

ESET Tech Center

Knowledgebase > ESET Secure Authentication > ESET Secure Authentication (ESA) Setup Checklist

ESET Secure Authentication (ESA) Setup Checklist

Ondersteuning | ESET Nederland - 2017-11-27 - Comments (0) - ESET Secure Authentication

<https://support.eset.com/kb3290>

Issue

Install and configure ESET Secure Authentication (ESA)
Grant remote access to the Outlook Web App (OWA) or Virtual Private Network (VPN)
Troubleshoot issues with ESA

Before installing and configuring ESET Secure Authentication, we highly recommend that you read the [Product manual](#).

[Known Issues](#)

Solution

Verify the items on the checklist below to prevent/troubleshoot common issues with ESET Secure Authentication (ESA):

- ☐ **Active Directory (AD) is installed and functional**
- ☐ **ESA services are being deployed in a supported environment under an account that is a member of "Domain Admins" and "Schema Admins"**

ESA is supported on Microsoft Windows 2003 Server SP2 and higher

- ☐ **Active Directory users have mailbox accounts with Microsoft Exchange for Outlook Web App (OWA) access (optional - only required if protecting OWA using ESA)**
- ☐ **ESA services are running**

□ **Mobile telephone numbers are entered for each Active Directory user in the following format: international code/area code/number**

For example: 16195555555, where 1 is the international code and 619 is the area code

Important!

When entering mobile telephone numbers in the **Telephones** tab in the **User Properties** window for Active Directory Users and Computers (ADUC), be sure to enter them into the **Mobile** field.



Figure 1-1

□ **The ESET Secure Authentication mobile app is installed and configured on client phones**

[Android](#)

[iPhone](#)

[BlackBerry](#)

□ **ESA RADIUS Server is configured properly**

In order for your ESA RADIUS server(s) to be utilized by your existing VPN appliance, you will need to reconfigure your appliance according to the relevant [Integration Guide](#)

□ **Your ESA Server is activated**

Once the ESA Server has been installed, you need to activate it using the ESET-issued Username and Password that you received after purchasing your product. To activate your ESA Server:

1. Launch the ESA Management Console.
2. Navigate to your domain node.

3. Enter the Username and Password for your ESA license. The ESA Server will obtain its license automatically and display the current license information.

□ **Outlook Web App (OWA) plug-in is installed and properly configured (Optional)**

The OWA plugin should be installed on the machine running your Microsoft Exchange server.

□ **When authenticating using a VPN and SMS one-time passwords, the end-user must enter their unique one-time password (OTP) the second time they are prompted for credentials**

During two-factor authentication using SMS messages on a VPN, an end-user might confuse the second password prompt and attempt to re-enter their Active Directory credentials. If they submit the wrong credentials too many times, that user will be locked out and will not be able to authenticate until the administrator unlocks their account.

Tags
2FA
ESA