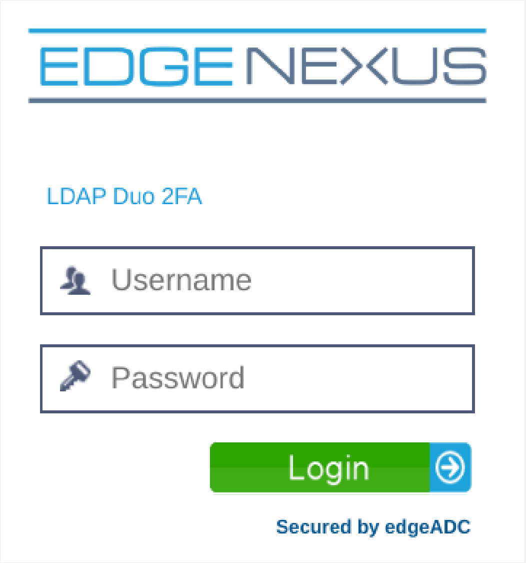
Users navigating the http://192.168.3.219:82, in our example, will see the dialog for authentication shown below. The IP address and Port you may use will almost definitely be different, perhaps using Port 443.



13. Enter the username and password of the test user you created in your LDAP server and the Duo Admin Panel.
14. If the credentials pass LDAP authentication, you will soon get a confirmation request in the Cisco Duo Mobile App on the phone associated with the Duo test user. It will look something like the example below.



15. If you Approve the request, you will be connected to the Real Server configured for the VIP. If you choose to Deny the confirmation request, you will see the login page again along with an error stating the username and/or password are incorrect.

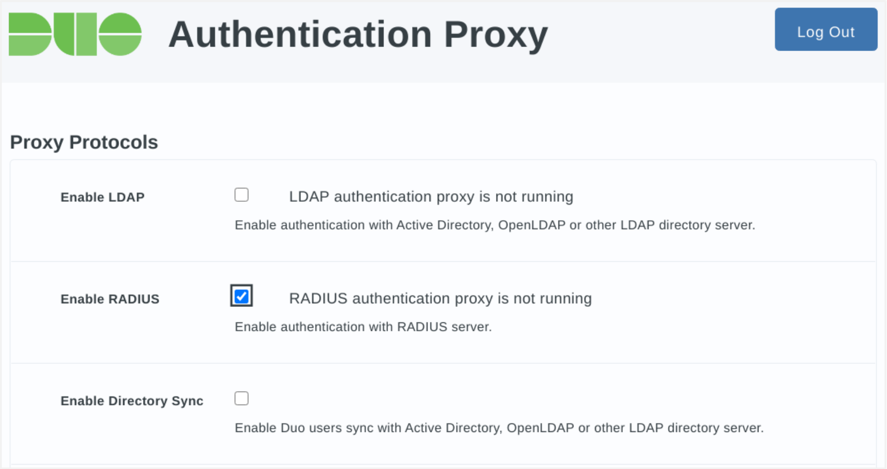


16. Guides for the iOS and Android phone Apps are available here:
    a. Cisco Duo App User Guide for Apple iOS
    b. Cisco Duo App User Guide for Android

Configuring for RADIUS Authentication

To use the Cisco Duo Authentication Proxy (CDAP) with RADIUS, we need to make some configuration changes to the CDAP App. This configuration change will allow you to use your existing RADIUS server as the primary authentication source.

Proxy Protocols



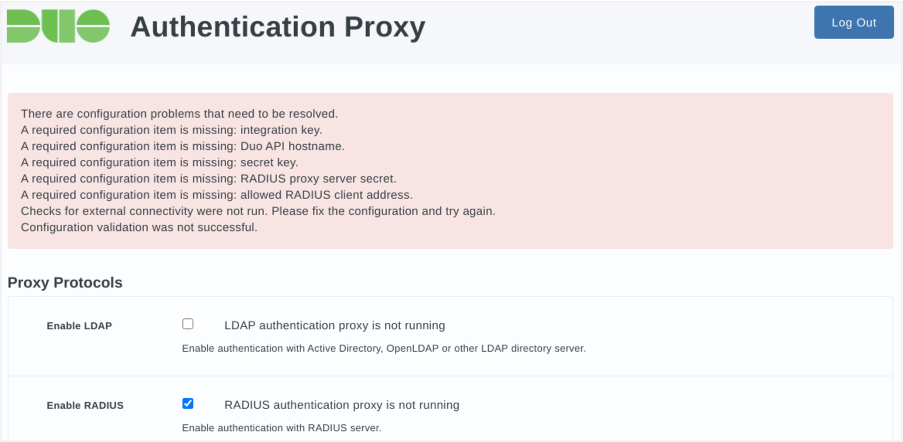
Proxy Protocols

Enable LDAP □ LDAP authentication proxy is not running
Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.

Enable RADIUS ☑ RADIUS authentication proxy is not running
Enable authentication with RADIUS server.

Enable Directory Sync □
Enable Duo users sync with Active Directory, OpenLDAP or other LDAP directory server.

1. When you are presented with the UI as shown above, please tick the Enable RADIUS checkbox
2. Click Save Settings.
3. Whenever you change the Duo Authentication settings, CDAP will initiate a configuration check to ensure there are no errors. If the RADIUS configuration is correct and operational, you should not see any errors. However, on the first run, you may see errors, as seen in the image below. There is nothing to worry about when such errors are displayed.



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.

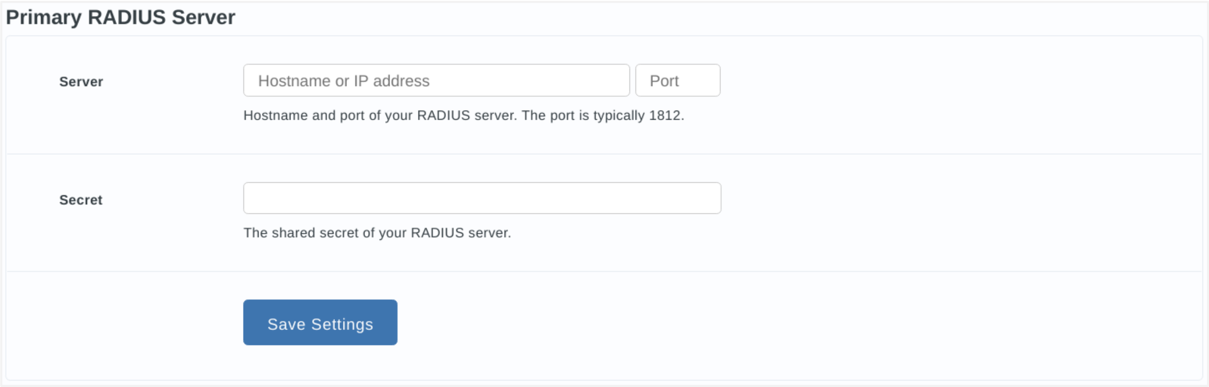
Proxy Protocols

Enable LDAP □ LDAP authentication proxy is not running
Enable authentication with Active Directory, OpenLDAP or other LDAP directory server.

Enable RADIUS ☑ RADIUS authentication proxy is not running
Enable authentication with RADIUS server.

4. The 'required configuration' errors you see are due to required data not being configured as yet – we will get to that later on.

Primary RADIUS Server



Primary RADIUS Server

Server Hostname or IP address | Port

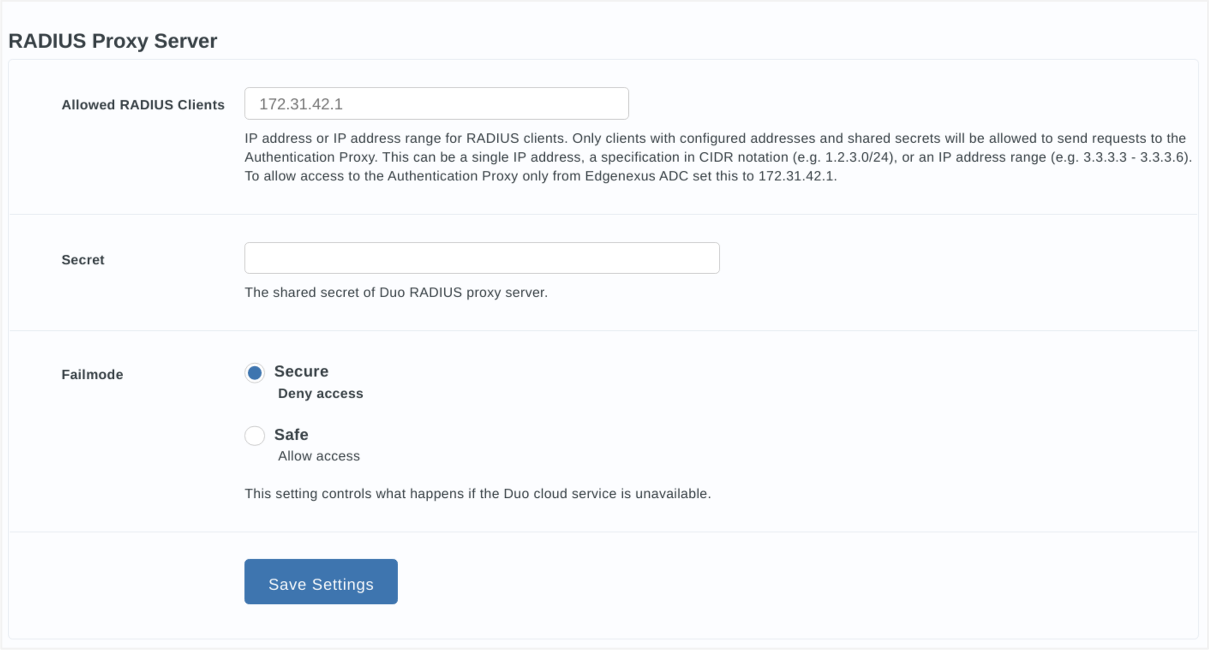
Hostname and port of your RADIUS server. The port is typically 1812.

Secret

The shared secret of your RADIUS server.

5. In the Primary RADIUS Server section shown below, fill in the RADIUS server hostname or IP address, together with the Port. Typically the port number is 1812.
6. You will also need to provide the Secret key value.
7. Click on Save Settings once this is done.

Radius Proxy Server



RADIUS Proxy Server

Allowed RADIUS Clients 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

The shared secret of Duo RADIUS proxy server.

Failmode

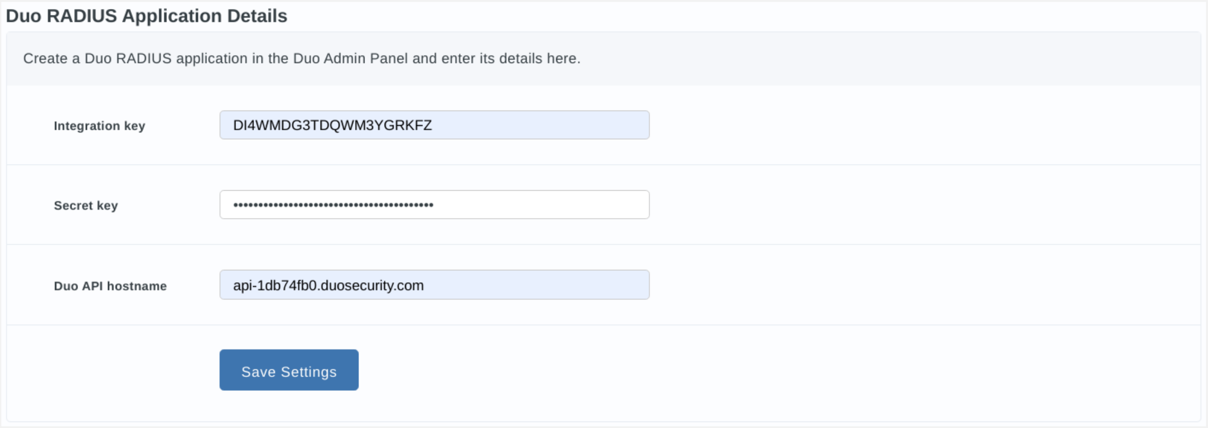
● **Secure**
Deny access

○ **Safe**
Allow access

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

8. In the Allowed RADIUS Clients field, you will need to specify an IP address or a range of IP addresses of the RADIUS clients allowed to connect to your CDAP installation. You would like to allow access to the RADIUS proxy only from the ADC in the simplest case. Communications between the ADC and its installed Add-ons are performed over the virtual Docker network within the ADC.
   The ADC IP address on the Docket network is displayed as a hint in the Allowed RADIUS Clients field before any input. Please use this IP address.
9. Please enter a suitable password in the Secret field that the RADIUS clients must use when connecting to the CDAP. We will use this password when configuring the Edgenexus ADC for RADIUS authentication.
10. The choice of Failmode setting determines whether access should be allowed if the Cisco Duo Cloud becomes unavailable.

Duo RADIUS Application Details



Duo RADIUS Application Details

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

Integration key: DI4WMDG3TDQWM3YGRKFZ

Secret key: ••

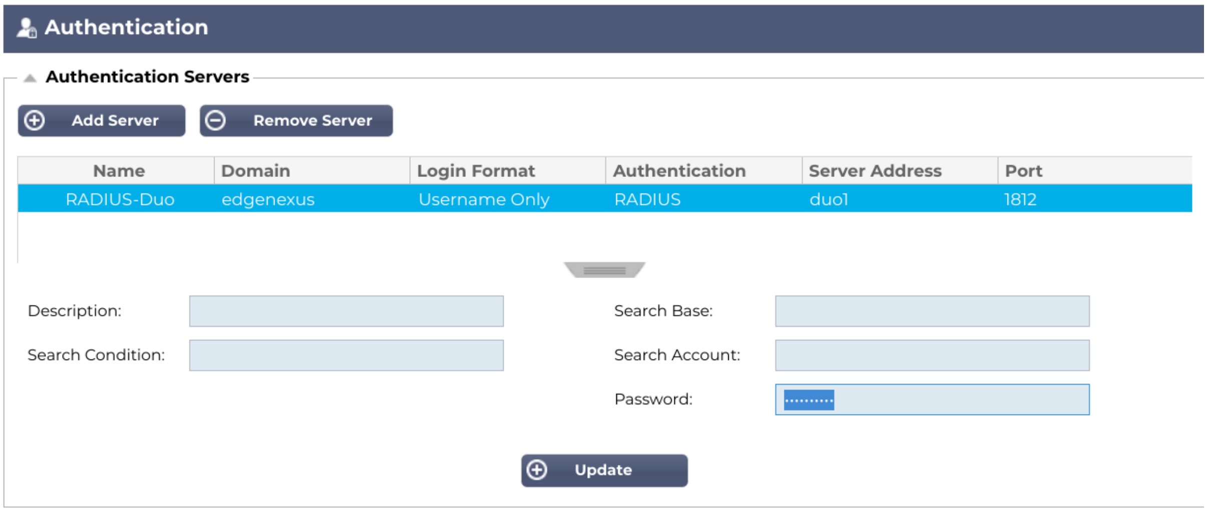
Duo API hostname: api-1db74fb0.duosecurity.com

11. Enter the Integration Key and Secret Key available from the Applications page on the Duo Admin Panel.
12. Click the Save Settings button once this is done.
13. If all is configured and connecting successfully, you will get a Success message. Any errors indicate that there could be a problem in the configuration that you need to correct.

Configuring the ADC for Duo with RADIUS Authentication

Now come the steps to configure the ADC so that users can authenticate using RADIUS and Cisco Duo. The guide will now assume that you are familiar with the ADC and its configuration methods and features.

Authentication Servers



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

Description:

Search Condition:

Search Base:

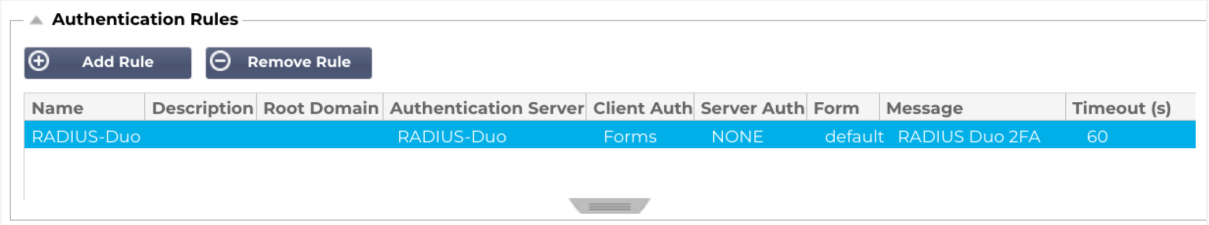
Search Account:

Password: ••••••••••

1. Proceed to Library > Authentication using the navigation panel of the ADC
2. You will now see the Authentication Servers section on the right panel.
3. Click Add Server
4. A new area will appear, showing fields that you will need to fill in. An example of the filled-in fields is shown below.

Field Name	Example and description
Name	The name can be any alphanumeric value, but for ease of understanding, let's use RADIUS-Duo
Domain	The value here should be your domain
Description	Optional, this value describes this entry
Login format	Select 'Username and Password' from the drop-down
Authentication	Select RADIUS from the drop-down
Server	The value you provide here should be the same as the name you gave your Cisco Duo Authentication Proxy – **this is important**.
Port	1812 is the standard Port used
Password	The RADIUS Secret
Search	Left blank
Search Base	Left blank

Authentication Rules



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

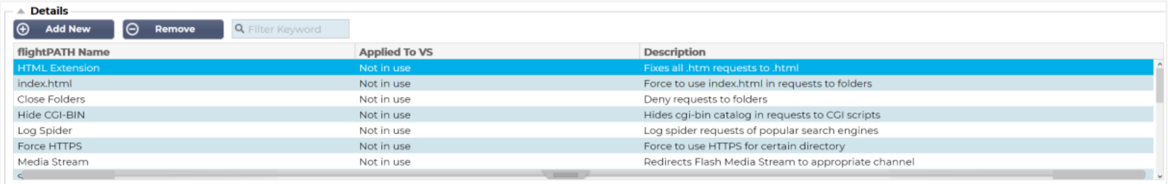
5. The next step is to create an authentication rule to handle the requests for Duo authentication. See the example below. Fill in the fields as explained in the table below the image.

Field Name	Explanation
Name	Add a suitable name for the rule – it could be something like RADIUS-Duo-Rule.
Description	Optional, this is the description for the rule.
Root Domain	Optional, unless you wish to use single-sign-on across sub-domains.
Authentication Server	A drop-down field – select the name of the Authentication Server you created in the previous steps.
Client Authentication	A drop-down field – select Forms
Server Authentication	A drop-down field – select None
Form	A drop-down field – select Default
Message	Will use the value to display a message on the form shown to the user. An example may be "RADIUS-Duo 2FA."
Timeout	The value is specified in seconds, after which the user will need to authenticate again.

Creating the flightPATH rule

For the Cisco Duo authentication to work correctly through the CDAP, we need to create a traffic management rule using fightPATH. The ADC will redirect the data received into the Virtual Service to the CDAP engine for action.

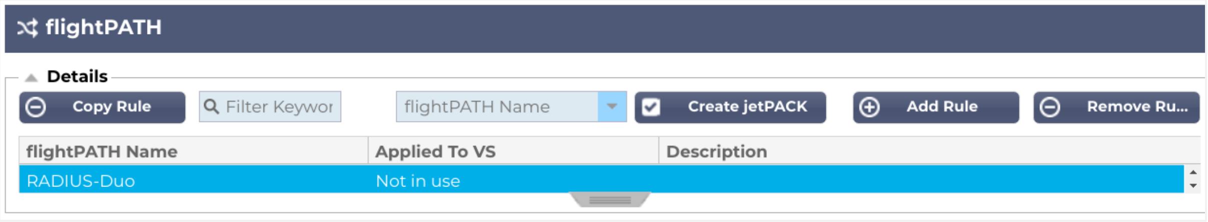
9. Navigate to Library > flightPATH using the left-side navigation pane.
10. You will see the flightpath configuration panel on the right of the navigation pane. There are some predefined rules in the Details section, but for Duo, we will be creating a new and straightforward rule.



flightPATH Name	Applied To VS	Description
HTML Extension	Not in use	Fixes all .htm requests to .html
index.html	Not in use	Force to use index.html in requests to folders
Close Folders	Not in use	Deny requests to folders
Hide CGI-BIN	Not in use	Hides cgi-bin catalog in requests to CGI scripts
Log Spider	Not in use	Log spider requests of popular search engines
Force HTTPS	Not in use	Force to use HTTPS for certain directory
Media Stream	Not in use	Redirects Flash Media Stream to appropriate channel

11. Click the Add New button located at the top left of the Details section.

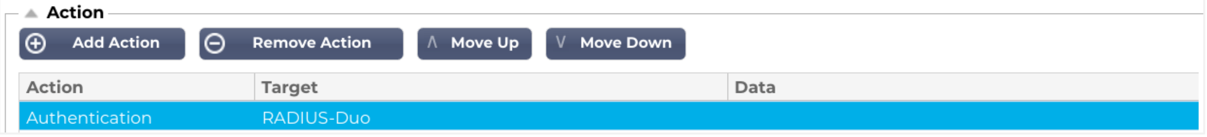
12. A new line for adding the flightPATH detail line will be shown.



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

Field	Description
flightPATH Name	This field represents the name you will give the flightPATH rule, and it is referred to within drop-down menus elsewhere in the GUI.
Applied to VS	Auto populated when you apply the rule to a Virtual Service
Description	The description is a plain language description to allow you to remember what the flightPATH rule was designed for

13. For this exercise, we have named the flightPATH rule as RADIUS-Duo
14. In this guide, we are not going to use any Conditions or Evaluations. You could, for example, configure a Condition that only allows access to the authentication form from a specific IP or subnet, or if you only want to challenge users that access a specific path such as '/secure.' More information on flightPATH can be found in the EdgeADC administrator guide.
15. Next, we will configure what will happen next in the Actions section.



Action	Target	Data
Authentication	RADIUS-Duo	

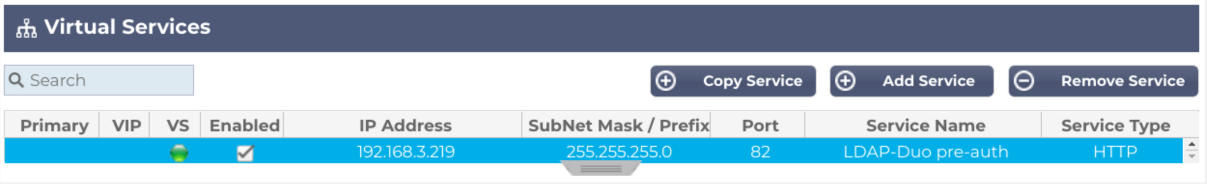
Field	Description
Action	This field informs what to do what the rule condition is met. In this case, the Action is Authentication.
Target	A drop-down field and the value you select here must be the Authentication Server you created, in this case, RADIUS-Duo.
Data	Leave blank

Creating the Cisco Duo Virtual Service

To make use of the Cisco Dup Authentication Proxy (CDAP), we need to create the Virtual IP (VIP) and Virtual Service (VS). It is this VIP that users will aim their browsers to access the software.

Creating the VIP/VS

17. Navigate to Services > IP Services using the left-side navigation panel.
18. The IP Services panel will be shown on the right side.
19. The IP Services panel consists of 2 main sections: Virtual Services and Real Servers.



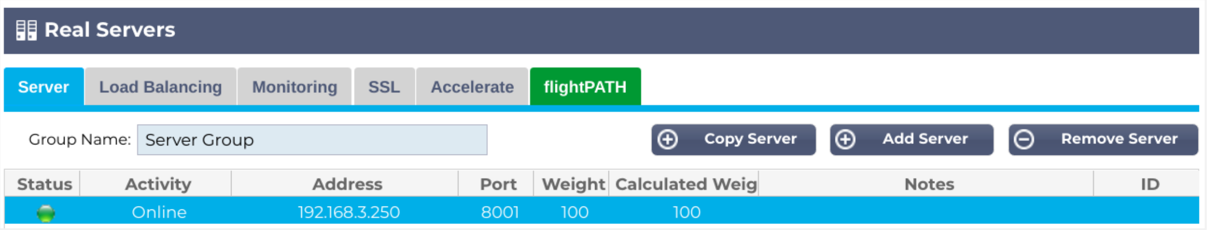
Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
		●	☑	192.168.3.219	255.255.255.0	82	LDAP-Duo pre-auth	HTTP

20. Click the Add Service button in the Virtual Services section. Fill in the details that are relevant to your network infrastructure. We have highlighted the areas you need to specify in GREEN. Remember to set the Service Type as HTTP.

Field	Description
Primary/Mode	An auto-populated field that indicates whether the VIP is Active, In Drain, or Disabled
VIP	A visual indicator that displays in a variety of colors to show the status of the VIP. See Admin Guide.
VS	A visual indicator that displays in a variety of colors to show the status of the VS. See Admin Guide.
Enabled	A checkbox used to enable or disable the VIP/VS
IP Address	The IP address that users will use to access the software – Please add the IP address you are going to use
Subnet Mask/Prefix	The relevant and applicable subnet mask for your network segment
Port	The Port that the users will specify in the URL (in our example, we are using 82)
Service Name	A short name for the VIP/VS
Service Type	This drop-down should be set to **HTTP** as we are going to use a flightPATH rule

21. Now we will start configuring the Real Servers section.

Real Servers



Group Name: Server Group

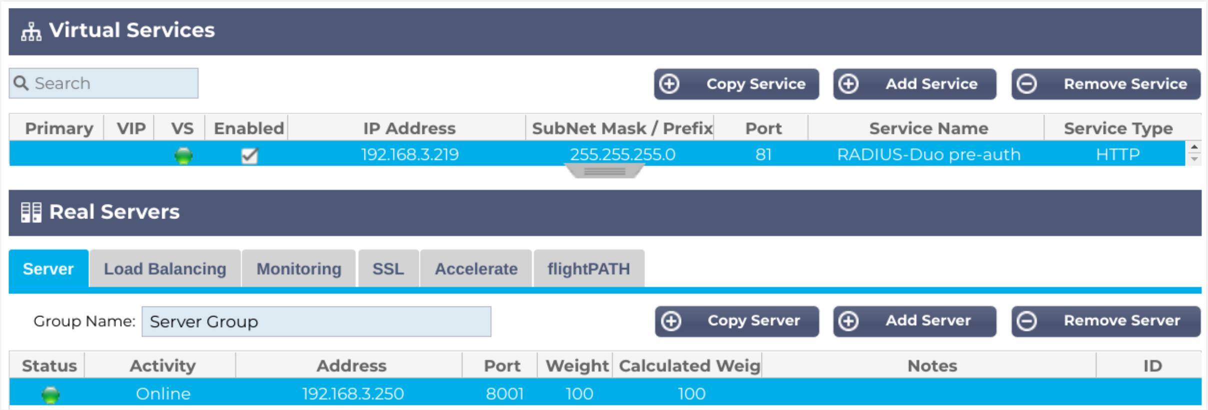
Status	Activity	Address	Port	Weight	Calculated Weig	Notes	ID
●	Online	192.168.3.250	8001	100	100		

The Server Tab

The Server Tab is used to specify the Real Server or load-balanced set of Real Servers you are trying to protect with Cisco Duo 2FA. In our example, there is only a single server.

Field	Description
Status	This indicator will display the current status of the connection to the Real Server. See the administration guide for the meaning of status colors.
Activity	Will show whether the Real Server is online or not
Address	The IP Address of the Real Server
Port	The Port configured for accessing the Real Server and its software
Weighting	This field can be configured if required, but we recommend that you let the ADC handle this.
Notes	This field describes Real Server and any relevant notes.

22. Fill in the details shown in GREEN per your requirements.
23. Once you have done that, the Status indicator should light up Green, and the VIP and VS lights on the Virtual Services section. If they are not Green, this indicates there may be an issue with connectivity or configuration. An example of this is shown below.

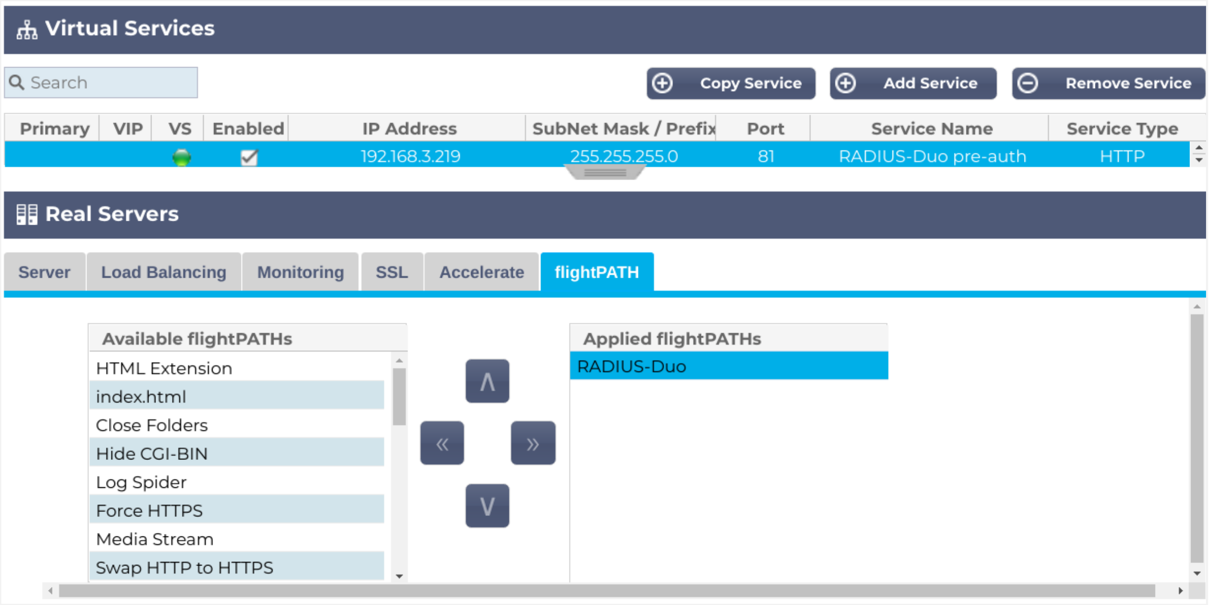


Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
		●	☑	192.168.3.219	255.255.255.0	81	RADIUS-Duo pre-auth	HTTP

Group Name: Server Group

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

24. Now click the flightPATH tab. You will see the flightPATH details as shown below.



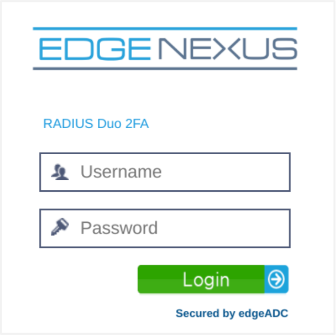
Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
		●	☑	192.168.3.219	255.255.255.0	81	RADIUS-Duo pre-auth	HTTP

25. Please scroll down the Available flightPATHs until you see the RADIUS-Duo rule we created.

26. Select the rule and click the right arrow button in the central area.
27. The flightPATH rule will be moved to the Applied flightPATH segment on the right of the arrow buttons.
28. The rule is immediately applied and is operational.

The Cisco Duo Authentication Proxy has now been installed and is fully operational. The Real Server(s) specified in the Real Servers section are now protected using Cisco Duo authentication using the CDAP engine.

Users navigating the http://192.168.3.219:82, in our example, will see the dialog for authentication shown below. The IP address and Port that you may use will almost definitely be different, perhaps using Port 443.

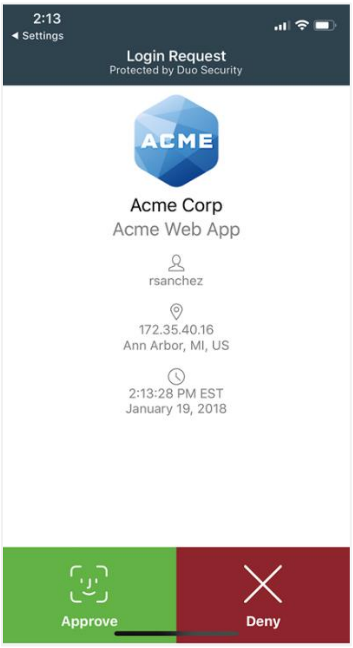


EDGENEXUS

RADIUS Duo 2FA

Secured by edgeADC

29. Enter the username and password of the test user you created in your RADIUS server and the Duo Admin Panel.
30. If the credentials pass RADIUS authentication, you will soon get a confirmation request in the Cisco Duo Mobile App on the phone associated with the Duo test user. It will look something like the example below.



Login Request
Protected by Duo Security

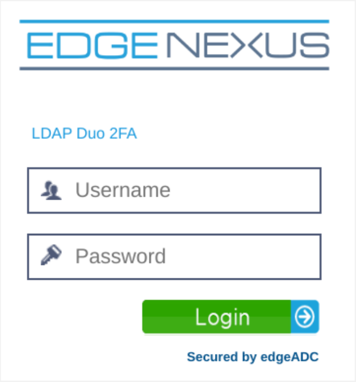
Acme Corp
Acme Web App

rsanchez

172.35.40.16
Ann Arbor, MI, US

2:13:28 PM EST
January 19, 2018

31. If you Approve the request, you will be connected to the Real Server configured for the VIP. If you choose to Deny the confirmation request, you will see the login page again along with an error stating the username and/or password are incorrect.



32. Guides for the iOS and Android phone Apps are available here:
    a. Cisco Duo App User Guide for Apple iOS
    b. Cisco Duo App User Guide for Android

Synchronizing the Cisco Duo Directory

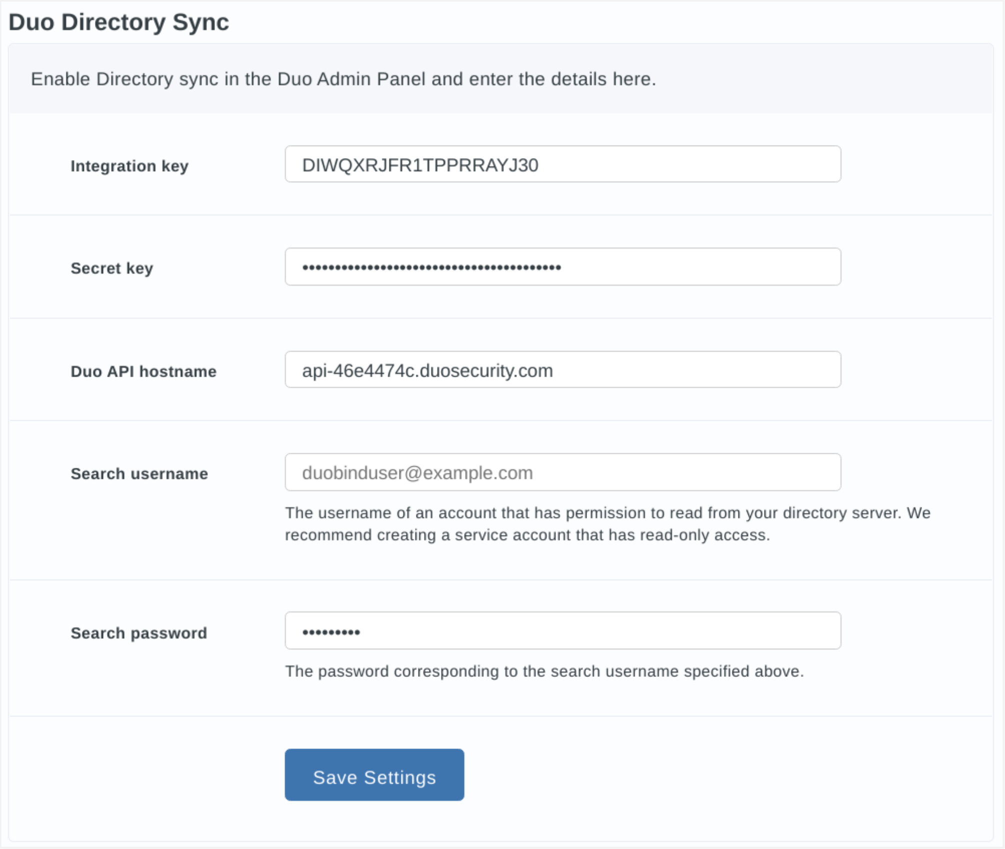
This feature from Cisco Duo allows you to import all the usernames and other information from your Active Directory (AD) Forest, Domain, or Active Directory Lightweight Directory Service (AD LDS) instance into Duo with Duo Security's Directory Sync feature.

A one-way operation, the process ensures that no information from Duo is copied to your AD. The sync process runs daily or can be run on demand using programmatic techniques via the Duo API.

Read the Synchronizing Users from Active Directory article before attempting to handle the Sync process. The article can be found here.

Starting the Duo Directory Sync Process

1. Follow the steps to setting up Sync services until you come to the Duo Authentication Proxy installation and configuration section, called Authentication Proxy (https://duo.com/docs/adsync#authentication-proxy).
2. Ensure you have the Integration Key, Secret Key, and Duo API Hostname details.
3. Fill in these details in the Duo Directory Sync section within the Duo Admin Panel's Authentication Proxy Add-On GUI.



Duo Directory Sync

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

Integration key: DIWQXRJFR1TPPRRAYJ30

Secret key: ••

Duo API hostname: api-46e4474c.duosecurity.com

Search username: 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: •••••••••

The password corresponding to the search username specified above.

4. Click Save Settings. You should get a Success message.
5. Carry on with the instructions in the Synchronizing Users from Active Directory article until done.

Technical Support

Should you require technical support setting up Cisco Duo on your EdgeADC, please email support@edgenexus.io, and one of our support engineers will contact you to assist.