ESET
SECURE
AUTHENTICATION

Microsoft RRAS PPTP VPN Integration Guide
## Contents

1. Overview .............................................................................................................4
2. Prerequisites ........................................................................................................4
3. Integration Instructions ......................................................................................7
4. Troubleshooting ..................................................................................................7
1. Overview

This document describes how to enable ESET Secure Authentication (ESA) Two Factor Authentication (2-FA) for a Microsoft RRAS VPN.

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 this VPN appliance supports it.

2. Prerequisites

Configuring the VPN for 2FA requires:

- A functional ESA RADIUS server that has your Microsoft RRAS VPN Server configured as a client, as shown in 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 VPN users).

- A Microsoft RRAS VPN Server
Figure 1.1 shows the RADIUS client settings for your Microsoft RRAS VPN device which uses MSCHAPv2 authentication.
Figure 1.2 shows the RADIUS client settings for your Microsoft RRAS VPN device which uses PAP authentication.

Note that the check boxes next to Mobile Application and Active Directory passwords without OTPs must be selected and the IP address is the address of your RRAS Server.
It is strongly recommended that you enforce PIN usage on the Mobile Application when not using Compound or SMS authentication.

3. Integration Instructions

1. Configure your RADIUS server in RRAS
   a. In Server Manager, navigate to Routing and Remote Access under the Network Policy and Access Services Role. Right-click it and select Properties from the context menu.
   b. Navigate to the Security tab and ensure that the authentication provider is RADIUS Authentication.
   c. Click Configure.
   d. Add your ESA RADIUS server with the same shared secret used in Figure 1, in addition to:
      i. timeout = 30
      ii. initial score = 30
      iii. port = 1812
      iv. leave always use message authenticator option disabled
   e. Click OK twice and click Authentication Methods.
   f. Make sure that the check box next to MS CHAPv2 is selected, and all other check boxes are deselected.

2. Test the authentication:
   a. Launch the native Microsoft VPN client.
   b. Ensure that the VPN type has been set to PPTP.
   c. Make sure that Maximum Encryption has been selected.
   d. Make sure that the Authentication Protocol has been set to MS-CHAPv2 (and all others have been unselected).
   e. Enter the credentials of your test user from step 1:
      i. Ensure that you are using a user that has been enabled for Mobile Application 2FA using ESA.
      ii. In the password field, enter the OTP generated by the Mobile Application.

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 the firewall is not blocking UDP 1812 between your VPN device and your RADIUS server.
4. If you are still unable to connect, contact ESET Customer Care.