



CyberArk EPM Elevation MFA with Duo Security Integration Technical Documentation

Name of Company: Duo Security

Website: www.duo.com

Name of Product: Radius Authentication

Date: September 2019

OVERVIEW

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and Zero Trust for the Workforce provider. Duo's zero-trust security platform, Duo Beyond, enables organizations to provide secure access to all of their critical applications - for any user, from anywhere, and with any device.

This integration allows a user to take advantage of Duo's multifactor authentication capabilities when elevating privileges, by receiving a push or a token.

DUO CONFIGURATION

DUO APPLICATION

1. Sign up for a Duo account.
2. Log in to the Duo Admin Panel and navigate to **Applications**.
3. Click **Protect an Application** and locate **CyberArk Privileged Account Security LDAP/RADIUS** in the applications list. Click Protect this Application to get your integration key, secret key, and API hostname.



CyberArk Privileged Account
Security LDAP/RADIUS

[Protect this Application](#)

[Read the documentation](#)

CyberArk Privileged Account Security LDAP/RADIUS

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

See the [CyberArk documentation](#) to add Duo RADIUS or LDAP authentication to your Privileged Account Security Solution.

Details

[Reset Secret Key](#)

Integration key	DI4TK6OZTZPVXYQWHN2T	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	api-fb00ecce.duosecurity.com	select

4. Create and enroll your users. Make sure they're setup for Duo Mobile.

DUO AUTHENTICATION PROXY

These instructions need to be followed on the EPM server.

- 1) Download the most recent Authentication Proxy for Windows from <https://dl.duosecurity.com/duoauthproxy-latest.exe>. Note that the actual filename will reflect the version e.g. duoauthproxy-2.13.0.exe. View checksums for Duo downloads [here](#).
- 2) Launch the Authentication Proxy installer on the target Windows server as a user with administrator rights and follow the on-screen prompts.
- 3) Add the following parameters to the **C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg** file:

```
[radius_server_duo_only]
ikey=<YOUR INTERGRATION KEY>
skey=<YOUR SECRET KEY>
api_host=<YOUR API HOST>
radius_ip_1=< Where the Duo Authentication Proxy is installed>
radius_secret_1=< Choose a Radius Secret>
port=1812
```

- 4) Test your configuration:

```
C:\Program Files (x86)\Duo Security Authentication Proxy\bin\authproxy_connectivity_tool.exe
C:\Users\mike>"C:\Program Files (x86)\Duo Security Authentication Proxy\bin\authproxy_connectivity_tool.exe"
The filename, directory name, or volume label syntax is incorrect.

C:\Users\mike>"C:\Program Files (x86)\Duo Security Authentication Proxy\bin\authproxy_connectivity_tool.exe"
Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes...
[info] Testing section 'radius_server_duo_only' with configuration:
[info] {'api_host': 'api-eebf4855.duosecurity.com',
       'ikey': 'DIZWD6U4WX1WMJ84GILS',
       'port': '1812',
       'radius_ip_1': '10.0.1.61',
       'radius_secret_1': '*****',
       'skey': '*****[40]'}
[info] There are no configuration problems
[info] -----
[info] Testing section 'radius_server_duo_only' with configuration:
[info] {'api_host': 'api-eebf4855.duosecurity.com',
       'ikey': 'DIZWD6U4WX1WMJ84GILS',
       'port': '1812',
       'radius_ip_1': '10.0.1.61',
       'radius_secret_1': '*****',
       'skey': '*****[40]'}
[info] The RADIUS Server has no connectivity problems.
[info] -----
[info] SUMMARY
[info] No issues detected

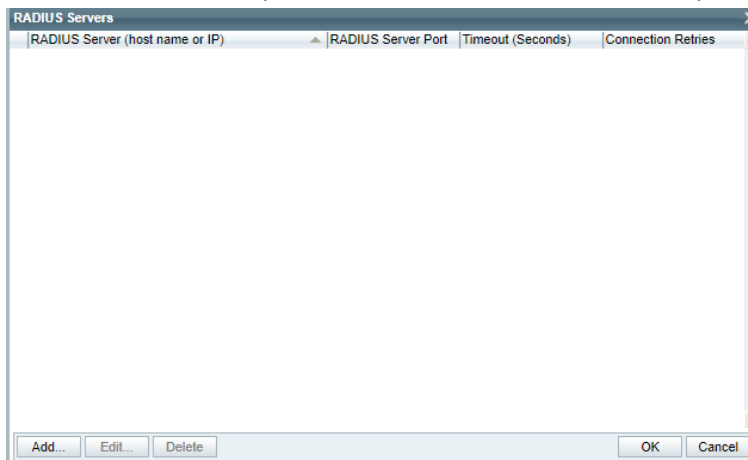
The results have also been logged in C:\Program Files (x86)\Duo Security Authentication Proxy\log\connectivity_tool.log
```

EPM CONFIGURATION

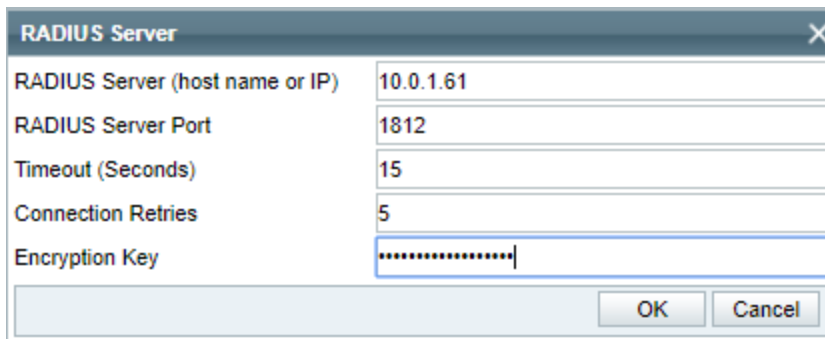
- 1) To configure the RADIUS Server, go to Advanced > Server Configuration tab of the CyberArk Endpoint Privilege Manager Server Management Console:



- 2) In the Radius Servers parameter, click the blue link that represents the current value, click Add:



- 3) Configure the following RADIUS Server parameters:

The 'RADIUS Server' configuration dialog box is shown with the following fields and values:

- RADIUS Server (host name or IP): 10.0.1.61
- RADIUS Server Port: 1812
- Timeout (Seconds): 15
- Connection Retries: 5
- Encryption Key: A masked field represented by a series of dots.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Where:

RADIUS Server (host name or IP): Where you installed the Duo proxy. In our case the EPM server.

RADIUS Server Port: This should be filled in, if not enter 1812.

Timeout: Leave the default

Connection Retries: Leave default

Encryption Key: The value for `radius_secret_1` in the `authproxy.cfg` on the previous step.

- 4) Add the Secure Token to the dialog boxes. In the End-user UI > Dialogs tab of the CyberArk Endpoint Privilege Manager Server Management Console, edit the Application Launch Alert, Elevate, and Elevate Trusted dialogs and include the User Name and Secure Token property in the dialog. You do not need to add User Name and Secure Token to all these dialogs. For this

Category	Policy Name	Configuration
Dialogs	Computer Shutdown	[DEFAULT] Shutdown
	Computer Sleep	[DEFAULT] Sleep
	Temporary permissions expiration	[DEFAULT] Temporary permissions expiration
	Temporary user permissions granted	[DEFAULT] Temporary user permissions granted
	Policy Automation for Administrator users	Application runs with administrative privileges
	Elevate	Launch with elevated privileges
Balloons		
Web Pages		
Advanced		

-
- The screenshot shows the 'Dialog editor' window. On the left, a list of dialog elements is shown with checkboxes and labels. The 'Launch with elevated privileges' dialog is selected, and its preview is shown on the right. The preview shows a green checkmark icon and the text 'Launch with elevated privileges'. Below this, the 'Description', 'Publisher', and 'Version' fields are visible, each with a placeholder value. The 'Authorized user' field is also visible, with a placeholder value. The 'Password' field is shown as an empty text box.
- | Element | Value |
|--------------------|-----------------------------------|
| Dialog Title | Launch with elevated privileges |
| Logo | No logo |
| Description | Launch with elevated privileges |
| Info Name 1 | Description |
| Info Value 1 | <\$VF_TARGET_DISPLAY_NAME> |
| Info Name 2 | Publisher |
| Info Value 2 | <\$VF_PUBLISHER> |
| Info Name 3 | Version |
| Info Value 3 | <\$VF_PRODUCT_VERSION> |
| Message | Write your message here. |
| Justification | <\$VF_USER_DISPLAYNAME> |
| Justification O... | I need application <\$VF_FILE_... |
| Justification O... | Option 2 |
| Justification O... | Option 3 |
| Justification O... | Option 4 |
- Launch with elevated privileges**
- Description** <\$VF_TARGET_DISPLAY_NAME> (<\$VF_FILE_NAME>)
- Publisher** <\$VF_PUBLISHER>
- Version** <\$VF_PRODUCT_VERSION>
- Authorized user
<\$VF_USER>
- Password
[Empty text box]
- OK Cancel

- 6) If you wish to receive a “PUSH”, enter the word PUSH in capital letters. This will send a push to your Duo mobile app:

 Launch with elevated privileges ×

 Launch with elevated privileges

Description	Windows PowerShell (powershell.exe)
Publisher	Microsoft Windows
Version	10.0.17763.1

Authorized user
DESKTOP\Jeff

Secure Token

Authenticating...

Cancel

OK