ESET Secure Authentication and Outlook Web Access

Date: **4-1-2017**

Document version: **1.0**

Author: Donny Maasland, Head of Cybersecurity Services and Research





1. INTRODUCTION	3
2. REQUIREMENTS	3
3. ESET SECURE AUTHENTICATION	1
3.1. INSTALLATION	1
3.2. CONFIGURATION	5
3.3. ENROLLING USERS	3
4. HARDENING EXCHANGE SERVICES.	3
4.1 INTRODUCTION	3
4.2 ACTIVESYNC	1
4.3 EXCHANGE SERVICES	1
5. CONCLUSION	7



1. INTRODUCTION

Many companies are using Microsoft Exchange as their solution for email, calendaring, etc. Most of them also allow their users to make use of the built-in "Outlook Web Access" or "Outlook Web App" (OWA) solution that allows users to access most of the features Exchange has to offer through a web browser.

	Outlook Web App
0	Domain\user name:
	Password:

In a default configuration however, OWA allows users to authenticate themselves with a username and password combination only. This is considered as a security risk by most professionals, as it is relatively easy for a person with malicious intent to abuse stolen / leaked credentials to gain access to sensitive company information (for example: email, files, etc.). Furthermore, OWA does not offer any Multi-Factor Authentication (MFA) capabilities out of the box.

This is why ESET has developed a product called "ESET Secure Authentication¹" (ESA). ESA is a product that allows MFA to be easiliy integrated with existing solutions such as OWA, allowing IT administrators to easily increase the level of security of their available applications.

The content of this document focusses on integrating ESA with OWA in a few simple steps. Furthermore, it offers some best practices for securing access to services that Microsoft Exchange offers.

2. REQUIREMENTS

This document assumes that the following requirements are met:

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

Also see the "ESET Secure Authentication Setup Checklist" available at: <u>http://support.eset.com/kb3290/</u>.



3. ESET SECURE AUTHENTICATION

3.1 INSTALLATION

Start by downloading the ESA installer from the ESET download page².



After downloading the installation file, run it with administrative privileges on the system providing OWA.



Read and accept the license agreement.

-	ESET Secure Authentication Setup	x
SECURE AUTHENTICATION	N v2.5.2	23.0
Review license agreement Perform startup checks Select components Check prerequisites Install Complete	IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS. Software End-User License Agreement. Under the terms of this Software End-User License Agreement (hereinafter referred to as "the Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31 333 535 or another company from the ESET Group (hereinafter referred to as "You" or "the End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below. THIS IS AN AGREEMENT ON END-USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to	< 111
	I do <u>n</u> ot accept I <u>a</u> ccept	

ESCT ENJOY SAFER TECHNOLOGY**

Make sure all startup checks are successful, and click on "Next".

ED	ESET Secure Authentication Setup	_ 🗆 X
ESET SECURE AUTHENTICATIO	N	v2.5.23.0
Review license agreement	Mapping installation environment	Successful ^
Perform startup checks	Active Directory membership	Successful
Select components	Domain Admin privileges	Successful
Check prerequisites	Installer is elevated	Successful
Install	System connectivity	Successful ≡
Complete	AD Containers location	Successful
	The .Net Framework Version 4.0 Full Install (Win 7 only)	Successful
	Determining installable components	Successful
	Determining installable components	Successful
	The .Net Framework Version 4.0 Full Install	Successful
	Active Directory DNS	Successful
	Domain functional level	Successful V
	Back	<u>N</u> ext

Select what you want to install. At least the following items are needed:

- Management Tools
- Authentication Server³
- Microsoft Exchange Server 2013, 2010 or 2007

Wait for the installation to complete.

	ESET Secure Au	thentication Setup	- 🗆 X	
ESET SECURE AUTHENTI	ICATION		v2.5.23.0	
Review license ag Perform startup ci Select component Check prerequisit Install Complete	reement Installing hecks ts es Removing applications	ESET Secure Authentication Setup		X
	ESET SECURE AUTHENTICATION			v2.5.23.0
	Perform startup checks Select components Check prerequisites Install Complete	Installation co	mplete	
	comprete			
			Export log files	Close



3.2 CONFIGURATION

After the installation has completed, upon up the ESET Secure Authentication management console.



This console is were all the settings for ESET Secure Authentication are made. The first step is entering your license details and activating the product. This can be done by clicking on your Windows Domain name in the left pane and entering your details on the right. After that, click on "Activate".







ESET Secure Authentication should now be activated.



After entering your license details some initial configuration has to be done. To do this, click on "Basic Settings" in the left pane. In the right pane, under "Mobile Application", specify a name that will be shown to users using the ESET Secure Authentication app on their mobile devices (in this case "Demo Company").



After that, scroll down to "Web Application Protection" and expand it. Make sure that both "Outlook Web Access" and "Exchange Control Panel" are protected by ESA. For enhanced security it is recommended to uncheck "Users without 2FA enabled may still log in".



Scroll down to "IP Whitelisting" and expand it. Check the box labeled "Allow access without 2FA from:" and enter the following two addresses:

- ::]
- 127.0.0.1



This will ensure that IT administrators cannot be completely locked out from the system if they are not able to use MFA for whatever reason. Furthermore, it is possible to enable ESA only for external IP addresses 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:

- 10.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Finally, make sure that the whitelist is enabled for both OWA and the Exchange Control Panel (ECP).



3.3 ENROLLING USERS

To allow users to use ESET Secure Authentication, they need to be configured for one of the available "Token Types". The most basic Token Type is the "SMS-Based OTP". To enable this token, make sure that all users have a mobile phone numer configured for their account (via "Active Directory Users and Computers").

Active	e Directory Us	ers and Computers		-	D X			
i 🖬 💽	.	1 🔻 🗵 🐍						
Name 🔱 Henk Test	Type User	Description				le is	ready	
			Member Remote General	Of Dial-in Desktop Servi Address	n Enviro ices Profile Account	onment COM+ Profile	Sessions ESET Sec Telephone	Remote control ure Authentication s Organization
			Telep Hom Page Mobi	e: r: e:	2345678			Other Other Other
			IP ph	one:				Other

eset enjoy safer technology*

If all users have their mobile phone number set, click on the "ESET Secure Authentication" tab⁴.



Click the checkbox labeled "SMS-based OTPs" and click "Apply".

		Henk Te	st Prop	erties	? X
Member Of	F Dial-ir	n Enviro	nment	Sessions	Remote control
General	Address	Account	Profile	Telephone	s Organization
Remote De	sktop Servi	ces Profile	COM+	ESET Sec	ure Authentication
P	2FA is a	activated w	ith SMS-	based OTP:	5
Enabled	2FA is a Token Type	activated w	ith SMS-	based OTP:	3
Enabled	2FA is a Token Type S-based OT	activated w es Ps	ith SMS-	based OTP:	s nd Application
Enabled SM: Mobile	2FA is a Token Type S-based OTI Application OTP	activated w s Ps Push	ith SMS-	based OTP:	and Application

This user is now configured to use SMS-based OTPs. When the user attempts to log in to OWA, ESET Secure Authentication will display a page requesting the user to input their OTP.

	«Web A	٩р
DOMAIN\Henk		
Password: ← → C ▲ https://ex01.domain.local.	iowa/_esaInternalContentOtp.aspx?returnUrl=%2fowa%2f	NatioNad1
J si (Enter OTP delivered via SMS text.
ESET	Copyright (c) 2012-2016 ESET, spol. s r.o. All rights reserved.	



ESET Secure Authentication will send an SMS with an OTP (One-Time Password) to the user.



After entering this OTP, the user will be able to use OWA as normal.

ESET SECURE AUTHENTIC	CATION
8 Denk Test - Outlook Wei	Developments of the second sec
	.domain.local/owa/#path=/mail
o <mark>≊</mark> Outlook Web App	
(+) new mail	𝒫 search Mail and People
	INBOX CONVERSATIONS BY DATE 👻
~~	all unread to me flagged
⊿ Favorites	
Inbox	
Sent Items	
Deleted Items	
⊿ Henk Test	
Inbox	
Drafts	
Sent Items	 There are no items to
Deleted Items	show in this view.
Junk Email	
Notes	
RSS Feeds	

CSCT ENJOY SAFER TECHNOLOGY™

A mobile application⁵ is also available. To allow a user to use a mobile application, enable the checkbox labeled "OTP" and click "Apply".

General	Address	Account	Profile	Telephones	s Organization
Member Of	Dial-in	Enviro	nment	Sessions	Remote control
Remote Desk	top Servic	es Profile	COM+	ESET Secu	ure Authentication
1	2FA is a SMS-bas	ctivated; u ed OTPs	useristra to a Mob	ansitioning fr ile Applicatio	om on
Enabled To	2FA is an SMS-base	ctivated; u ed OTPs	useristra to a Mob	ansitioning fr ile Application	om on d Application
Enabled To SMS- Mobile Ap	2FA is a SMS-bas oken Types based OTP plication	ctivated; u æd OTPs s	user is tra to a Mob	ansitioning fr ile Application	om on d Application

Then click on the "Send Application" button. This will send an SMS to the user containing all the information needed to install and provision the mobile application⁶.



After successful installation the device will show the company name as set during the configuration phase.



Tapping the company name will show the current OTP.



5. Available for Android, iOS, Windows Phone and BlackBerry.

6. http://support.eset.com/kb3297/ - Android

http://support.eset.com/kb3283/ - iOS





The ESA webpage will now ask for the OTP generated on the users' device.



The last Token Type this document will cover is the "Push" Token⁷. This can be enabled by enabling the checkbox labeled "Push" and clicking "Apply".

		Henk Te	est Prop	erties	?)
General	Address	Account	Profile	Telephone	s Organization
Member Of	f Dial-in	Enviro	nment	Sessions	Remote control
Remote De	esktop Servic	es Profile	COM+	ESET Sec	ure Authentication
P	2FA is a	ctivated w	rith a Mol	bile Applicat	ion
Enabled	2FA is a Token Types	ctivated w	rith a Mol	bile Applicat	ion
Enabled	2FA is a Token Types S-based OTF	ctivated w	rith a Mol	bile Applicat	t ion Ind Application
Enabled SM: Mobile	2FA is a Token Types S-based OTF Application OTP V F	ctivated w s 's Push	rith a Mol	bile Applicat	tion Ind Application Jnlock 2FA

This will cause ESET Secure Authentication to display just a randomly generated login ID.

ESET SECURE AUTHENTICATION

Approve login ID: 868
prove the login on your device or enter the OTP.

On the currently enrolled device the user will receive a push notification asking to approve or reject the authentication attempt, while showing the same ID to verify the legitimacy of the request.



eset enjoy safer technology[™]

This notification can also be tapped for more detailed information.

■ 🛜 "∦ 6% 💈 15:43
CET SECURE AUTHENTICATION
9
Authentication Request
ID: 868 Demo Company Exchange
User Henk
IP Address 10.0.0.11
Time November 14, 2016 15:43:40
✓ APPROVE × REJECT

4. HARDENING EXCHANGE SERVICES4.1 INSTALLATION

Besides OWA, a default installation of Microsoft Exchange Server will also provide a number of other services to the internet. These include ActiveSync, Autodiscover and Exchange Web Services (EWS).



Recent research has shown that some of these services (for example: EWS) can be used to bypass MFA solutions⁸ like ESET Secure Authentication. To prevent this it is highly recommended to limit the access to these services from outside the company network.



4.2 ACTIVESYNC

Microsoft ActiveSync is a technique that allows mobile devices to easily connect to Microsoft Exchange so that users can access their email and appointments while on the road. ESET Secure Authentcation does not support Microsoft ActiveSync however, so it is recommended to limit access to this service.

The easiest way of doing this is by not allowing all devices to connect to the ActiveSync service, but to 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 admin cer	nter		
Eneriange aanni cei		Exchange ActiveSync Access Settings - Internet Explorer	_ D X
recipients	mobile device access		Help
permissions		Exchange ActiveSync access settings	
compliance management	Exchange ActiveSync Access Allow synchronization with mobi	Connection Settings When a mobile device that isn't managed by a rule or personal	^
organization	You haven't selected any admini- No custom text is added to mes	exemption connects to Exchange: Allow access	
protection		succk access Quarantine - Let me decide to block or allow later	
mail flow	Quarantined Devices	Quarantine Notification Email Messages Select administrators to receive email messages when a mobile device	
mobile	/ 40 46 LL C	is quarantined.	
public folders	USER	DISPLAY NAME SMTP ADDRESS	
unified messaging		Administrator Administrator@domain.nl	
servers			
hybrid		Text to include in messages sent to users whose mobile device is in	
tools		quarantine, blocked, or in the process of being identified:	
	Device Access Rules + 🖉 🛅 🖨		~
	5	save	cancel

For more information, please refer to: <u>http://exchangeserverpro.com/</u> <u>preventing-new-activesync-device-types-from-connecting-to-exchange-</u> <u>server-2010/</u>.

4.3 EXCHANGE SERVICES

For all other publicly available services it is recommended to restrict access to the following services based on IP addresses:

- Autodiscover
- EWS
- mapi
- Microsoft-Server-ActiveSync
- OAB
- PowerShell
- Rpc

eset enjoy safer technology*

These restrictions can be set by opening up the OWA website in the IIS Manager, and then navigating to "IP Address and Domain Restrictions⁹" for each of the aforementioned items.

8 <u>3</u>							Inter	net Informa	ation Servic	es (IIS) Mana
EX01 > Sites > Default Web	Site 🔸 EWS 🔸									
File View Help										
Connections										
🔍 - 🗟 🖄 🔗	/EWS	Home								
Start Page	Filter:		• 🔻 Go - 🕻	Show All	Group by: Ar	ea	• 📴 •			
	ASP.NET .NET Authorizat Co	.NET	A04 .NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users	Application Settings	Connection M Strings
 	Authentic Co	mpression	Default Document	Directory Browsing	A04 Error Pages	Failed Request Tra	Handler Mappings	HTTP Redirect	HTTP Respon	IP Address and Domain Restrictions
 Proversnell Proversnell Proversnell Rpc Exchange Back End 	Configurat IIS Editor Pe	Manager								

Then, click on "Edit Feature Settings".

Act	ions
	Add Allow Entry
	Add Deny Entry
	Edit Feature Settings
	Revert To Parent
	View Ordered List

In the newly opened dialog, set "Access for unspecified clients" to "Deny". For security reasons it is recommended to also change the "Deny Action Type" to "Not Found". This can possibly deter automated scanners and inexperienced attackers looking for Microsoft Exchange servers to attack.

Edit IP and Domain Restrictions Settings	?	x
Access for unspecified clients:		
Deny 🗸		
Enable domain name restrictions		
Enable Proxy Mode		
Deny Action Type:		
Not Found 🗸		
Unauthorized Forbidden		
Not Found C	ancel	
noon		

After that, click on the "Add Allow Entry" link and add the following addresses:

- 127.0.0.1
- ::1

Add Allow Restriction Rule	?	x
Allow access for the following IP address or domain name:		
Specific IP address:		
::1		
O IP address <u>r</u> ange:		
Mark or Drofin		



This will prevent the system itself from being unable to access certain resources it might need during operation.

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

	Add Allow Restriction Rule	? X	
All O	low access for the following IP address or domain name: Specific IP address:		
۲	IP address <u>r</u> ange:		
	<u>M</u> ask or Prefix: 8		
	ОК	Cancel	

Repeat this for all services.

G			
EX01 > Sites > Default Web	Site 🕨 EWS 🕨		
<u>F</u> ile <u>V</u> iew <u>H</u> elp			
Connections Connections Start Page Connection Start Page Connection Connections Connectio	Use this fea Group by:	Address and I ture to restrict or grant No Grouping	Domain Restrictions
⊿ 🧃 Sites	Mode	Requestor	Entry Type
4 🌀 Default Web Site	Allow	:1	Local
▷ i aspnet_client	Allow	10.0.0(8)	Local
▷ P Autodiscover	Allow	127.0.0.1(8)	Local
bin	Allow	172.16.0.0(12)	Local
⊳ · · · · · · · · · · · · · · · · · · ·	Allow	192.168.0.0(16)	Local



CONCLUSION

Using this document, you can install ESET Secure Authentication and configure it to increase your level of security when using Outlook Web App. It also sets the baseline for possibly securing other platforms such as "Microsoft SharePoint" and "Microsoft Remote Desktop Web Access".

Furthermore, by providing some best practices from a security perspective, you have limited the potential attack service by restricting access to the Microsoft Exchange services available by default.

As with any major (or minor) change in an IT environment. It is important to thoroughly test the impact of these changes to ensure that users will not experience any discomfort while working, and that all automated processes continue to work as expected.

Should you experience any issues during the installation or configuration of ESET Secure Authentication, please don't hesitate to contact our support department via <u>https://www.eset.com/int/support/contact/</u>.