AppGate SDP

AppGate SDP and Duo Authentication Integration Guide

V2.0
Tested for use on versions:
AppGate SDP v5.0 or newer
Last updated: March 2020

AppGate SDP – Duo Authentication: Integration Guide
Copyright © 2020 Cyxtera Cybersecurity, Inc. d/b/a AppGate

All rights reserved. AppGate is a trademark of Cyxtera Cybersecurity, Inc. d/b/a AppGate.
All other product names mentioned
herein are trademarks of their respective owners

TABLE OF CONTENTS

INTRODUCTION 3
BEFORE YOU START 3
STEP BY STEP GUIDE 4
1. DUO PROXY SERVER CONFIGURATION: 4
2. APPGATE SDP CONFIGURATION: ADDING A NEW MFA PROVIDER 4
3. TESTING INTEGRATION 5
USING DUO MFA AUTHENTICATION 6
1. User authentication 6
2. Device enrolment 6
3. User interactions 6
4. MFA for Admins 7
5. On-boarding new devices 8
TROUBLESHOOTING 8
HELP AND SUPPORT....................10
FEEDBACK 10

Copyright © 2020 AppGate

INTRODUCTION

Multi-factor authentication can be used for controlling user access to network resources, administrator access to the Admin UI, and new device on-boarding.

AppGate SDP can be configured to utilize either the built in default time-based OTP provider, FIDO provider or an external RADIUS provider.
This document refers to the settings required to use Duo Authentication as an external RADIUS authentication provider.

BEFORE YOU START

Test topology

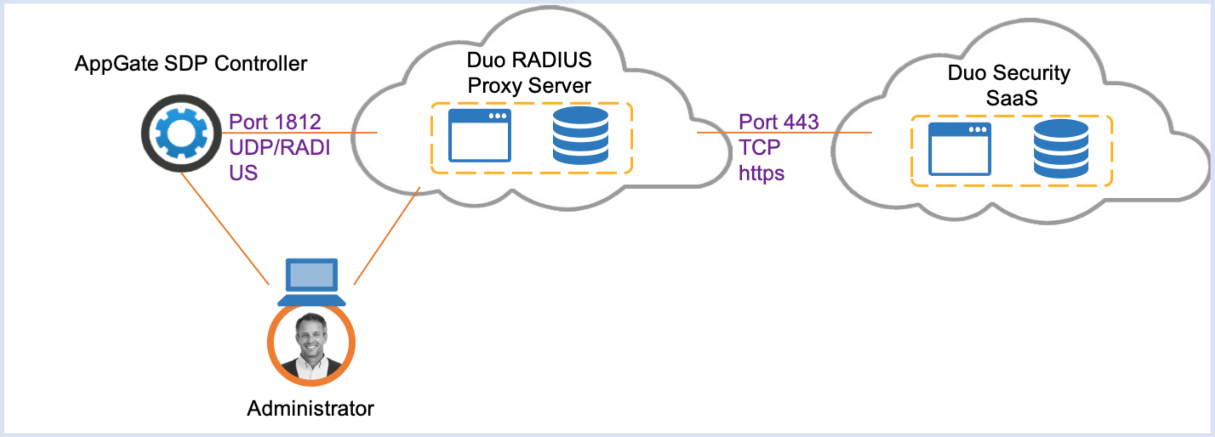


Figure 1: Duo integration test topology

This integration requires the following:

- A Duo Security account configured for RADIUS protection
- A Duo Authentication Proxy server installed and accessible on your network. Information for setting up and configuring a Duo Authentication Proxy can be found here: https://duo.com/docs/radius
- a test user account setup on your identity provider database
- An AppGate SDP Controller installed and accessible on your network. Information for setting up your Controller can be found in the Admin UI: https://help.appgate.com/adminguide/index.html

Information you will need:

- From your Duo Security account:
  - hostname/IP address, integration key, secret key, and API hostname
- From your Duo Authentication Proxy:
  - Hostname/IP address of the proxy host
- From your AppGate SDP console:
  - Controller appliance IP address

Copyright © 2020 AppGate

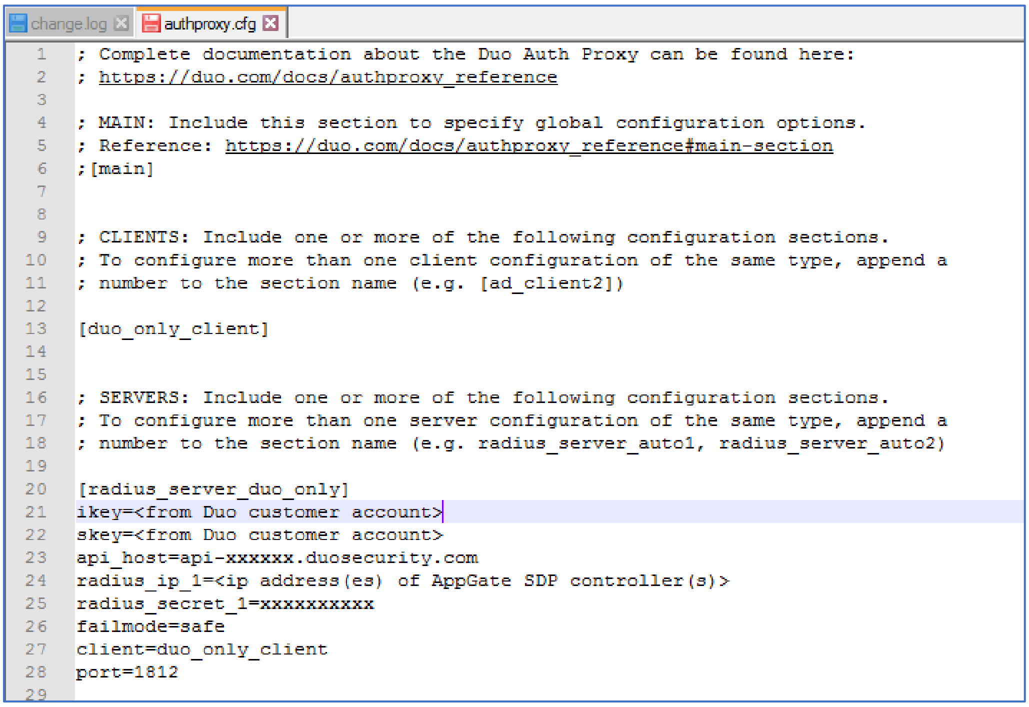
STEP BY STEP GUIDE

1. DUO PROXY SERVER CONFIGURATION:

Open the config file for your Duo Authentication Proxy server and edit the following fields:

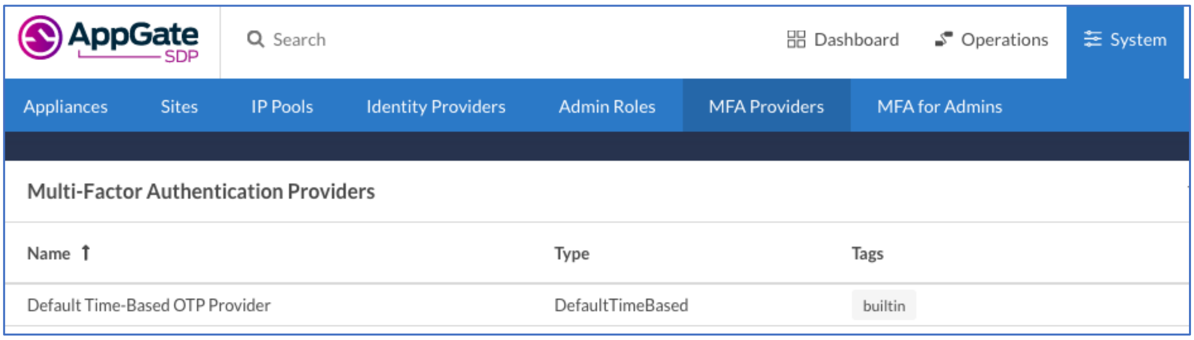
- *ikey* – enter the Integration Key from your Duo account
- *skey* – enter the Secret Key from your Duo account
- *api host* – enter the API hostname from your Duo account
- *radius_secret_1* – enter a secret to be shared with the AppGate SDP Controller
- *radius_ip_1* – enter the IP address of your AppGate SDP Controller
- *Client* – select the option ‘duo_only_client’ (do not perform primary authentication)
- *Port* – enter 1812

A completed config file would look something like this:



```
; Complete documentation about the Duo Auth Proxy can be found here:
; https://duo.com/docs/authproxy_reference

; MAIN: Include this section to specify global configuration options.
; Reference: https://duo.com/docs/authproxy_reference#main-section
;[main]


; CLIENTS: Include one or more of the following configuration sections.
; To configure more than one client configuration of the same type, append a
; number to the section name (e.g. [ad_client2])

[duo_only_client]


; SERVERS: Include one or more of the following configuration sections.
; To configure more than one server configuration of the same type, append a
; number to the section name (e.g. radius_server_auto1, radius_server_auto2)

[radius_server_duo_only]
ikey=<from Duo customer account>
skey=<from Duo customer account>
api_host=api-xxxxxx.duosecurity.com
radius_ip_1=<ip address(es) of AppGate SDP controller(s)>
radius_secret_1=xxxxxxxxxx
failmode=safe
client=duo_only_client
port=1812

```

2. APPGATE SDP CONFIGURATION: ADDING A NEW MFA PROVIDER



Multi-Factor Authentication Providers

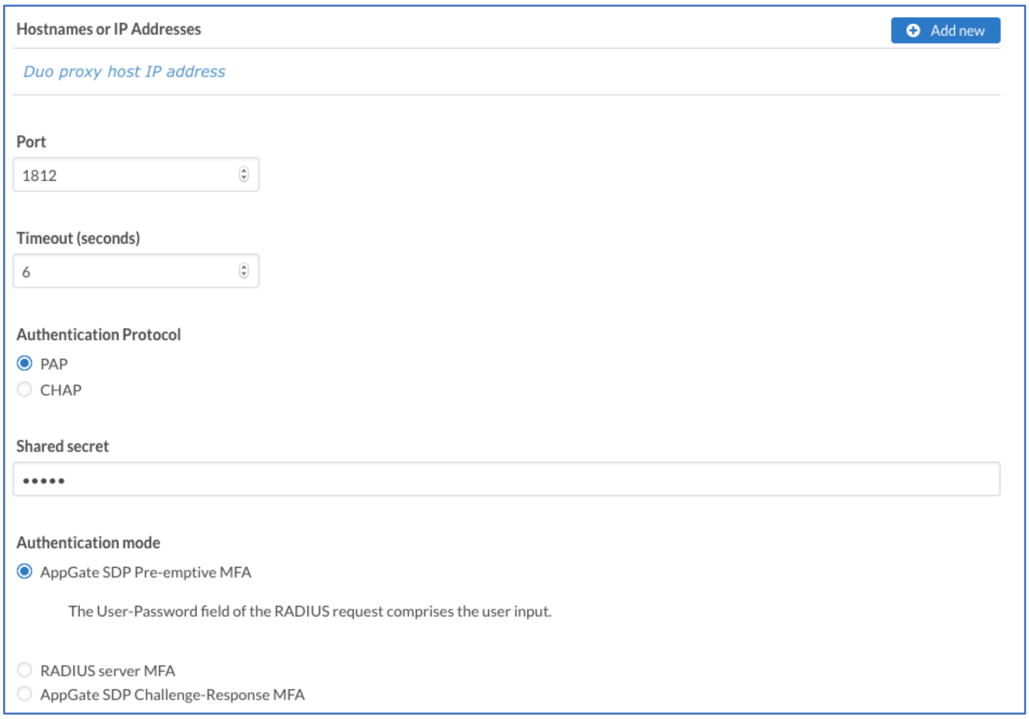
Name ↑	Type	Tags
Default Time-Based OTP Provider	DefaultTimeBased	builtin

Copyright © 2020 AppGate

In your AppGate SDP console, select System > MFA Providers

- create a new MFA Provider
- for the following fields select these options:
  - *Hostnames or IP Addresses* – enter the Hostname/IP address of the proxy host
  - *Port* – enter 1812
  - Authentication Protocol – select 'PAP'
  - *Shared secret* – enter the same shared secret that was entered in the Duo Proxy config file
  - *Authentication mode* – select 'AppGate SDP Pre-emptive MFA'

The completed form should look like this:



Hostnames or IP Addresses

Duo proxy host IP address

Port

1812

Timeout (seconds)

6

Authentication Protocol

● PAP

○ CHAP

Shared secret

•••••

Authentication mode

● AppGate SDP Pre-emptive MFA

The User-Password field of the RADIUS request comprises the user input.

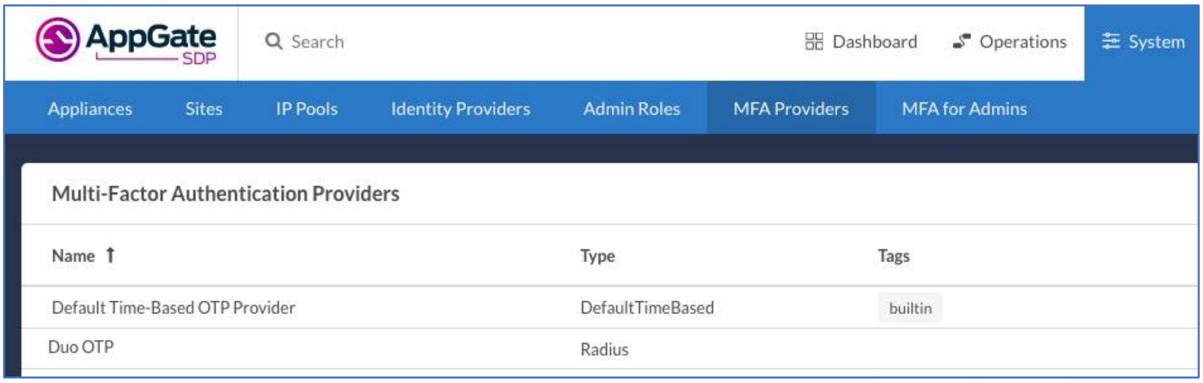
○ RADIUS server MFA

○ AppGate SDP Challenge-Response MFA

3. TESTING INTEGRATION

After completing the MFA Provider form on the AppGate SDP console:

- Save the configuration
- Use the <Test Connection> button to test system integration.
- If the test is successful, your Duo provider should now be listed on the MFA Provider console



Multi-Factor Authentication Providers

Name ↑	Type	Tags
Default Time-Based OTP Provider	DefaultTimeBased	builtin
Duo OTP	Radius	

Copyright © 2020 AppGate

USING DUO MFA AUTHENTICATION

Once your MFA Provider has been configured, you can use it for controlling user access to network resources, authenticating administrators logging in to the Admin UI, and on-boarding new devices.

1. User authentication

Once integration has been completed successfully, user experience will depend on which authentication mode you select on your AppGate SDP, and the authentication method that is chosen when the user enrolls with your RADIUS server.

AppGate SDP Authentication Modes:
AppGate SDP external RADIUS support includes:

- Pre-emptive MFA: the user will be prompted by the AppGate SDP client for authentication response, which the RADIUS server validates.
- RADIUS server MFA: Often referred to as Push OTP. The RADIUS server initiates the required challenge and response.
- Challenge-Response MFA: the RADIUS server may initiate an action, such as sending an SMS, and asks the AppGate SDP Client to prompt the user for an authentication response.

Authentication mode is configured in the AppGate SDP console, simply edit the configuration for your MFA provider and choose the required mode.
For more information about RADIUS provider authentication modes refer to the Admin Guide > MFA Providers

2. Device enrolment

- Each user authentication device (eg. cell phone or security key) must be pre-enrolled with your RADIUS server before MFA authentication can be used.
- Provide any training required for users to self-enrol with the MFA provider and / or to use the authentication device

Unlike the built-in time-based OTP provider where setup of the authenticator app on the user's mobile device is handled automatically by AppGate SDP, device enrolment for RADIUS MFA providers is not automated and needs to be managed separately.
For more details refer to: Duo > Add Device and Duo Self-Enrolment.

3. User interactions

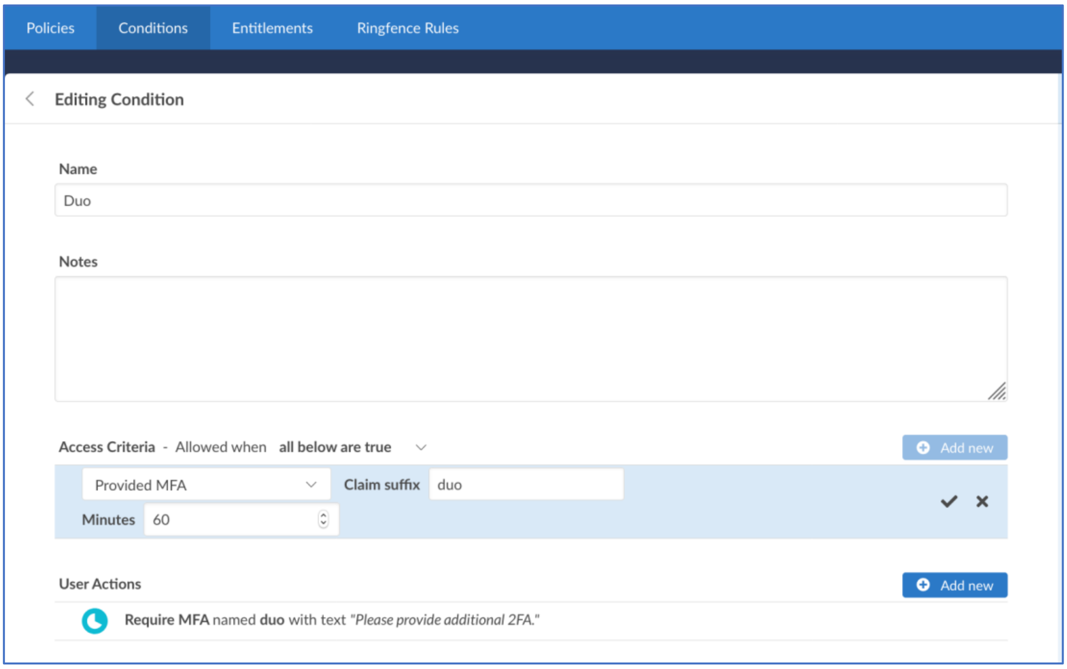
AppGate SDP uses MFA in Conditions combined with user interactions to control conditional access to specific network resources.
MFA methods are configured within Conditions.

On your AppGate SDP Admin UI:

- Open the Condition configuration form, edit the following fields:
  - *User Interaction* – select <Require MFA>
  - *Message* - enter “%RADIUS_MESSAGE%” to use the reply-message (24) from the Duo server
  - *MFA Provider* – Choose the required MFA provider from the drop-down list.

Copyright © 2020 AppGate

The Condition form should look like this:



Editing Condition

Name: Duo

Notes:

Access Criteria - Allowed when all below are true

Provided MFA — Claim suffix: duo — Minutes: 60

User Actions

Require MFA named duo with text *"Please provide additional 2FA."*

Once configured, use this Condition in any user Entitlements requiring MFA authentication.

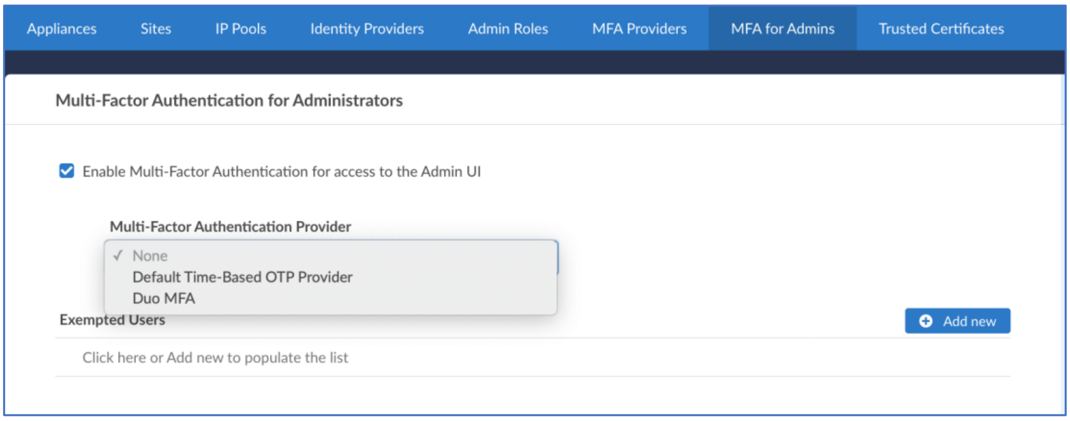
For more information refer to the Admin Guide, What is a user interaction and Configuring user interactions.

4. MFA for Admins

Multi-factor authentication can be mandated for system administrators to control access to the Admin UI. MFA for administrators is strongly recommended to control port 444 (or 8443) access to the Admin UI from the internal network. Where administrators are connecting to the Admin UI through AppGate SDP from an external network, include MFA in the appropriate Entitlement (see above).

On your AppGate SDP Admin UI:

- On the **System > MFA For Admins** console, edit the following fields:
  - Enable Multi-Factor Authentication – tick the box
  - *Multi-Factor Authentication Provider* – Choose the required MFA provider from the drop-down list.



Multi-Factor Authentication for Administrators

☑ Enable Multi-Factor Authentication for access to the Admin UI

Multi-Factor Authentication Provider

✓ None
Default Time-Based OTP Provider
Duo MFA

Exempted Users

Click here or Add new to populate the list

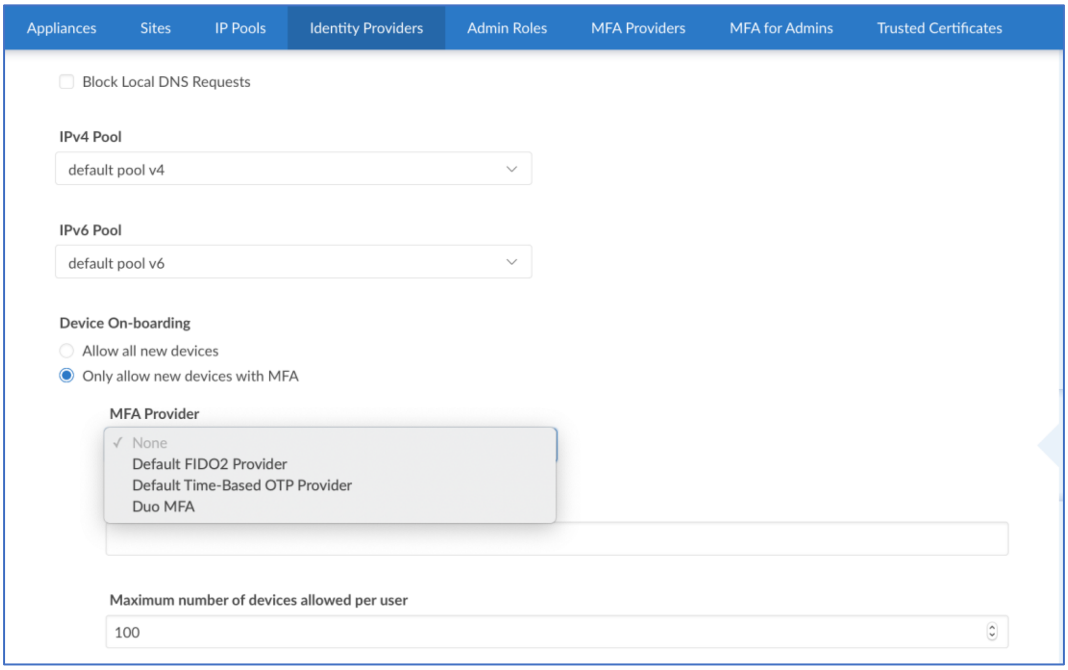
For more information refer to: Configuring MFA for Admins

Copyright © 2020 AppGate

5. On-boarding new devices

AppGate SDP has the option to restrict which devices are allowed to connect to the system. This is specifically aimed at preventing one of the most common forms of breach, namely when stolen credentials are used (from a new device).
The most usual mode of operation is <**Require Multi-factor authentication>** which means a user can on-board their own devices but will be required to provide additional authentication the first time.

- On your AppGate SDP Admin UI, in the Identity Provider configuration form, edit the following fields:
  - *On-boarding mode* – select <Require Multi-Factor authentication>
  - *On-boarding MFA Provider* – Choose the required MFA provider from the drop-down list.



□ Block Local DNS Requests

IPv4 Pool: default pool v4

IPv6 Pool: default pool v6

Device On-boarding
○ Allow all new devices
● Only allow new devices with MFA

MFA Provider
✓ None
Default FIDO2 Provider
Default Time-Based OTP Provider
Duo MFA

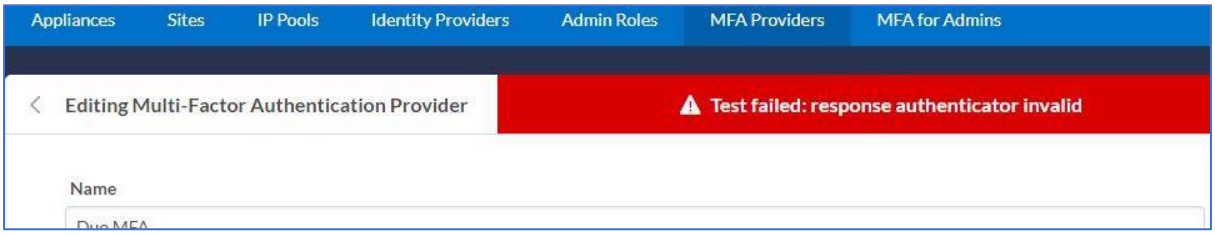
Maximum number of devices allowed per user: 100

For more information refer to: [Configure Identity Providers]()

TROUBLESHOOTING

1. Integration test error: configuration / networking issues

If there is a problem with the Integration test, AppGate SDP will display an error message incorporating any error information from the Duo Proxy server.
In the example below, <Test Connection> returned the following error:



Editing Multi-Factor Authentication Provider

⚠ Test failed: response authenticator invalid

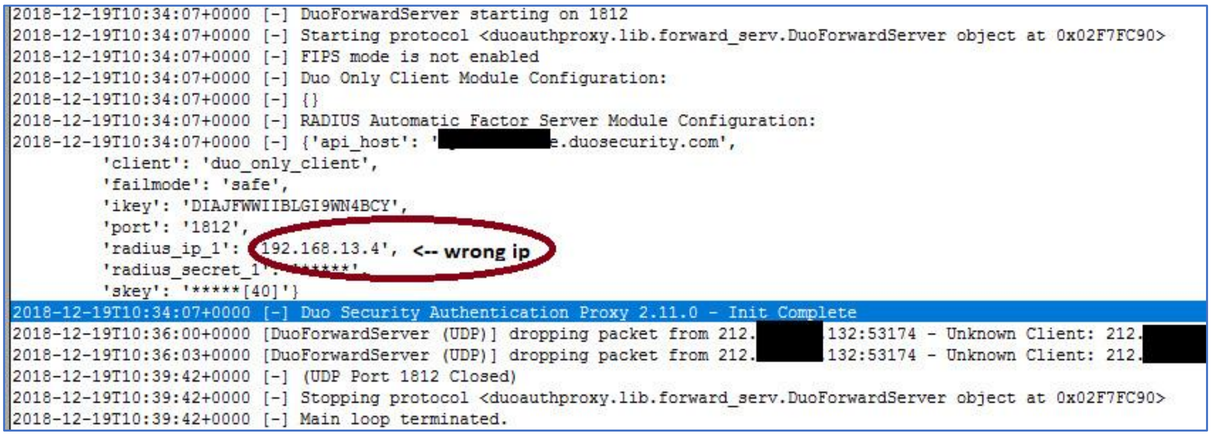
Name: Duo MFA

Copyright © 2020 AppGate

To find the source of the error you have two options:

Use the Duo log file to find the possible source of the problem.

The Duo Proxy logfile shows the source of the error: in this case there is an error in the Duo configuration for field *radius_ip_1* where the wrong IP address for the AppGate SDP Controller has been entered.

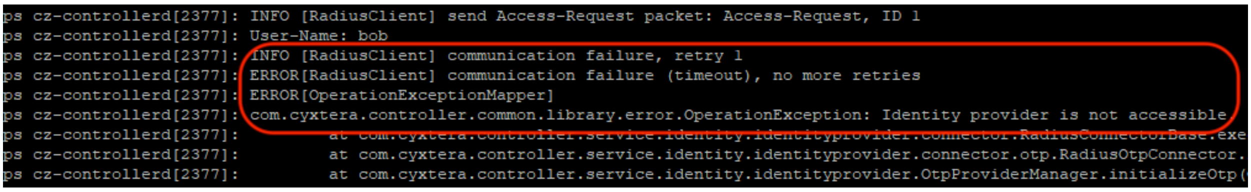


```
2018-12-19T10:34:07+0000 [-] DuoForwardServer starting on 1812
2018-12-19T10:34:07+0000 [-] Starting protocol <duoauthproxy.lib.forward_serv.DuoForwardServer object at 0x02F7FC90>
2018-12-19T10:34:07+0000 [-] FIPS mode is not enabled
2018-12-19T10:34:07+0000 [-] Duo Only Client Module Configuration:
2018-12-19T10:34:07+0000 [-] {}
2018-12-19T10:34:07+0000 [-] RADIUS Automatic Factor Server Module Configuration:
2018-12-19T10:34:07+0000 [-] {'api_host': '[redacted]e.duosecurity.com',
        'client': 'duo_only_client',
        'failmode': 'safe',
        'ikey': 'DIAJFWWIIBLGI9WN4BCY',
        'port': '1812',
        'radius_ip_1': '192.168.13.4',  <-- wrong ip
        'radius_secret_1': '******'
        'skey': '*****[40]'}
2018-12-19T10:34:07+0000 [-] Duo Security Authentication Proxy 2.11.0 - Init Complete
2018-12-19T10:36:00+0000 [DuoForwardServer (UDP)] dropping packet from 212.[redacted]132:53174 - Unknown Client: 212.[redacted]
2018-12-19T10:36:03+0000 [DuoForwardServer (UDP)] dropping packet from 212.[redacted]132:53174 - Unknown Client: 212.[redacted]
2018-12-19T10:39:42+0000 [-] (UDP Port 1812 Closed)
2018-12-19T10:39:42+0000 [-] Stopping protocol <duoauthproxy.lib.forward_serv.DuoForwardServer object at 0x02F7FC90>
2018-12-19T10:39:42+0000 [-] Main loop terminated.
```

Use the AppGate SDP *controllerd* debug log to find the source of the error.

- Launch the terminal window and enter the command: journalctl -u cz-controllerd -f
- Try to login to the Controller Admin UI using your SAML IdP and watch the controllerd log
- You may see something like this:

  Jan 21 10:14:01 envy-172-17-112-1.devops cz-controllerd[2377]: ERROR[OperationExceptionMapper]
  Jan 21 10:14:01 envy-172-17-112-1.devops cz-controllerd[2377]: com.cyxtera.controller.common.library.error.OperationException: Identity provider is not accessible.

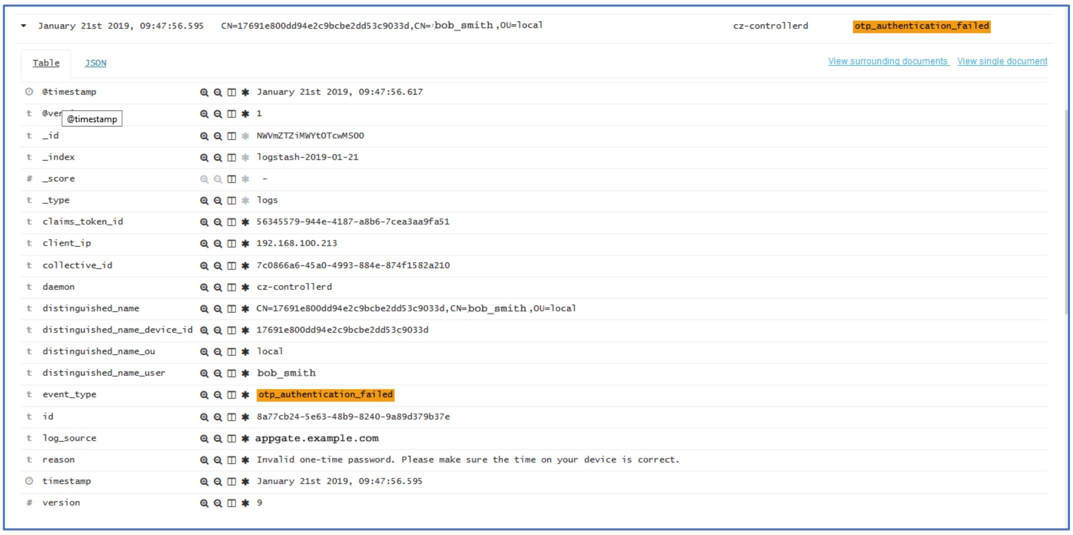


```
ps cz-controllerd[2377]: INFO [RadiusClient] send Access-Request packet: Access-Request, ID 1
ps cz-controllerd[2377]: User-Name: bob
ps cz-controllerd[2377]: INFO [RadiusClient] communication failure, retry 1
ps cz-controllerd[2377]: ERROR[RadiusClient] communication failure (timeout), no more retries
ps cz-controllerd[2377]: ERROR[OperationExceptionMapper]
ps cz-controllerd[2377]: com.cyxtera.controller.common.library.error.OperationException: Identity provider is not accessible
ps cz-controllerd[2377]:         at com.cyxtera.controller.service.identity.identityprovider.connector.RadiusConnectorBase.exe
ps cz-controllerd[2377]:         at com.cyxtera.controller.service.identity.identityprovider.connector.otp.RadiusOtpConnector.
ps cz-controllerd[2377]:         at com.cyxtera.controller.service.identity.identityprovider.OtpProviderManager.initializeOtp(
```

Copyright © 2020 AppGate

2. User access error

If everything is set up correctly but there are issues with user or OTP, you can see the details of the failure on the AppGate SDP audit logs.
For example:



```
▾ January 21st 2019, 09:47:56.595   CN=17691e800dd94e2c9bcbe2dd53c9033d,CN=bob_smith ,OU=local        cz-controllerd        otp_authentication_failed

t  @timestamp                   January 21st 2019, 09:47:56.617
t  @ver                         1
t  _id                          NWVmZTZiMWYtOTcwMS00
t  _index                       logstash-2019-01-21
#  _score                        -
t  _type                        logs
t  claims_token_id              56345579-944e-4187-a8b6-7cea3aa9fa51
t  client_ip                    192.168.100.213
t  collective_id                7c0866a6-45a0-4993-884e-874f1582a210
t  daemon                       cz-controllerd
t  distinguished_name           CN=17691e800dd94e2c9bcbe2dd53c9033d,CN=bob_smith ,OU=local
t  distinguished_name_device_id 17691e800dd94e2c9bcbe2dd53c9033d
t  distinguished_name_ou        local
t  distinguished_name_user      bob_smith
t  event_type                   otp_authentication_failed
t  id                           8a77cb24-5e63-48b9-8240-9a89d379b37e
t  log_source                   appgate.example.com
t  reason                       Invalid one-time password. Please make sure the time on your device is correct.
   timestamp                    January 21st 2019, 09:47:56.595
#  version                      9
```

If the user experiences an authentication problem:

- Check the logs on the user's device – they should include the error message that is returned by the RADIUS server.
- Check the logs on the Duo server.
- Ensure this Condition is included in the user access entitlement.
- Re-trigger the Client to start the OTP setup process again: the user needs to logout from the Client and log back in again

HELP AND SUPPORT

For more information about the next steps in setting up your AppGate SDP system, refer to the Admin Guide

Please visit the Help Center to browse the knowledge base or log a support ticket for all Cyxtera products. Learn more about the Help Center below.

Self-service help
Self-service help can be browsed or searched for technical solutions. Browse FAQs, known issues, best practices, service examples, guides and manuals.

Customer support requests
Customers can submit support requests in accordance with their Support and Maintenance contracts. We recommend that you sign in to the support portal and submit from your own support account. If you do not have access, please fill in the "request a login" form available on the Help Centre.

FEEDBACK

If there is any information in this Integration Guide that needs to be updated, or instructions that need further clarification, please let us know. Contact send your feedback to Send your feedback to the Help Center.

Copyright © 2020 AppGate