ESET
SECURE
AUTHENTICATION

Citrix Access Gateway SSL VPN Integration Guide
Contents

1. Overview ................................................. 4
2. Prerequisites ............................................. 4
3. Integration instructions ................................. 5
4. Troubleshooting .......................................... 5
1. Overview

This document describes how to enable ESET Secure Authentication (ESA) Two-Factor Authentication (2FA) for a Citrix Access Gateway SSL VPN appliance.

2. Prerequisites

Configuring the device for 2FA requires:

- A functional ESA RADIUS server that has your Citrix Access Gateway VPN 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**).


![Figure 1](image-url)

The RADIUS client settings for your Citrix Access Gateway 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 Citrix appliance.
3. Integration instructions

1. Add a new Authentication Profile:
   a. Login to your Citrix Access Gateway admin interface.
   b. Click Management > Authentication Profiles.
   c. Click Add.
   d. Select RADIUS.
   e. In the RADIUS Properties window, enter a Profile Name (for example, ESA RADIUS)
   f. Click New below the Servers list section, and fill in the following values:
      i. Server: The IP Address of your ESA RADIUS server
      ii. Shared Secret: The shared secret, as shown in Figure 1
      iii. Confirm Secret: Same as above
   g. Click OK.
   h. Click Save.

2. Add a logon point:
   a. Click Management > Logon Points.
   b. Click Add (or Edit an existing logon point).
   c. In Authentication Profiles, next to the Primary field, select ESA RADIUS.
   d. Click Save.

3. Test the authentication:
   a. Navigate to the URL that you normally use for SSL VPN logins with your Citrix Access Gateway 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 user 2FA) and verify that you are able to connect.
   1. If you are still able to connect with 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.
   2. If you are still unable to connect, contact ESET technical support.