Install and setup ESET Secure Authentication with Microsoft Outlook Web Access (OWA)

Ondersteuning | ESET Nederland - 2017-11-06 - 0 Comments - in ESA

https://support.eset.com/kb6298

Issue

Integrate ESET Secure Authentication with OWA

Best practices for securing access to Microsoft Exchange services

Solution

Before installing the ESET Secure Authentication application on your device

Before you can use the ESET Secure Authentication app on your mobile phone, you must install and configure the ESET Secure Authentication core service on your server and then provision the devices you want to use with the ESET Secure Authentication mobile app.

The instructions below detail the configuration of ESET Secure Authentication for use with Microsoft Outlook Web Access. For more information on server setup and provisioning, or to configure ESET Secure Authentication for use with a VPN, see the ESET Secure Authentication

Installation Manual.

If after configuring the ESET Secure Authentication core service you are still experiencing issues, visit our ESET Secure Authentication (ESA) Setup Checklist.

Prerequisites

The instructions below require the following prerequisites:

A working OWA environment
Access to an account with "Domain Administrator" privileges
A valid ESET Secure Authentication license

For further information, see the ESET Secure Authentication (ESA) Setup Checklist and the ESET Secure Authentication Installation Manual.

Install

1. Download the ESET Secure Authentication installer file.

2. On the system providing the OWA environment, run the installer file with Admin rights.

3. Review the license agreement and click **I accept**.

Figure 1-1

4. Make sure all startup checks are **Successful** and then click **Next**.

Figure 1-2

5. Select which components you want to install and click **Next**. The following components are required:

   - Management Tools
   - Authentication Server

> Do not install the Authentication Server unless the current system is also the system providing ESA services to other systems in the network

- Microsoft Exchange Server 2013, 2010 or 2007

Figure 1-3

6. Click **Close** when the installation completes.

Figure 1-4

Configure

1. Open the ESET Secure Authentication management console.

2. Click your Windows Domain name in the left menu, type in your license details and then click **Activate**.

Figure 2-1

3. Click **Basic Settings** in the left menu, under **Mobile Application** specify a token name and then click **Save**.

> The Token Name will be shown to users using the ESET Secure Authentication app on their mobile devices
>
> For this example, "Demo Company" is used.

Figure 2-2

4. Expand the **Web Application Protection** section and verify that both **Protect Outlook Web Access with**

2FA and **Protect Exchange Control Panel with 2FA** are selected.

For enhanced security, we recommend deselecting the check box next to **Users without 2FA enabled may still log in**.

Figure 2-3

5. Expand **IP Whitelisting** and select the check box next to **Allow access without 2FA from**. Type the following two addresses (for IPv6 and IPv4) to ensure that IT administrators cannot be completely locked out from the system if they are not able to use MFA:

    - ::1
    - 127.0.0.1

> ### It is possible to enable ESA for external IP adresses only by adding your own internal IP ranges to the whitelist
>
> To allow all internal addresses to log in without using ESA, add the following IP ranges:
>
> 10.0.0.0/8
> 172.16.0.0/12
> 192.168.0.0/16

6. Ensure that the whitelist is enabled for both **Outlook Web App** and the **Exchange Control Panel**.

Figure 2-4

Enroll Users

To allow access to ESET Secure Authentication, users need to be configured for one of the available Token Types. The most basic Token Type is **SMS-Based OTP**. To enable this token, make sure that all users have a mobile phone number configured for their account

(using the Windows Server option "Active Directory Users and Computers").

If all users have their mobile phone number set, follow the instructions below.

> **Important!**
>
> If you need to allow a user to use a mobile application, select the check box next to **OTP** and then click **Apply**.
>
> Click **Send Application** and an SMS will be sent to the user containing all the information needed to install and provision the mobile application. For more information, see one of the following Knowledgebase articles for your mobile device:
>
> Android
> iOS
> Windows Phone
> BlackBerry

1. Click the **ESET Secure Authentication** tab.
2. Select the check box **SMS-based OTPs** and click **Apply**.

This user is now configured to use SMS-based OTPs. When the user attempts to log in to OWA, ESET Secure Authentication will request the user's OTP.

Enable Push token on Android mobile devices

If you want to use a push token instead of the SMS-Based OTP, follow the instructions below.

1. Click the **ESET Secure Authentication** tab.

2. Select the check box next to **Push** and then click **Apply**.

ESET Secure Authentication will display a randomly generated login ID and on the currently enrolled device the user will receive a push notification asking to **Approve** or **Reject** the authentication attempt.

Harden Exchange Services

This section provides some security best practices.

A default installation of Microsoft Exchange Server will also provide a number of other services to the internet including ActiveSync and Exchange Web Services (EWS). Research shows that some of these services can be used to bypass MFA solutions such as ESET Secure Authentication. To prevent this, we strongly recommend that you limit access to these services from outside the company network.

ActiveSync

Microsoft ActiveSync allows mobile devices to easily connect to Microsoft Exchange. ESET Secure Authentication does not support Microsoft ActiveSync and therefore, we recommend that you limit access to this service.

We recommend that you specify only certain devices (for example, company phones) to connect via ActiveSync. This can be done through the **Exchange Control Panel** as well as the **Exchange Management Shell**.

Exchange Services

For all publicly available services, we recommend that you restrict access to the following services based on IP addresses:

Autodiscover
EWS
mapi
Microsoft-Server-ActiveSync

OAB
PowerShell
Rpc

1. To set these restrictions, open the OWA website in the Internet Information Services (IIS) Manager and navigate to **IP Address and Domain Restrictions** for each of the services listed above.

> ### If IP Address and Domain Restrictions is not available
>
> If **IP Address and Domain Restrictions** is not available, it may need to be installed separately.
>
> See https://technet.microsoft.com/en-us/library/cc725769(v=ws.10).aspx.

2. In the **Actions** window, click **Edit Feature Settings**.

3. From the **Access for unspecified clients** drop-down menu, select **Deny**.

4. From the **Deny Action Type** drop-down menu, select **Not Found**.

> ### Security best practice
>
> For security reasons we recommend that you also change the “Deny Action Type” to “Not Found”. This can deter automated scanners and inexperienced attackers looking for Microsoft Exchange servers to attack.

Figure 5-1

5. Click **Add Allow Entry** and in the **Specific IP address** field, add the following addresses (to prevent the system itself from being unable to access certain resources it might need during operation):

   - ::1

- 127.0.0.1

> Optionally, the following addresses can be added to allow access from the internal network
>
> IP address range: 10.0.0.0 – Mask or Prefix: 8
> IP address range: 172.16.0.0 – Mask or Prefix: 12
> IP address range: 192.168.0.0 – Mask or Prefix: 16

6. Repeat steps 1– 5 for all services.

Tags

ESA

OWA