1. Overview

This document describes how to enable ESET Secure Authentication (ESA) Two-Factor Authentication (2FA) for an OpenVPN Access Server appliance.

This integration guide utilizes **VPN does not validate AD user name and password** VPN type for this particular VPN appliance. If you wish to utilize other VPN type, refer to *generic description of VPN types* and verify with the vendor if the VPN appliance supports it.

2. Prerequisites

Configuring the VPN for 2FA requires:

1. A functional ESA RADIUS server that has your OpenVPN Access Server configured as a client, as shown in Figure 1.
   - We recommend that you enable **Active Directory passwords without OTPs** to allow existing users (that have not yet been configured for 2FA) to continue logging in during the transitioning phase.
   - We recommend that you restrict VPN access to an Active Directory (AD) security group (for example, **VPN Users** in Figure 1) otherwise all AD users will have access to the VPN.

Figure 1

This screenshot shows the RADIUS client settings for your OpenVPN Access Server. 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 Open VPN appliance.
3. Integration instructions

1. Enable RADIUS authentication:
   a. Using a web browser, log into the OpenVPN administrative interface.
   b. In the Authentication section on the left click General.
   c. Select the radio button next to RADIUS and then click Save Settings, as shown in Figure 2.
   d. DO NOT click Update Running Server, this will lock out all your current users.

![Figure 2](image)

Figure 2 shows how to configure RADIUS authentication. Do not click Update Running Server yet.

2. Configure RADIUS:
   a. Click RADIUS under Authentication in the left pane.
   b. Select PAP as the RADIUS Authentication Method.
   c. Under RADIUS Settings, use the following values (as shown in Figure 3):
      i. Hostname or IP Address: the IP address of your ESA RADIUS server.
      ii. Shared Secret: your shared secret, as shown in Figure 1.
      iii. Authentication Port: 1812
      iv. Account Port: N/A
d. Click **Save Settings**.
e. Click **Update Running Server**.

**RADIUS Authentication Method**

The Access Server supports multiple authentication methods for RADIUS. Please see the Help page for more information.

**Select RADIUS Authentication Method**

- PAP
- CHAP
- MS-CHAP v2

**RADIUS Settings**

<table>
<thead>
<tr>
<th>Hostname or IP Address</th>
<th>Shared Secret</th>
<th>Authentication Port</th>
<th>Accounting Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.51.61</td>
<td>**********</td>
<td>1812</td>
<td>1813</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1812</td>
<td>1813</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1812</td>
<td>1813</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1812</td>
<td>1813</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1812</td>
<td>1813</td>
</tr>
</tbody>
</table>

**Figure 3**

3. Testing the connection:

a. Connect to your SSL VPN with a user account that has been configured for 2FA using the ESA Mobile Application. When prompted for a password, append the one-time password (OTP) generated by the Mobile Application to your AD password. For example, 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 your old Authentication Profile on the VPN device and verify that you are able to connect.
3. If you are able to connect using the old profile, restore the new profile and verify that there is no firewall blocking UDP 1812 between your VPN device and RADIUS server.
4. If you are still unable to connect, contact ESET Customer Care.