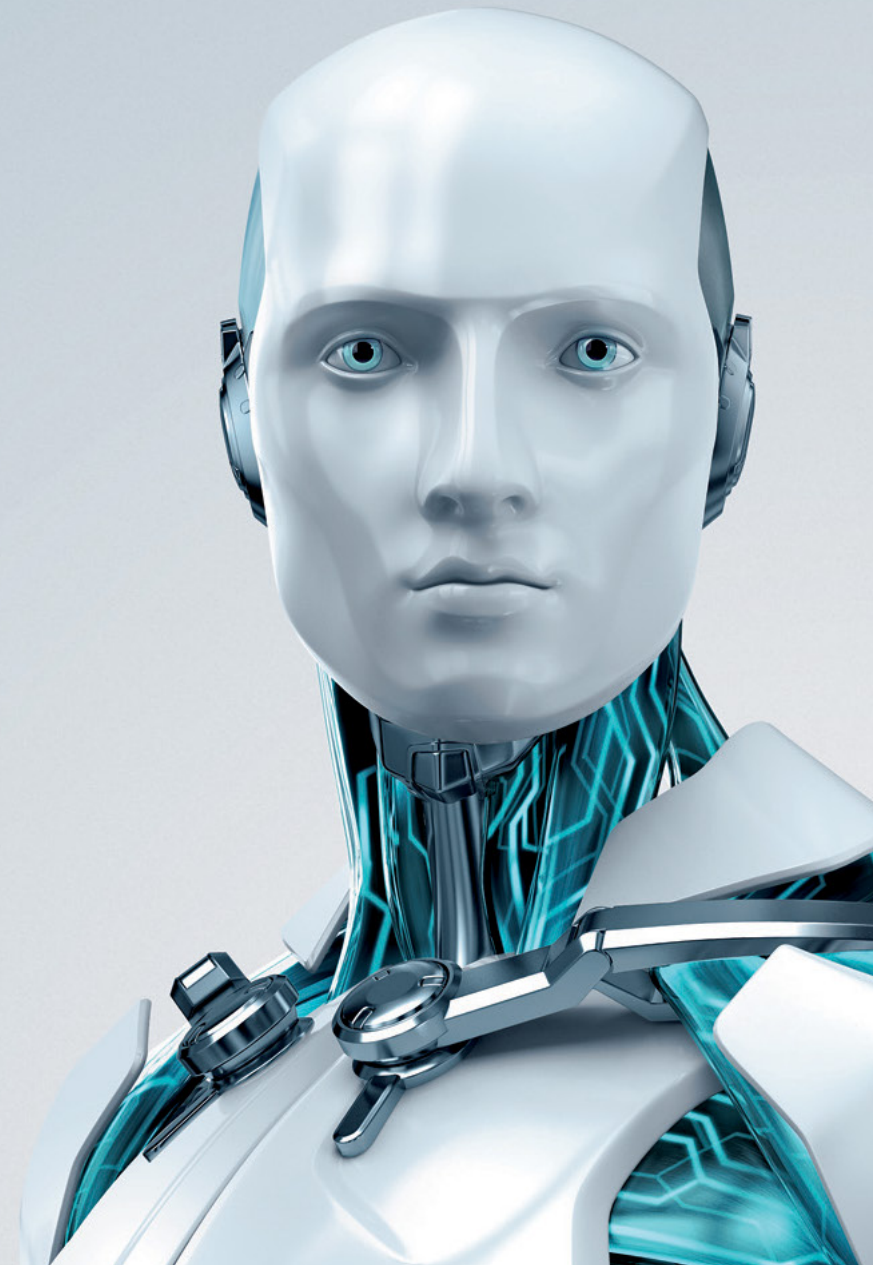


ESET Secure Authentication and Outlook Web Access

Date:
4-1-2017

Document version:
1.0

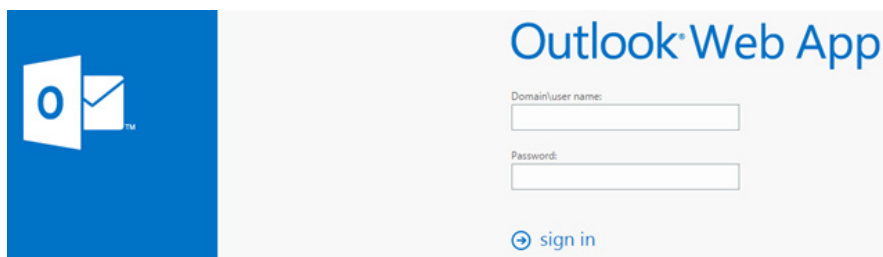
Author:
Donny Maasland, Head of Cybersecurity Services and Research



1. INTRODUCTION	3
2. REQUIREMENTS	3
3. ESET SECURE AUTHENTICATION	4
3.1. INSTALLATION	4
3.2. CONFIGURATION	6
3.3. ENROLLING USERS.	8
4. HARDENING EXCHANGE SERVICES.	13
4.1 INTRODUCTION	13
4.2 ACTIVESYNC	14
4.3 EXCHANGE SERVICES	14
5. CONCLUSION	17

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.



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 Authentication” (ESA). ESA is a product that allows MFA to be easily 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.

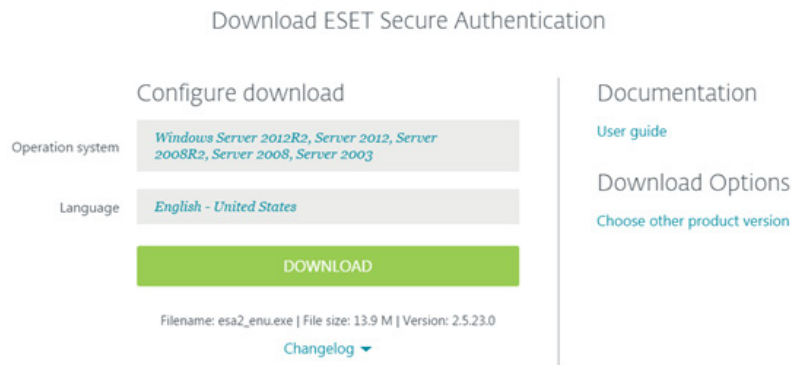
Also see the “ESET Secure Authentication Setup Checklist” available at:

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

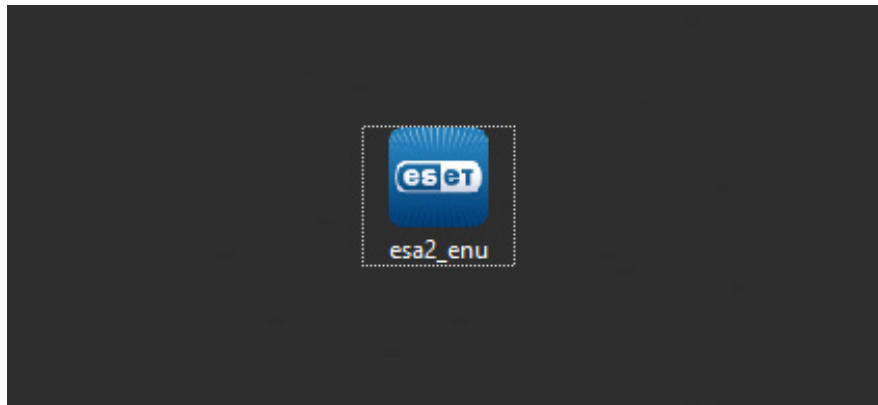
3. ESET SECURE AUTHENTICATION

3.1 INSTALLATION

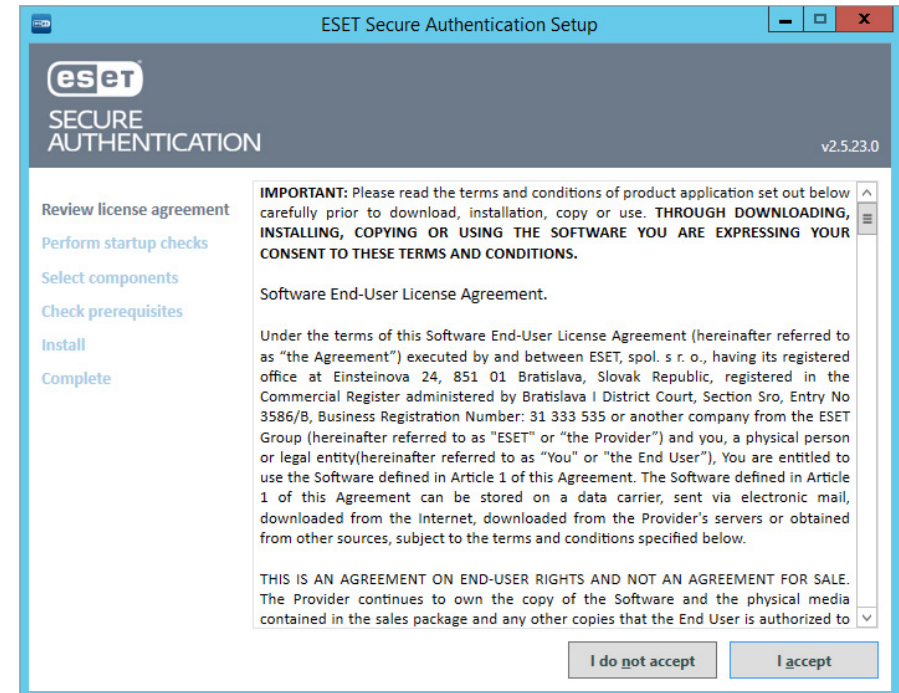
Start by downloading the ESA installer from the ESET download page².



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

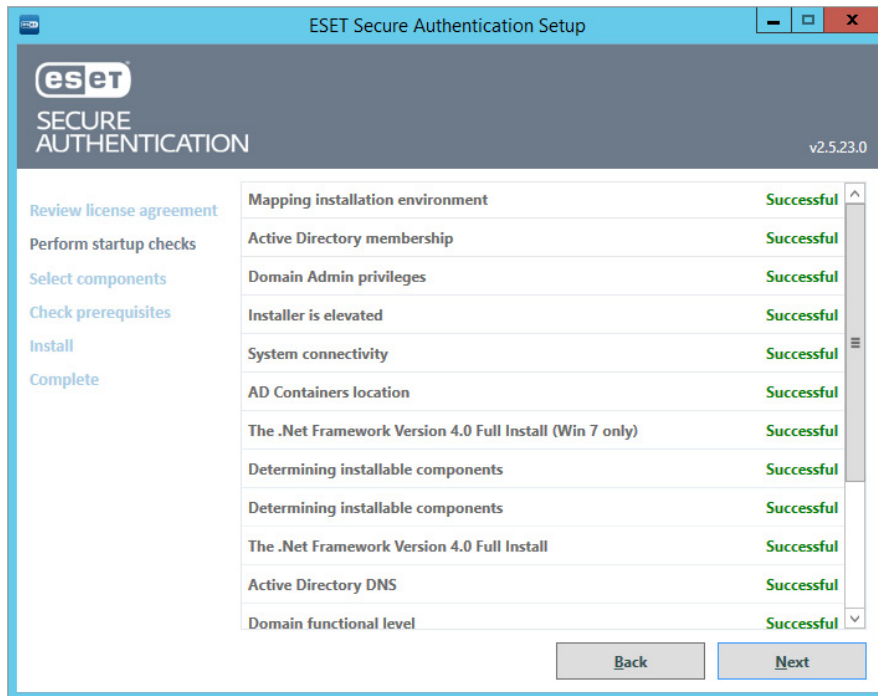


Read and accept the license agreement.

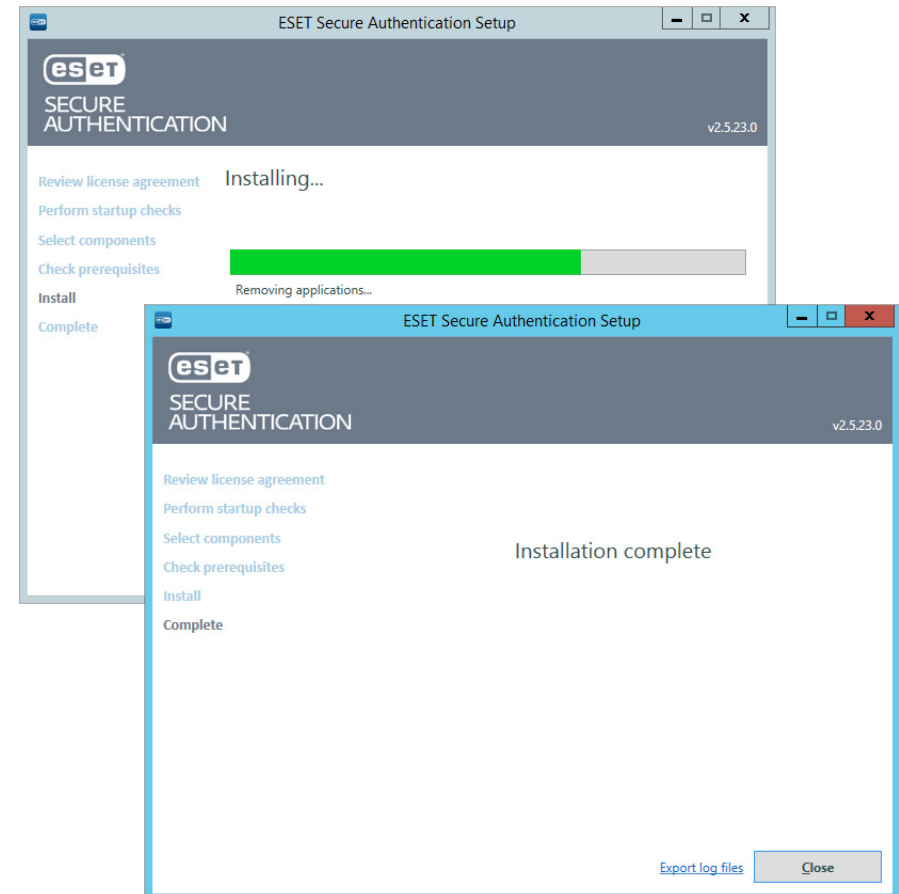


2. <https://www.eset.com/int/business/endpoint-security/two-factor-authentication/#download>

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



Wait for the installation to complete.



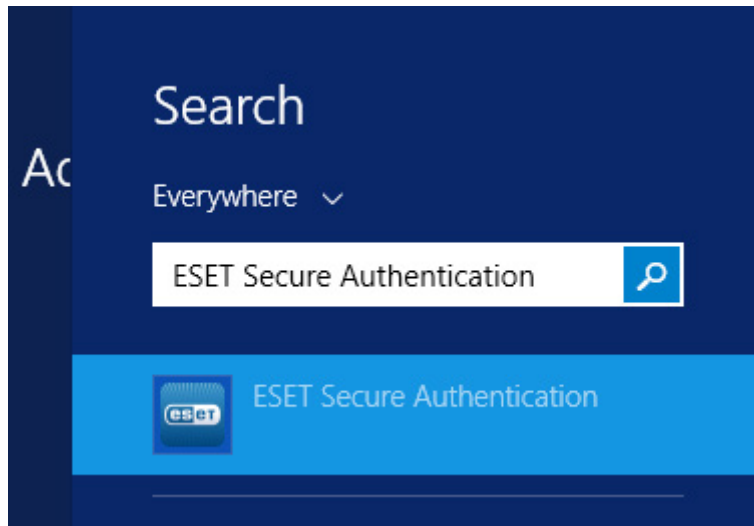
Select what you want to install. At least the following items are needed:

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

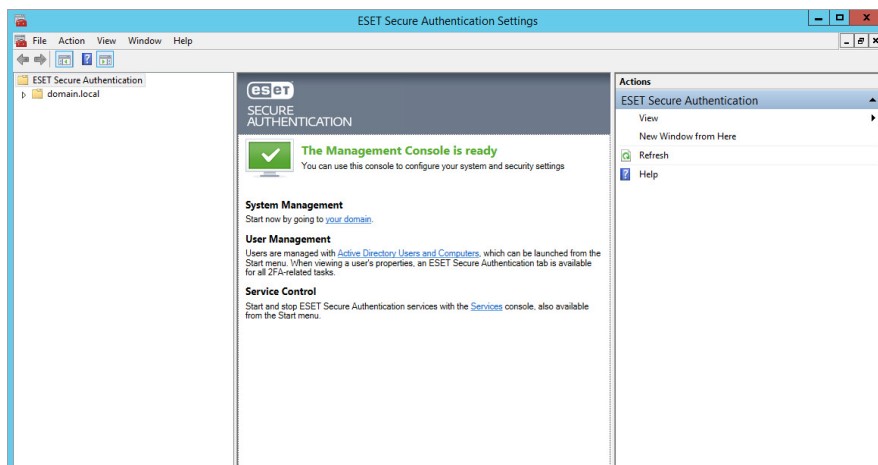
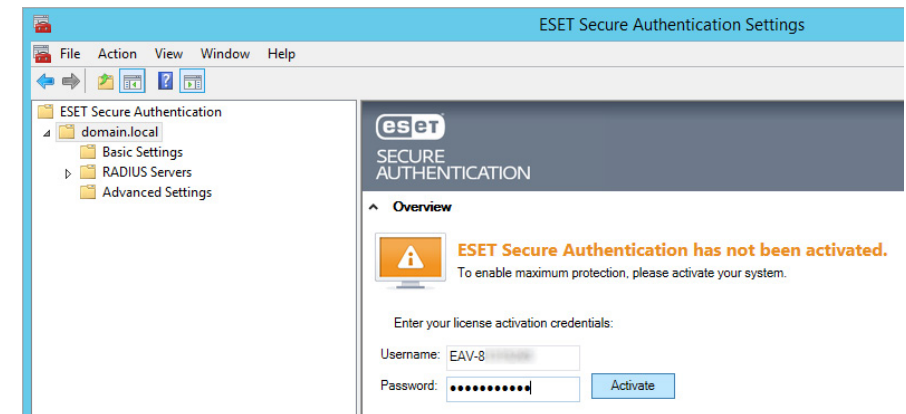
3. In this case it is assumed that the current system is also the system providing ESA services to other systems in the network. If this is not the case, please do not install this feature.

3.2 CONFIGURATION

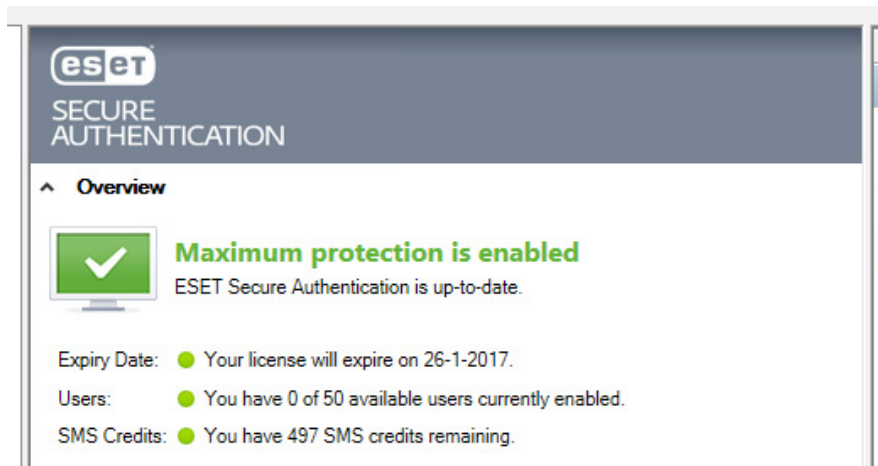
After the installation has completed, upon up the ESET Secure Authentication management console.



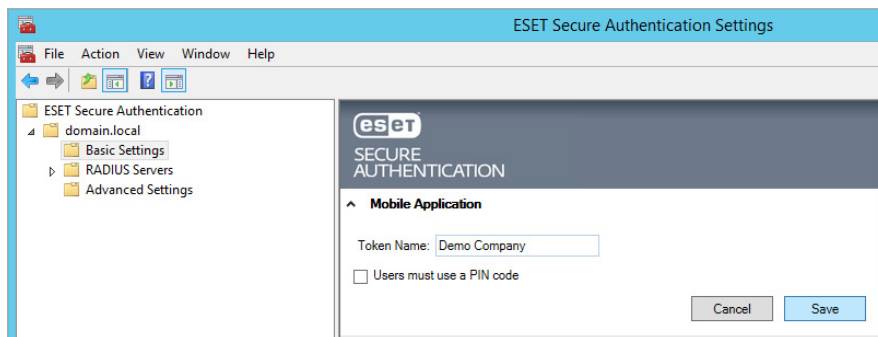
This console is where all the settings for ESET Secure Authentication are made. The first step is entering your license details and activating the product. This can be done by clicking on your Windows Domain name in the left pane and entering your details on the right. After that, click on "Activate".



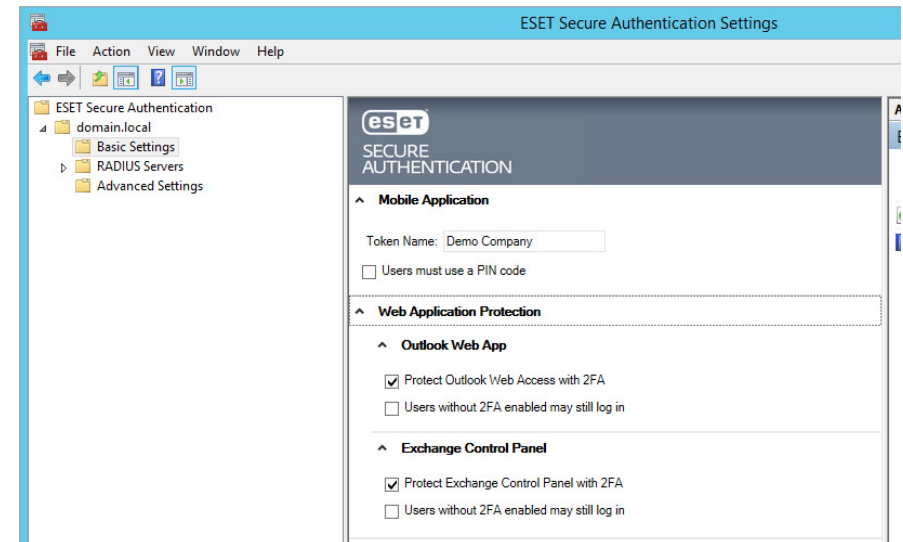
ESET Secure Authentication should now be activated.



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”.



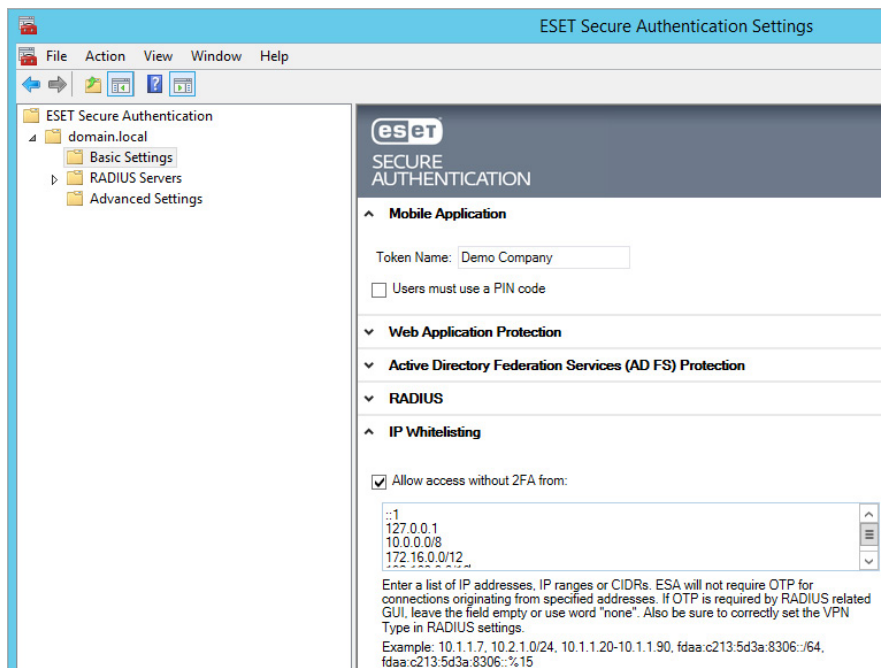
Scroll down to “IP Whitelisting” and expand it. Check the box labeled “Allow access without 2FA from:” and enter the following two addresses:

- ::1
- 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:

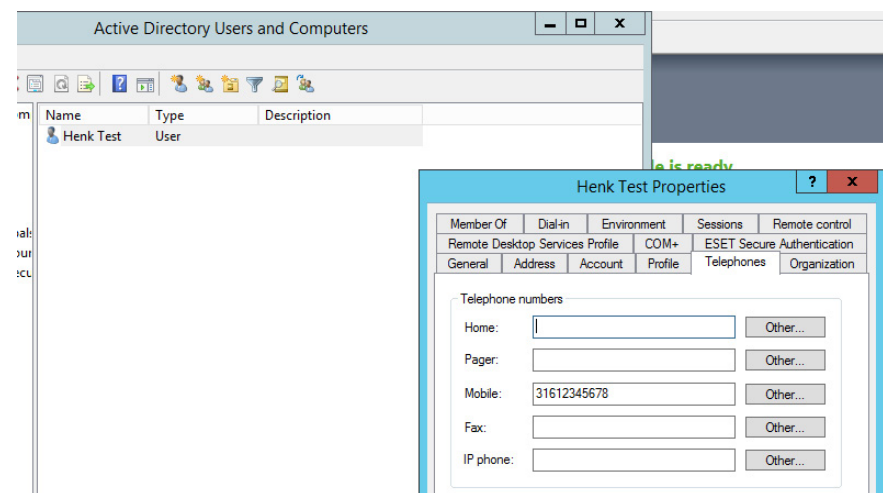
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

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

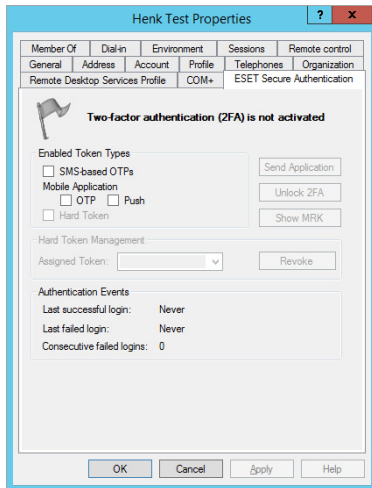


3.3 ENROLLING USERS

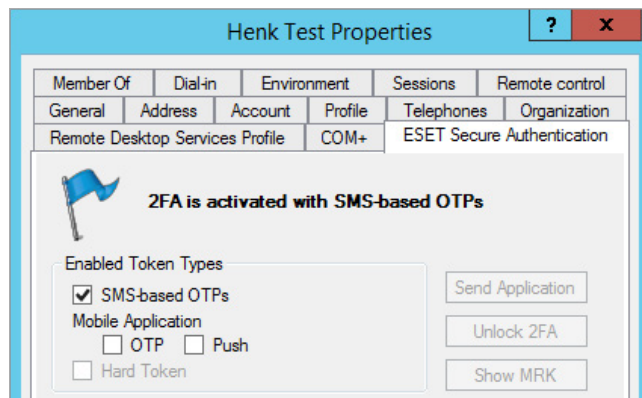
To allow users to use ESET Secure Authentication, they need to be configured for one of the available “Token Types”. The most basic Token Type is the “SMS-Based OTP”. To enable this token, make sure that all users have a mobile phone number configured for their account (via “Active Directory Users and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



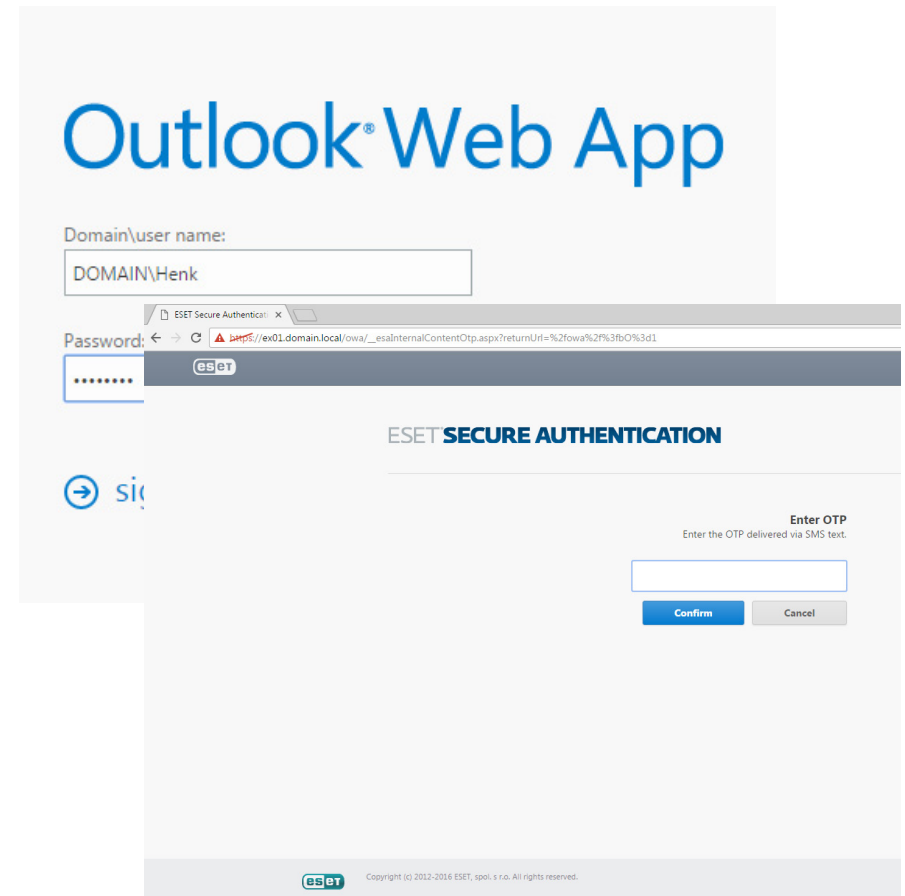
If all users have their mobile phone number set, click on the “ESET Secure Authentication” tab⁴.



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

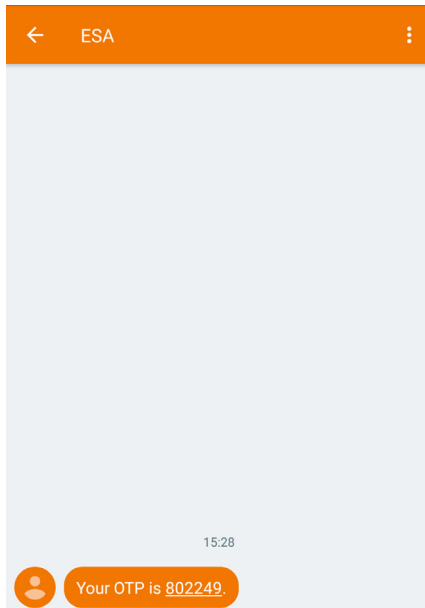


This user is now configured to use SMS-based OTPs. When the user attempts to log in to OWA, ESET Secure Authentication will display a page requesting the user to input their OTP.

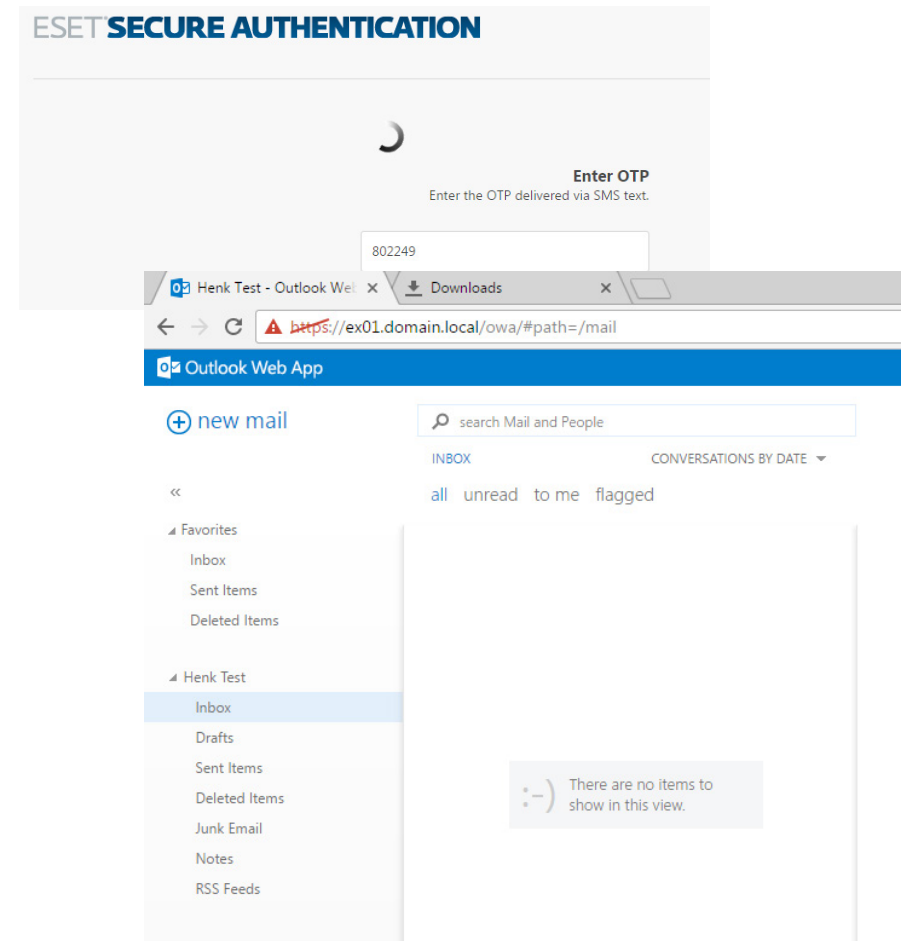


⁴ If you administer users from a different system, you may need to install “Management Tools” from the ESET Secure Authentication installation package.

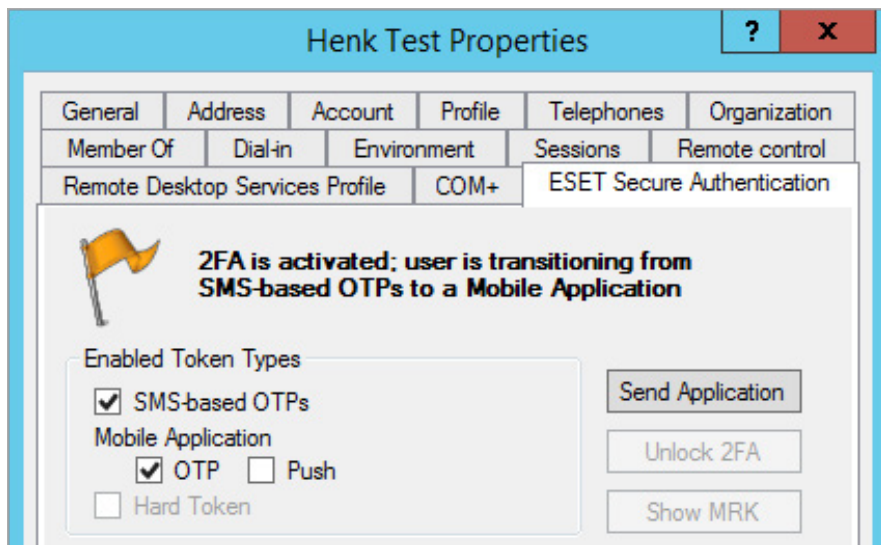
ESET Secure Authentication will send an SMS with an OTP (One-Time Password) to the user.



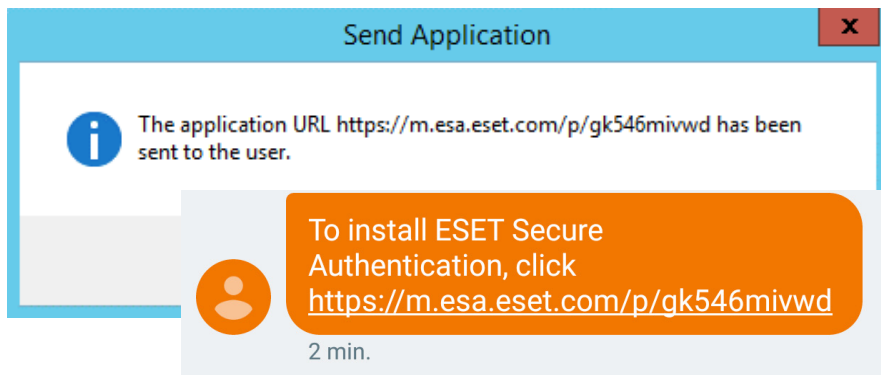
After entering this OTP, the user will be able to use OWA as normal.



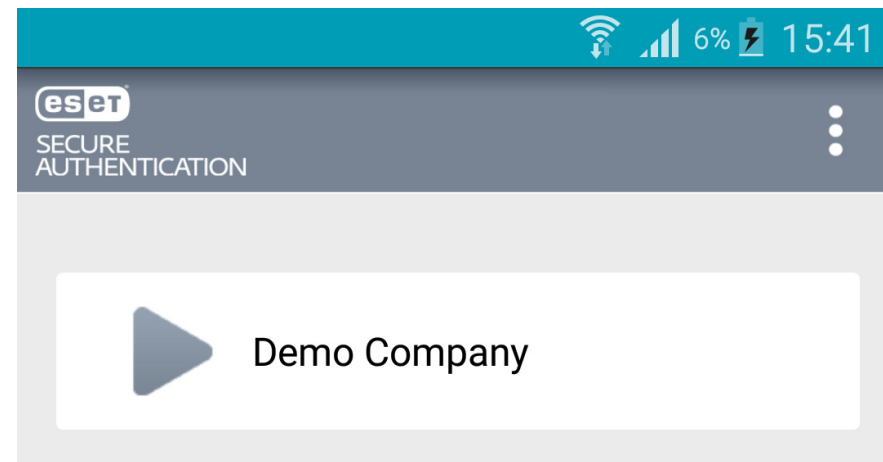
A mobile application⁵ is also available. To allow a user to use a mobile application, enable the checkbox labeled “OTP” and click “Apply”.



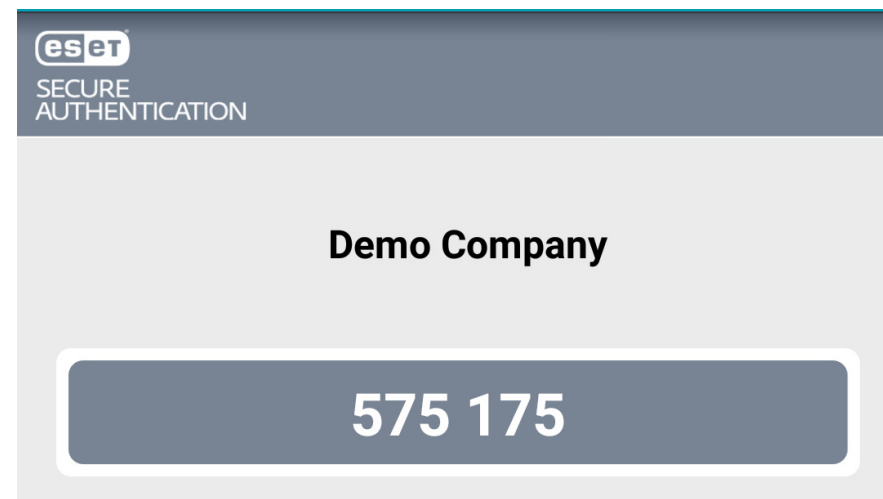
Then click on the “Send Application” button. This will send an SMS to the user containing all the information needed to install and provision the mobile application⁶.



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.

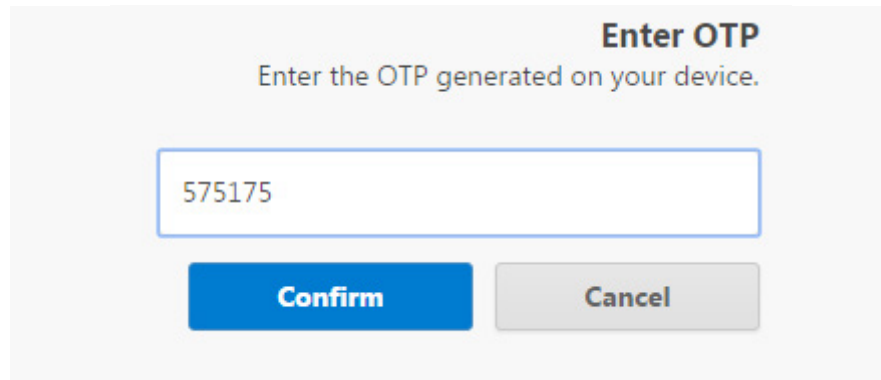
6. <http://support.eset.com/kb3297/> - Android

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

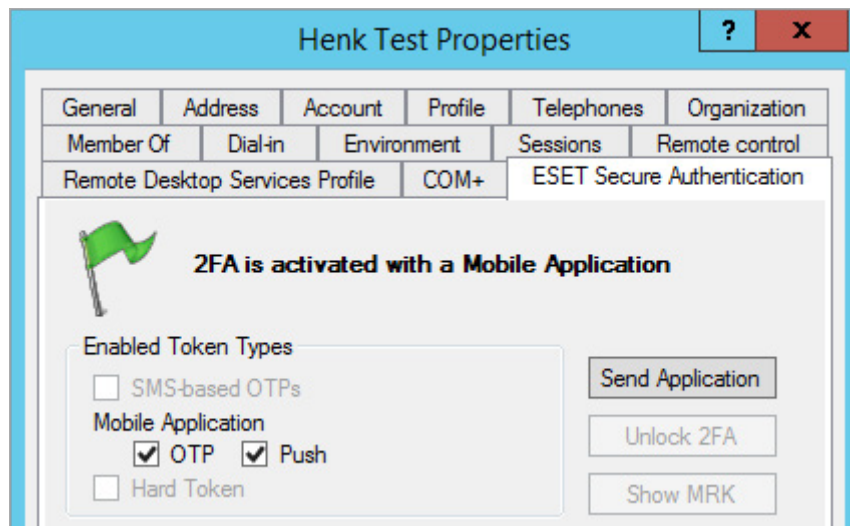
<http://support.eset.com/kb5703/> - Windows Phone

<http://support.eset.com/kb3298/> - BlackBerry

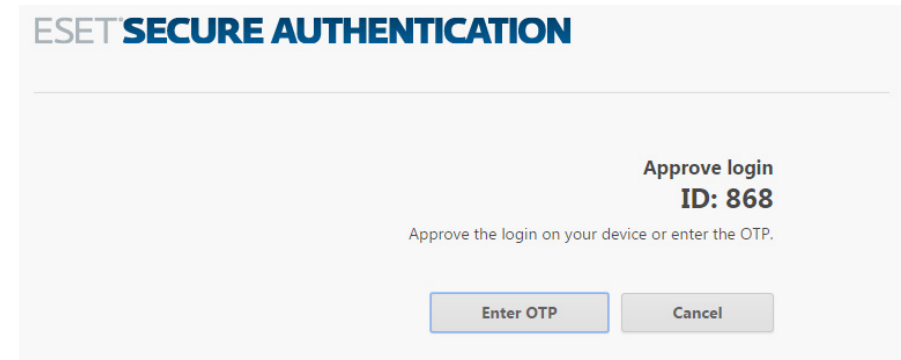
The ESA webpage will now ask for the OTP generated on the users' device.



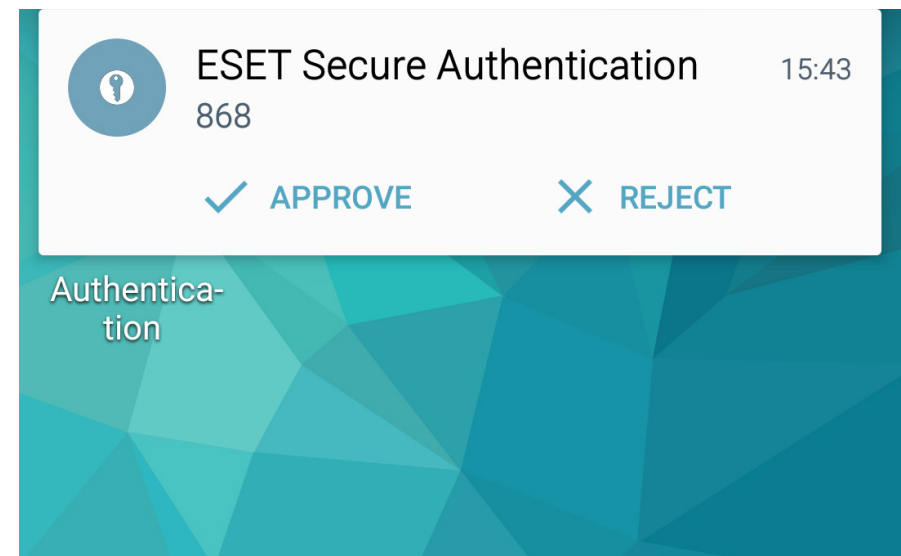
The last Token Type this document will cover is the "Push" Token⁷. This can be enabled by enabling the checkbox labeled "Push" and clicking "Apply".



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

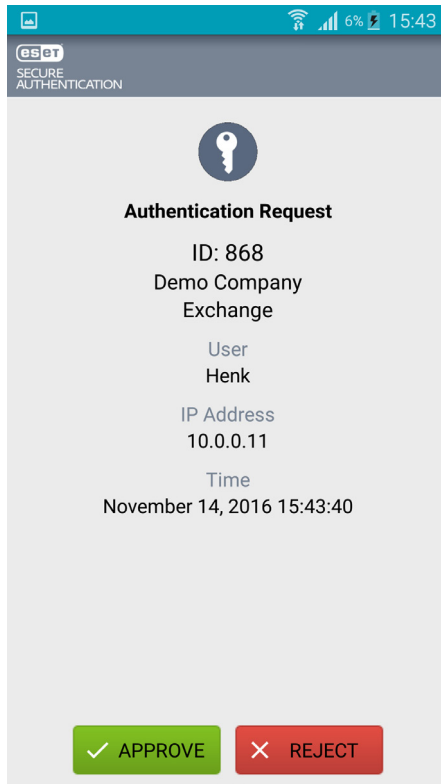


On the currently enrolled device the user will receive a push notification asking to approve or reject the authentication attempt, while showing the same ID to verify the legitimacy of the request.



⁷ Currently only supported when using the ESET Secure Authentication app on Android.

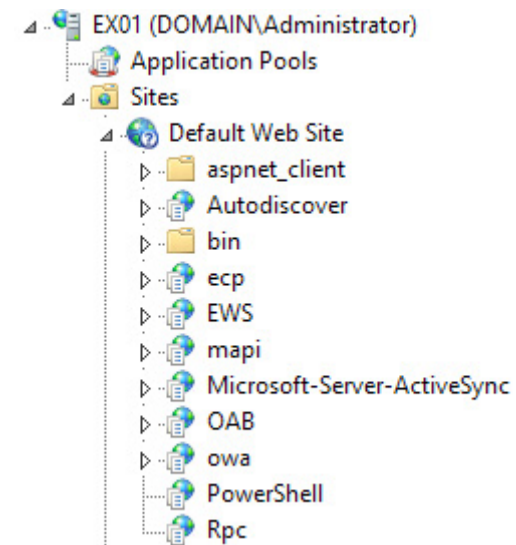
This notification can also be tapped for more detailed information.



4. HARDENING EXCHANGE SERVICES

4.1 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).



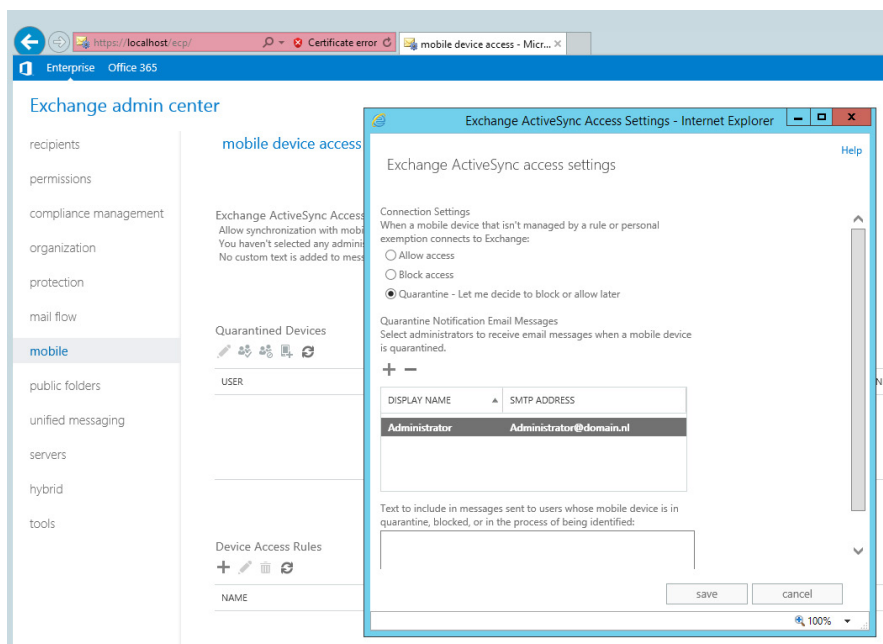
Recent research has shown that some of these services (for example: EWS) can be used to bypass MFA solutions⁸ like ESET Secure Authentication. To prevent this it is highly recommended to limit the access to these services from outside the company network.

⁸ <http://www.blackhillsinfosec.com/?p=5396>

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 Authentication 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.



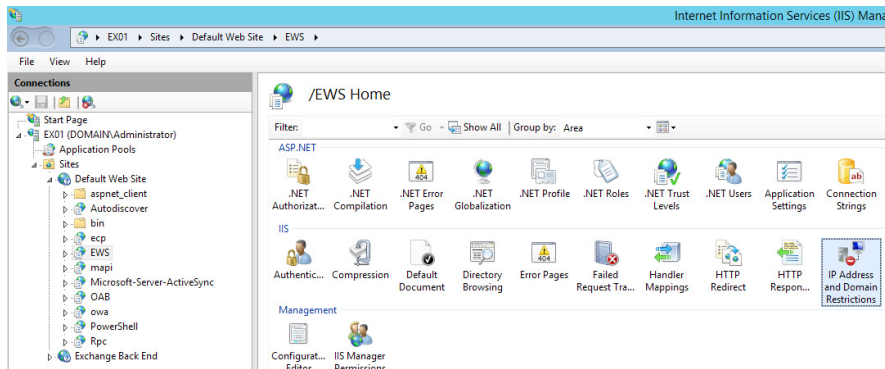
For more information, please refer to: <http://exchangeserverpro.com/preventing-new-activesync-device-types-from-connecting-to-exchange-server-2010/>.

4.3 EXCHANGE SERVICES

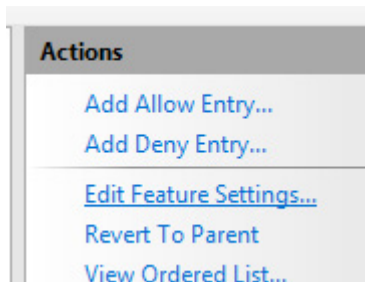
For all other publicly available services it is recommended to restrict access to the following services based on IP addresses:

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

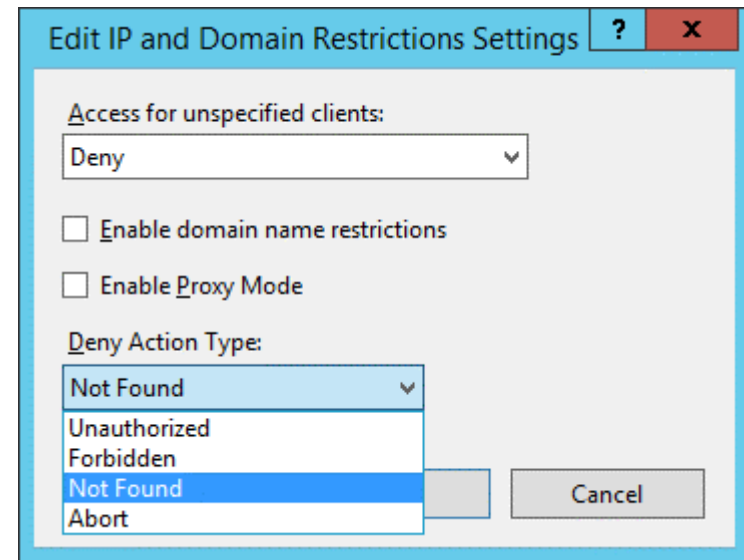
These restrictions can be set by opening up the OWA website in the IIS Manager, and then navigating to "IP Address and Domain Restrictions"⁹ for each of the aforementioned items.



Then, click on "Edit Feature Settings".

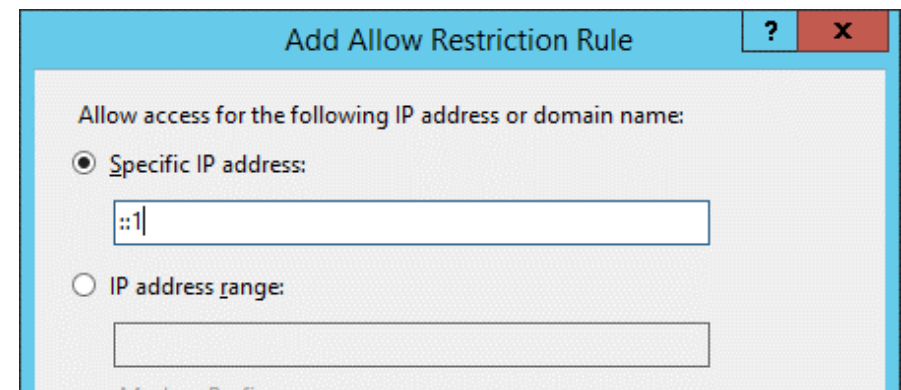


In the newly opened dialog, set "Access for unspecified clients" to "Deny". For security reasons it is recommended to also change the "Deny Action Type" to "Not Found". This can possibly deter automated scanners and inexperienced attackers looking for Microsoft Exchange servers to attack.



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

- 127.0.0.1
- ::1



⁹ This feature might need to be installed separately. Please refer to: [https://technet.microsoft.com/en-us/library/cc725769\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc725769(v=ws.10).aspx)

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

Allow access for the following IP address or domain name:

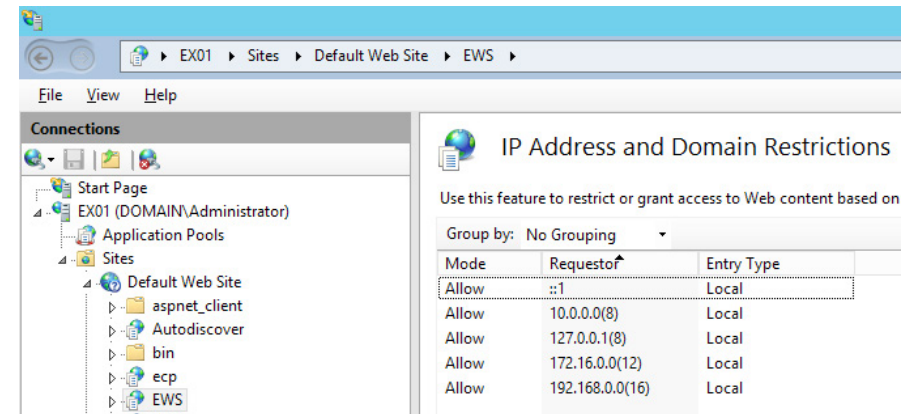
☐ Specific IP address:

☒ IP address range:

Mask or Prefix:

OK Cancel

Repeat this for all services.



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 surface 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 <https://www.eset.com/int/support/contact/>.