ESET

SECURE AUTHENTICATION

Fortinet FortiGate SSL VPN Integration Guide
1. Overview
This document describes how to enable ESET Secure Authentication (ESA) Two Factor Authentication for a Fortinet FortiGate SSL VPN appliance.

2. Prerequisites
Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Fortinet FortiGate appliance configured as a client, as per Figure 1.

**Note:** To prevent locking any existing, non-2FA enabled AD users out of your VPN, we recommend that you allow Active Directory passwords without OTPs during the transitioning phase. It is also recommended that you limit VPN access to a security group (for example **VPNusers**).

- A Fortinet FortiGate SSL VPN appliance.

![Citrix Access Gateway Properties](image)

**Figure 1**
The RADIUS client settings for your Fortinet FortiGate SSL VPN device. Note that the check boxes next to **Mobile Application**, **Compound Authentication** and **Active Directory passwords without OTPs** must be selected and the IP Address is the internal address of your Fortinet appliance.
3. Integration instructions

1. Configure the RADIUS server settings:
   a. Login to the FortiGate admin interface.
   b. Navigate to Authentication > RADIUS Server.
   c. Click Create New.
   d. Enter a name for the server (for example, ESA RADIUS)
   e. Enter the IP address of your ESA RADIUS server.
   f. Enter your shared secret, as shown in Figure 1.
   g. Enter secondary server information, if you have configured a redundant ESA RADIUS server.
   h. Click OK.

2. Configure a User Group:
   a. Click the User section on the left and navigate to User Group > User Group.
   b. Click Create New (or edit an existing group).
   c. Click Add and select the server created in step 1-d (for example, ESA RADIUS).
   d. Leave Firewall selected.
   e. Click OK.

3. Test the authentication:
   a. Navigate to the URL that you normally use for SSL VPN logins with your Fortinet FortiGate appliance
   b. Enter the credentials of your test user:
      i. Ensure that you are using a user that has been configured for Mobile Application 2FA using ESA.
      ii. In the password field, append the OTP generated by the Mobile Application to your AD password. i.e. if the user has an AD password of Esa123 and an OTP of 999111, then type in Esa123999111.

4. Troubleshooting

If you are unable to authenticate via the ESA RADIUS server, ensure you have performed the following steps:

1. Run a smoke test against your RADIUS server, as described in the Verifying ESA RADIUS Functionality document.
2. If you are still unable to connect, revert to an existing sign-in configuration (that does not use 2FA) and verify that you are able to connect.
3. If you are able to connect using the old settings, restore the new settings and verify that your firewall is not blocking UDP 1812 between your VPN device and your RADIUS server.
4. If you are still unable to connect, contact ESET technical support.