

ESET SECURE AUTHENTICATION

Product Manual

(intended for product version 2.4)



ESET SECURE AUTHENTICATION

Copyright © 2016 by ESET, spol. s r.o.

ESET Secure Authentication was developed by ESET, spol. s r.o.

For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care: www.eset.com/support

REV. 3/24/2016

Contents

1. Overview	5
2. Requirements	5
2.1 Supported Operating Systems	5
2.2 Supported Web Applications	6
2.3 Supported Mobile Phone Operating Systems	6
2.4 Installation Requirements	7
2.5 Supported Active Directory Environments	8
2.6 Firewall exceptions	9
2.7 Policies	9
3. Installation	10
3.1 Installation of the Core components	11
3.2 Installation of the Remote Desktop plugin	14
3.3 Installation of the Web App plugin	15
3.4 Installation of Windows Login plugin	16
3.5 Basic Configuration	17
4. User Management - Provisioning	18
5. Custom delivery options	20
6. Windows Login protection	23
6.1 Master recovery key	24
7. VPN Protection	25
7.1 Configuration	25
7.2 Usage	27
7.3 RADIUS PAM modules on Linux/Mac	27
7.3.1 Mac OS - configuration	27
7.3.2 Linux - configuration	29
7.3.3 Other RADIUS configurations	32
8. Web Application Protection	36
8.1 Configuration	36
8.1.1 Allowing Non-2FA Users	37
8.2 Usage	37
9. Remote Desktop Protection	38
9.1 Configuration	38
9.1.1 Allowing Non-2FA Users	39
9.2 Usage	40
9.3 Remote Desktop Web Access	40
10. IP address whitelisting	41
11. Hard Tokens	42
11.1 Hard Token Management	42
11.1.1 Enable	43
11.1.2 Import	43
11.1.3 Delete	45
11.1.4 Resynchronize	45
11.2 Hard Token User Management	46
11.2.1 Enable and Assign	46
11.2.2 Revoke	48
12. API	48
12.1 Integration Overview	49
12.2 Configuration	49
12.3 Replacing the SSL Certificate	49

12.3.1	Prerequisites	49
12.3.2	Importing the New Certificate	50
12.3.3	Replacing the ESA Certificate.....	50
13.	Advanced User Management	51
13.1	User States	52
13.2	Provisioning Multiple Phones	61
13.3	Override Mobile Number Field	63
13.4	Groups Based User Management	63
14.	Advanced VPN Topics	64
14.1	VPN Authentication Options	64
14.1.1	SMS-based OTPs	64
14.1.2	On-demand SMS-based OTPs.....	65
14.1.3	Mobile Application.....	65
14.1.4	Hard Tokens.....	65
14.1.5	Migration from SMS-Based OTPs to Mobile Application.....	65
14.1.6	Non-2FA Pass-through.....	66
14.1.7	Access Control Using Group Membership.....	66
14.2	OTPs and Whitespace	66
14.3	ESA Authentication Methods and PPP Compatibility.....	66
15.	AD FS 3	67
16.	Auditing and Licensing	69
16.1	Auditing	69
16.2	Licensing	70
16.2.1	Overview.....	70
16.2.2	Warnings	70
16.2.3	License States.....	70
16.2.4	License Enforcement.....	71
17.	High Availability View	71
18.	Glossary	72

1. Overview

ESET Secure Authentication (ESA) adds Two Factor Authentication (2FA) to Microsoft Active Directory domains, that is, an one-time password (OTP) is generated and has to be supplied along the generally required username and password. The ESA product consists of the following components:

- The ESA Web Application plug-in provides 2FA to various Microsoft Web Applications.
- The ESA Remote Desktop plug-in provides 2FA for the Remote Desktop Protocol.
- The ESA RADIUS Server adds 2FA to VPN authentication.
- The ESA Authentication Service includes a REST-based API that can be used to add 2FA to custom applications.
- ESA Management Tools:
 - ESA User Management plug-in for Active Directory Users and Computers (ADUC) is used to manage users.
 - ESA Management Console, titled as ESET Secure Authentication Settings, is used to configure ESA.

ESA requires Active Directory infrastructure, since it stores data in the Active Directory data store. This means that there is no need for additional backup policies, since ESA data is automatically included in your Active Directory backups.

2. Requirements

An Active Directory domain is required to Install ESET Secure Authentication. The minimum supported functional level for an Active Directory domain is Windows 2000 Native.

The installer automatically selects the Authentication Service and Management Tools components. Should the user select a component that cannot be installed, the installer will inform them of the exact prerequisites that are outstanding.

2.1 Supported Operating Systems

ESET Secure Authentication Services and Management Tools have been tested and are supported on the following operating systems:

Server operating systems (SOS)

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Small Business Server 2008
- Windows Small Business Server 2011
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

Client operating systems (COS)

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

The Management Tools are also supported on client operating systems from Windows 7.

NOTE: When you install a RADIUS Server on Windows Small Business Server 2008 or 2011, the default NPS port must be changed from 1812 to 1645. Verify that there are no processes listening on port 1812 before installing ESA by running the following command: `C:\> netstat -a -p udp | more`

2.2 Supported Web Applications

ESET Secure Authentication provides 2FA for the following Microsoft products:

- Microsoft Exchange 2007
 - Outlook Web Access - Exchange Client Access Server (CAS)
- Microsoft Exchange 2010
 - Outlook Web App - Exchange Client Access Server (CAS)
 - Exchange Control Panel
- Microsoft Exchange 2013
 - Outlook Web App - Exchange Client Access Server (CAS)
 - Exchange Admin Center
- Microsoft Dynamics CRM 2011
- Microsoft Dynamics CRM 2013
- Microsoft Dynamics CRM 2015
- Microsoft SharePoint 2010 *
- Microsoft SharePoint 2013 *
- Microsoft Remote Desktop Web Access
- Microsoft Terminal Services Web Access
- Microsoft Remote Web Access

* Foundation version is not supported

2.3 Supported Mobile Phone Operating Systems

The ESET Secure Authentication Mobile app is compatible with the following mobile phone operating systems:

- iPhone iOS 4.3 to iOS9
- Android™ 2.1 to Android M
- Windows Phone 7 to Windows Phone 10
- Windows Mobile 6
- BlackBerry® 4.3 to 7.1
- BlackBerry® 10
- Symbian® - all supporting J2ME
- All J2ME enabled phones

2.4 Installation Requirements

Secure installation requires outbound connectivity to esa.eset.com on TCP port 443. The installer must be run by a member of the "Domain Administrators" security group. Another requirement for running the installer is .NET Framework Version 4 (Full Install). The installer will automatically attempt to install .NET 4 if it is not already installed.

ESA supports the installation of components in a distributed environment, with all components installed on computers that are joined to the same Windows domain.

Windows Firewall exceptions essential for the proper function of ESET Secure Authentication will be added automatically as part of installation. If you use a different firewall solution, see [Firewall exceptions](#) for information about important exceptions that you will need to create.

The prerequisites for the installation of each component are:

- Authentication Service:
 - Windows 2003 Server SP2 or later [SOS](#) in the list of [Supported Operating Systems](#)
 - The installer must be run as a user who is a member of the "Schema Admins" security group the first time an Authentication Service is installed on the domain.
- Management Tools:
 - Windows 7 or later [COS](#) in the list of [Supported Operating Systems](#), Windows 2003 Server SP2 or later [SOS](#) in the list of [Supported Operating Systems](#)
 - .NET Framework version 3.5
 - Windows Remote Server Administration Tools, Active Directory Domain Services component (RSAT AD DS)
 - **NOTE:** RSAT was previously known as the Remote Administration Pack (adminpack) and is downloadable from Microsoft. In Windows Server 2008 and later, this component may be installed from the "Add Feature" wizard in the Server Manager. All Domain Controllers already have these components installed.
- RADIUS Server:
 - Windows 2003 Server SP2 or later [SOS](#) in the list of [Supported Operating Systems](#)
- Web App Plug-in for Microsoft Exchange Server:
 - Microsoft Exchange Server 2007 or later (64-bit only), with the Client Access role (Outlook Web App / Outlook Web Access) installed
 - .NET Framework version 3.5
 - Internet Information Services 7 (IIS7) or later
- Web App Plug-in for Microsoft SharePoint Server:
 - Microsoft SharePoint Server 2010 or 2013 (64-bit only)
 - .NET Framework version 3.5
- Web App Plug-in for Microsoft Dynamics CRM:
 - Microsoft Dynamics CRM 2011, 2013 or 2015
 - .NET Framework version 3.5
- Web App Plug-in for Microsoft Terminal Services Web Access:
 - The Terminal Services role with the Terminal Services role service installed on Windows Server 2008
 - .NET Framework version 3.5
- Web App Plug-in for Microsoft Remote Desktop Services Web Access:
 - The Remote Desktop Services role with the Remote Desktop Web Access role service installed on Windows Server 2008 R2 and later [SOS](#) in the list of [Supported Operating Systems](#)
 - .NET Framework version 3.5
- Web App Plug-in for Microsoft Remote Web Access:

- The Remote Web Access role service installed on Windows SBS 2008 where it is called Remote Web Access, Windows SBS 2011, Windows Server 2012 Essentials and Windows Server 2012 Essentials R2
- .NET Framework version 3.5
- Remote Desktop Protection:
 - Windows Server 2008 R2 or later [SOS](#) in the list of [Supported Operating Systems](#)
 - Microsoft Windows 7 or later [COS](#) in the list of [Supported Operating Systems](#)
 - Only 64-bit operating systems are supported
- Windows login protection:
 - Windows Server 2008 R2 or later [SOS](#) in the list of [Supported Operating Systems](#)
 - Windows 7 or later [COS](#) in the list of [Supported Operating Systems](#)
- ADFS 3.0 protection:
 - Windows Server 2012 R2

.NET Requirements:

- All components: .NET 4 or 4.5 Full Install
- Core Server: .NET 4 or 4.5 Full Install
- RADIUS Server: .NET 4 or 4.5 Full Install
- Management Tools: .NET 3.5 (4 on Windows Server 2012)
- Web App Plugin: .NET 3.5

NOTE: The Authentication Service and RADIUS Server components are compatible with Windows7 and later [COS](#) in the list of [Supported Operating Systems](#), but will not be supported on these client operating systems.

2.5 Supported Active Directory Environments

ESET Secure Authentication supports either single domain or multiple domain Active Directory environments. The differences between these environments and their installation requirements are detailed below.

Single Domain, Single Forest

This is the simplest configuration, and the installer may be run as any Domain Admin. ESET Secure Authentication is available to all users within the domain.

Multiple Domain, Single Forest

In this deployment, a parent domain such as `example.corp` has multiple sub-domains such as `branch1.example.corp` and `branch2.example.corp`. ESET Secure Authentication may be deployed on any of the domains in the forest, but there is no cross-communication between the installations. Each installation will require it's own ESET Secure Authentication license.

In order to install ESET Secure Authentication on a sub-domain, the installer must be launched as a Domain Admin user from the top level domain.

For example, using the example domains defined previously:

To install ESET Secure Authentication on `server01.branch1.example.corp`, log on to `server01` as the `example.corp \Administrator` user (or any other Admin from `example.corp`). After installation, ESET Secure Authentication will be available to any user within the `branch1.example.corp` domain.

Multiple Domain, Multiple Forest

This is identical to the previous environment, in that ESET Secure Authentication installations on separate forests are not aware of each other.

2.6 Firewall exceptions

Windows Firewall exceptions essential for the proper function of ESET Secure Authentication will be added automatically as part of installation. If you use a different firewall, the following exceptions must be defined in that firewall manually:

Exception Name: ESET Secure Authentication Core Service

Scope: Any

Protocol: TCP

Local Port: 8000

Remote Ports: All

Exception Name: ESET Secure Authentication API

Scope: Any

Protocol: TCP

Local Port: 8001

Remote Ports: All

Exception Name: ESET Secure Authentication RADIUS Service

Scope: Any

Protocol: UDP

Local Port: 1812

Remote Ports: All

Exception Name: ESET Secure Authentication RADIUS Service (Alternative Port)

Scope: Any

Protocol: UDP

Local Port: 1645


Remote Ports: All

2.7 Policies

During installation ESA adds ESA_<computer name> user to the Log on as a service entity found at Local Security Policies > Local Policies > User Rights Assignments, while the <computer name> is replaced with the the name of the computer where ESA is being installed. This is essential to run the ESET Secure Authentication Service service that is started automatically when the operating system starts.

If you use Group Policy and you have the Log on as service defined there (Group Policy Management > <Forest> > Domains > <domain> > Default Domain Policy > Settings > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies), then you must add the ESA_<computer name> user to the Log on as a service entity there or not have the Log on as a service defined there at all.

To find the name of the computer where you are installing ESA:

- Press the **Windows key**  and **E** simultaneously so that the **File Explorer** shows up
- In the right pane right-click **This PC** or **Computer** and select **Properties**.

A window will display the **Computer name** and the name of the particular computer.

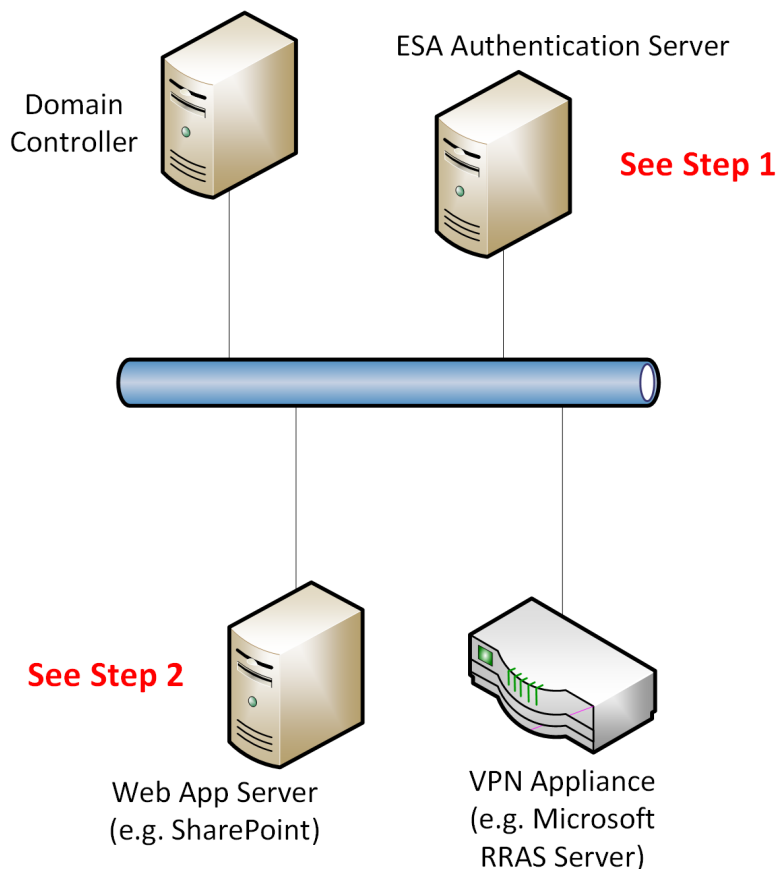
3. Installation

All of the following components are required for your first ESA installation:

- At least one instance of the Authentication Server
- At least one instance of the Management Tools
- At least one of the authentication endpoints (API, Web Application, Remote Desktop, or RADIUS)

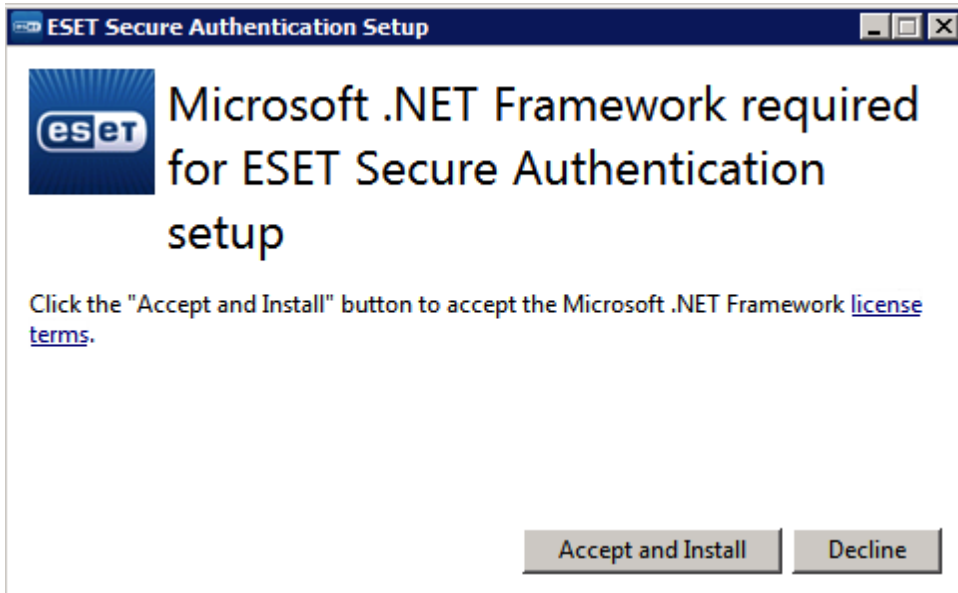
All the components may be installed on a single machine, or they may be installed across multiple machines in a distributed environment. As is the case with distributed systems, there are many possible installation scenarios.

The example below illustrates a generic installation scenario; however, this example can serve as a basic guide for other deployment scenarios. The example installation consists of two sequences—after completing both, your deployment will correspond with the figure below.

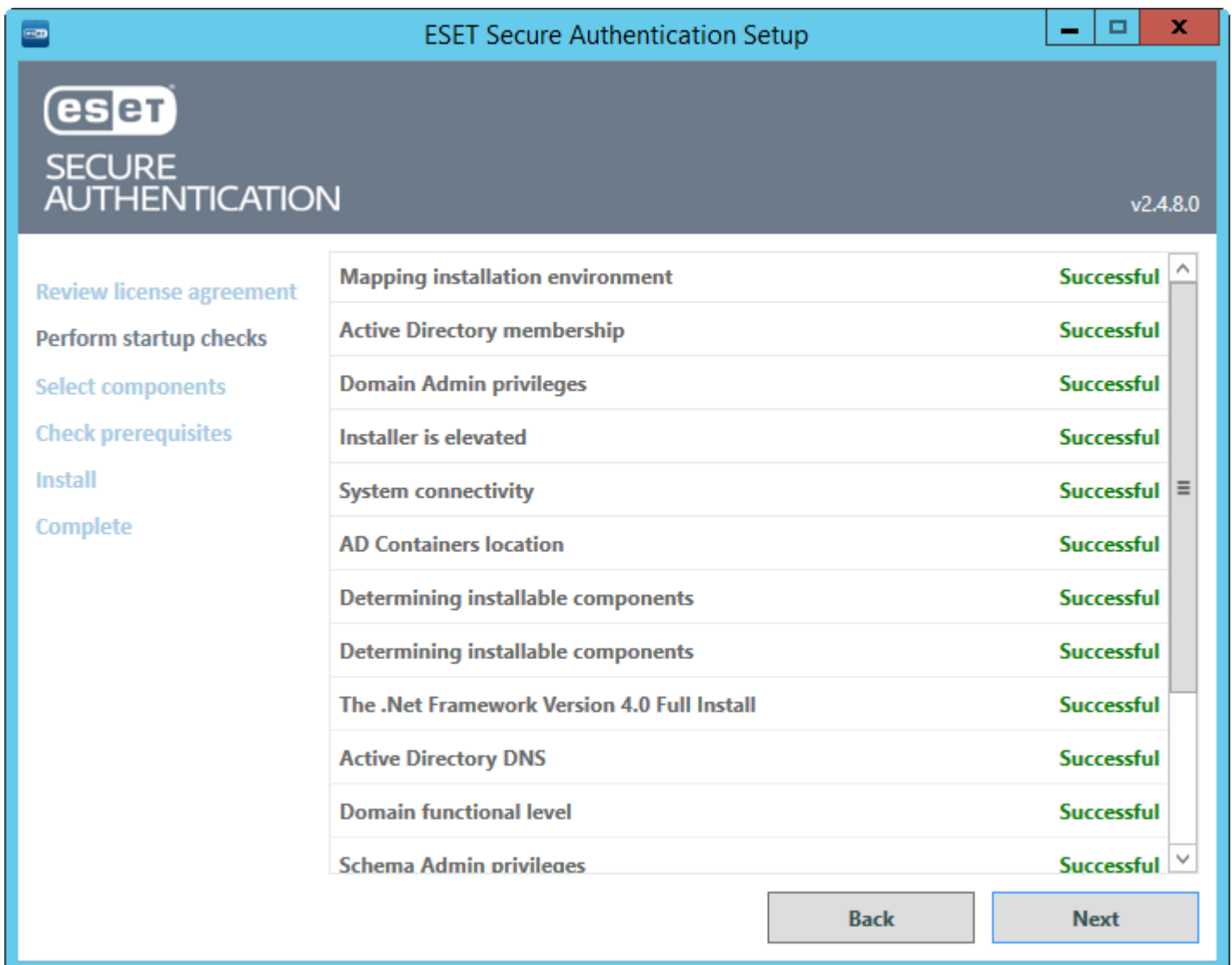


3.1 Installation of the Core components

Run the supplied .exe file to start installation on the machine hosting the ESA Authentication Service. The .NET Framework version 4.0 will be installed automatically if it is not detected.

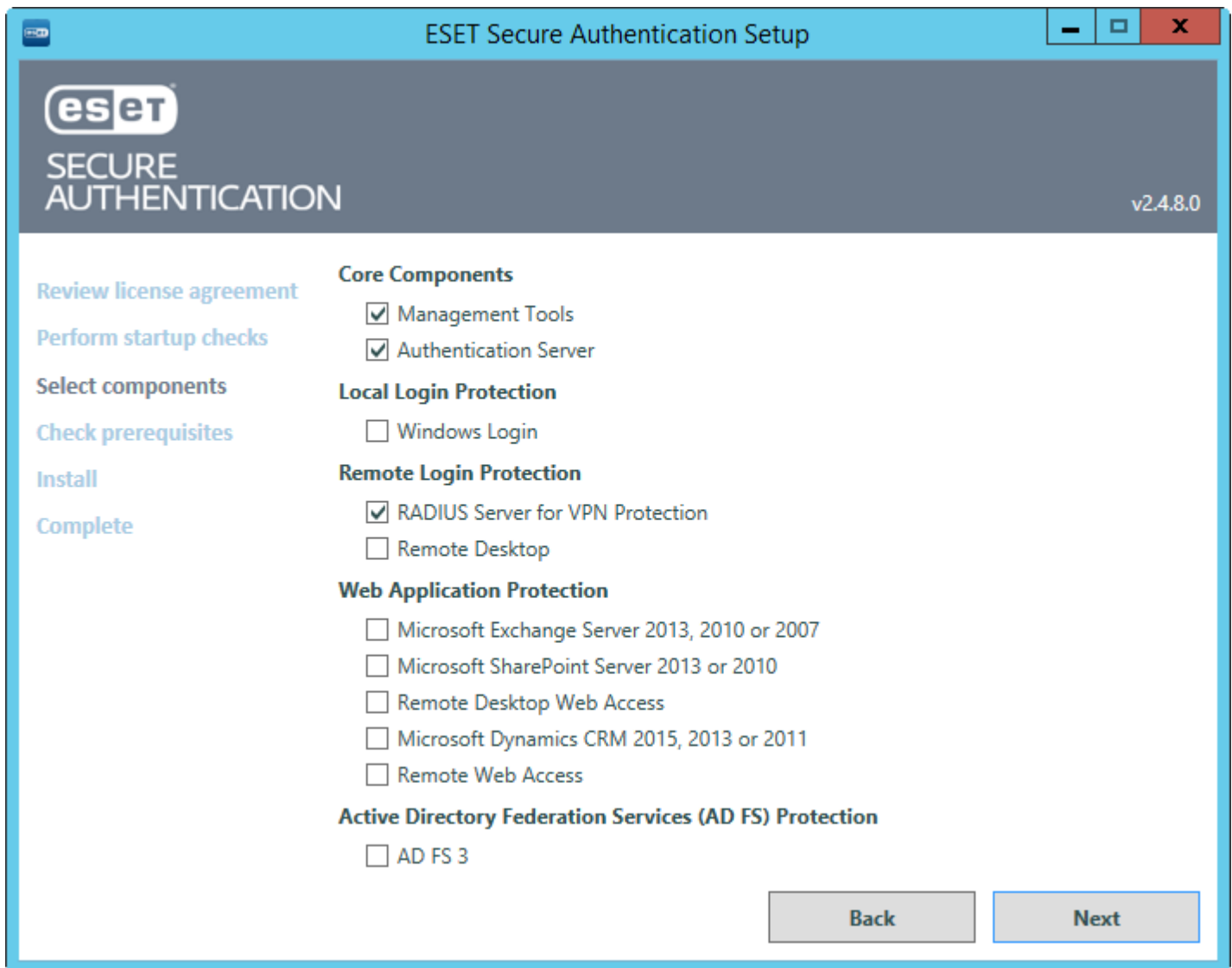


A number of prerequisite checks will be performed to ensure that the domain is healthy and that ESA can be installed. Any failures must be corrected before installation can proceed. Installation will continue when all prerequisites are successfully completed.



If the **Next** button is not available for more than 5 seconds, scroll down to see which requirements are still being checked.

When prompted, make sure that the "Management Tools", "Authentication Server" and "RADIUS Server for VPN Protection" components are selected, as per the figure below.

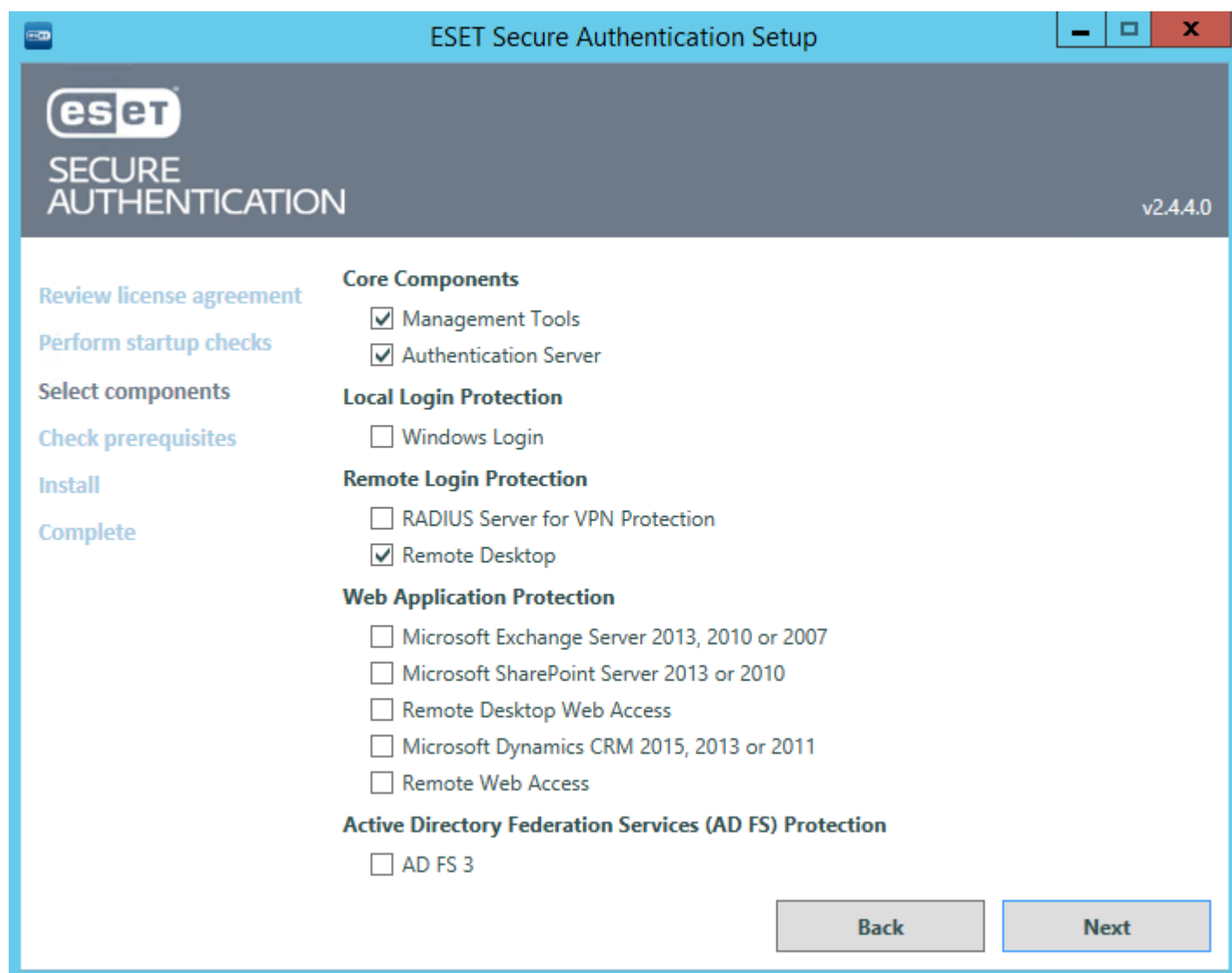


Go through the remainder of the steps as prompted by the installer and close the installer when complete.

3.2 Installation of the Remote Desktop plugin

From the Remote Desktop Access machine that is to be protected, run the supplied .exe file to start the installation. The installer will run a number of prerequisite checks as was done during the [Installation of the Core components](#).

The figure below shows the component selection for the installation of the Remote Desktop plugin.

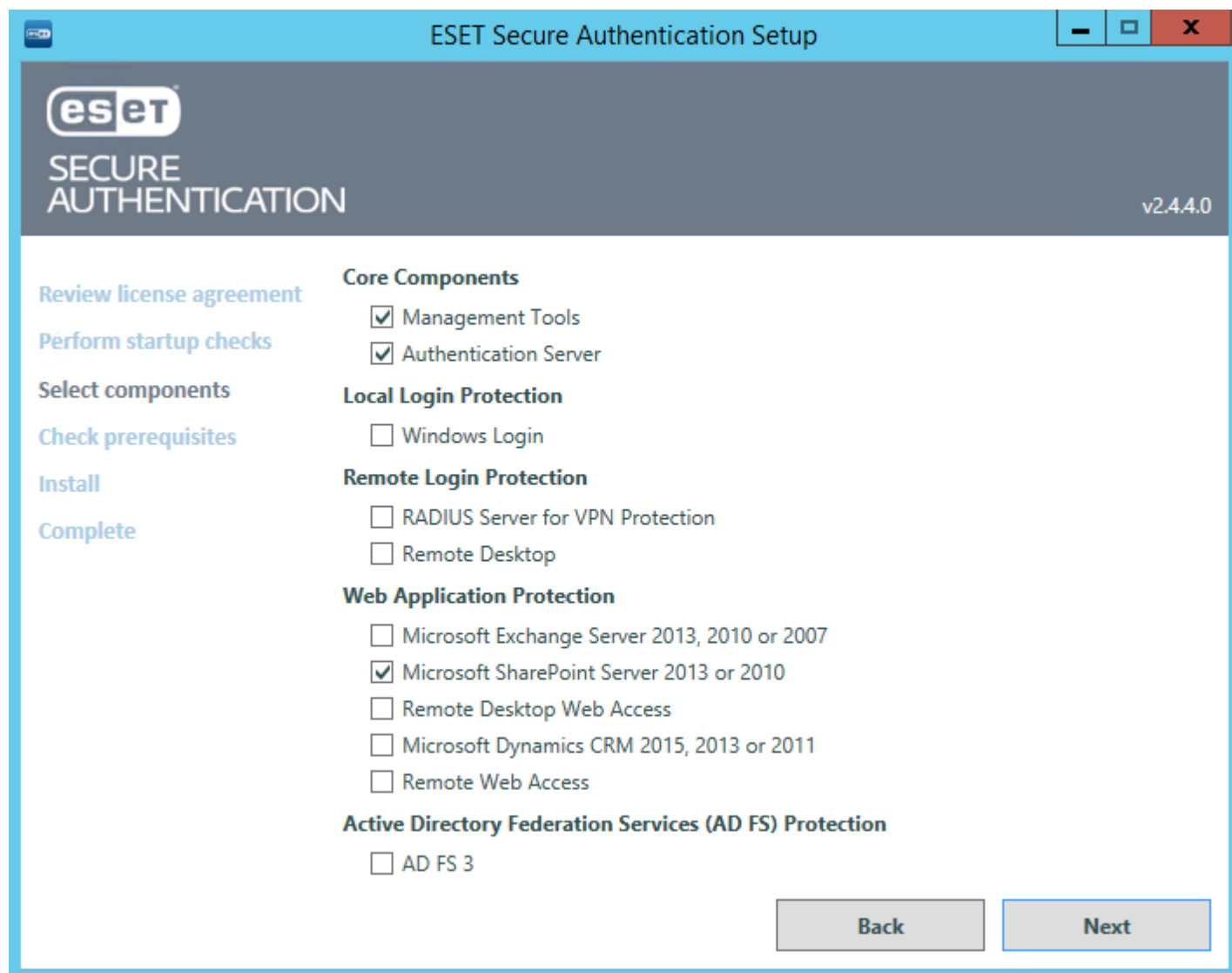


Prerequisite checks will be run to ensure that the ESA Remote Desktop plugin can be installed. Any failures must be corrected before the installation can proceed. Go through the remainder of the steps as prompted by the installer and close the installer when complete.

3.3 Installation of the Web App plugin

From the machine running the Web App that is to be protected, run the supplied .exe file to start the installation. The installer will run a number of prerequisite checks as was done during the [Installation of the Core components](#).

When prompted, make sure that the component for the appropriate Web App is selected. The figure below shows the component selection for the installation of the SharePoint Server plugin.

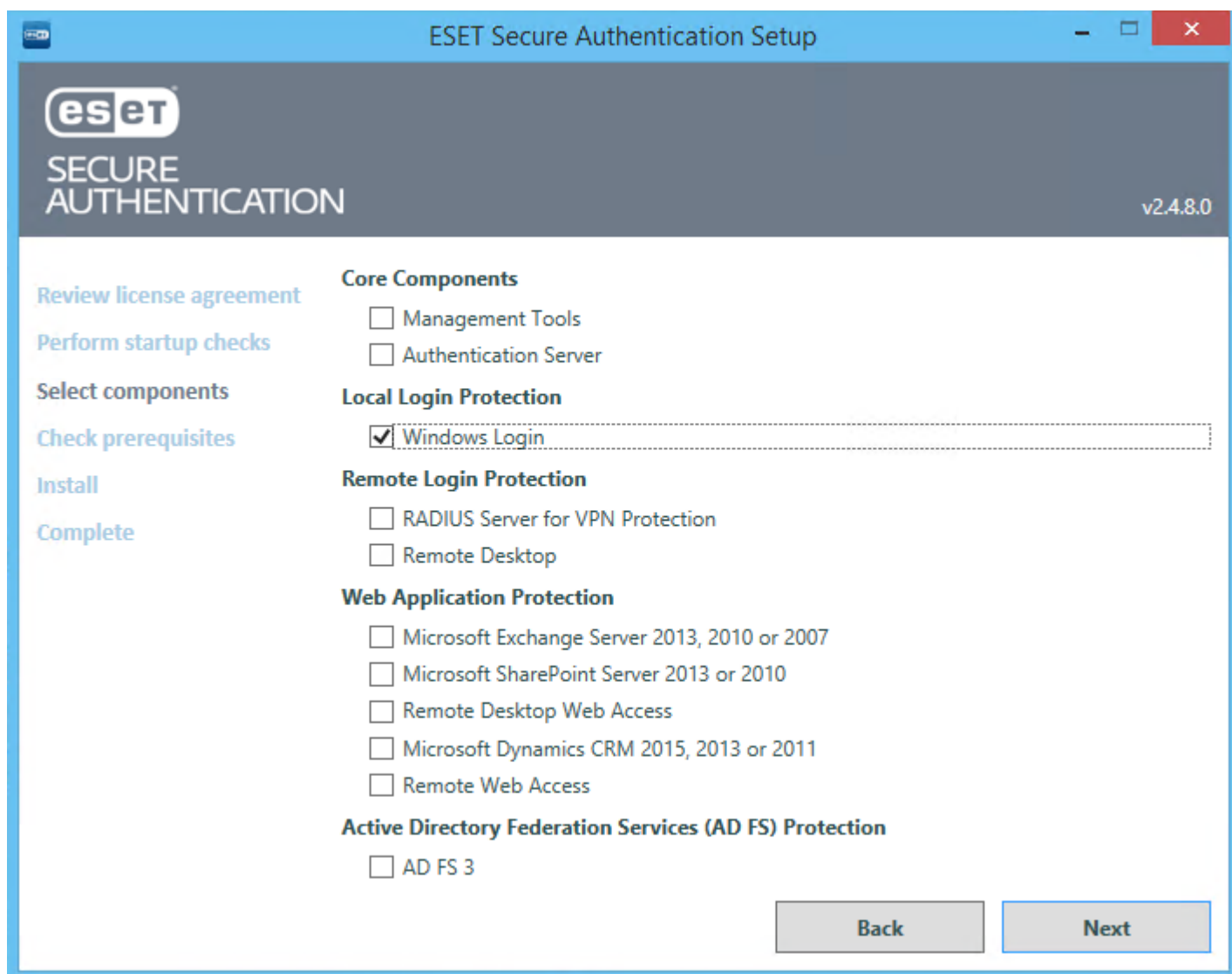


Prerequisite checks will be run to ensure that the Web App is running on the server and that the ESA Web App plugin can be installed. Any failures must be corrected before the installation can proceed.

Go through the remainder of the steps as prompted by the installer and close the installer when complete.

3.4 Installation of Windows Login plugin

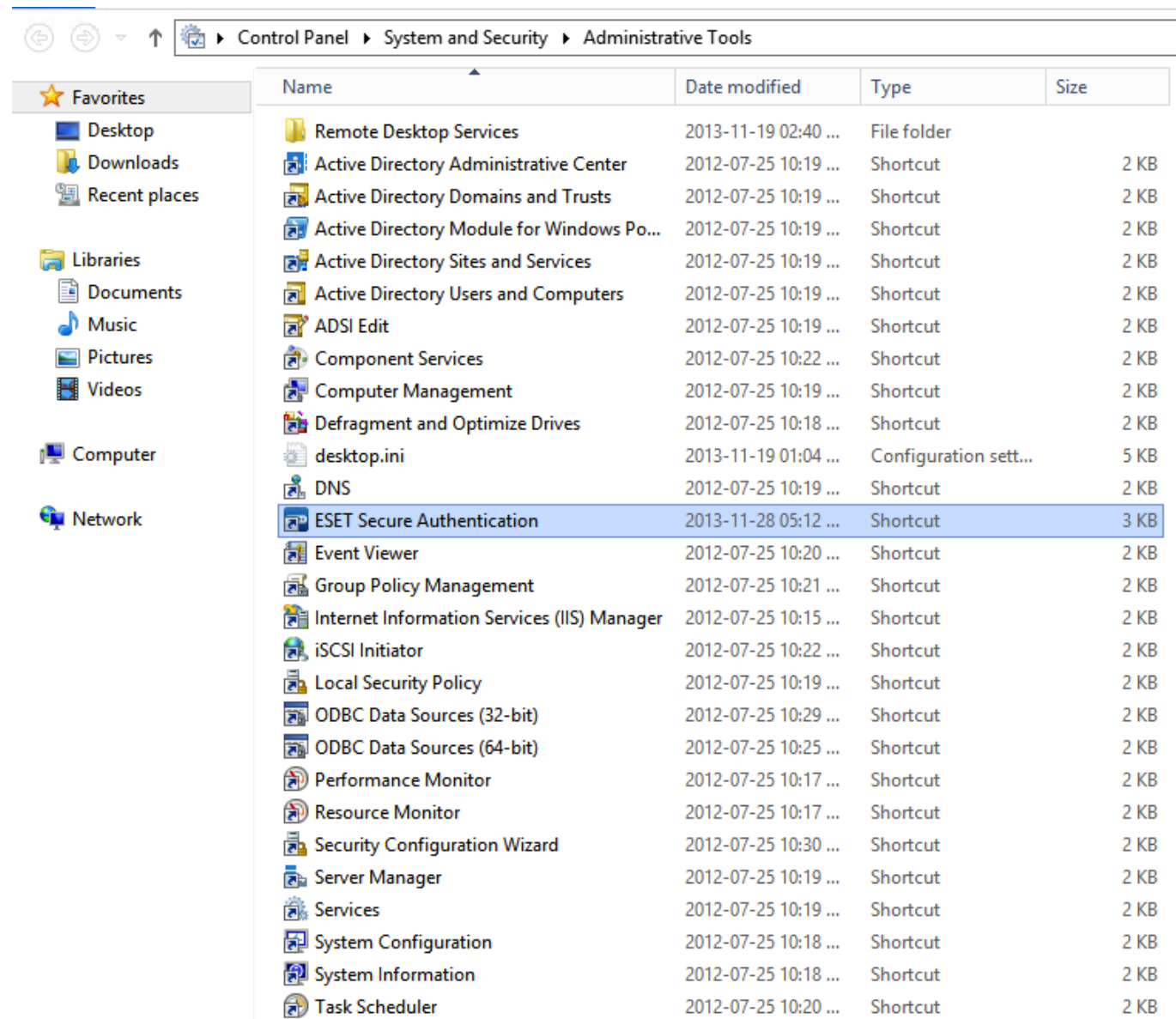
When installing ESA on the Windows machine you want to secure with 2FA, make sure you select the **Windows Login** component in the **Select components** page of installation wizard.



NOTE: There is no need to install the **Management Tools** component on each computer you want to protect with 2FA (this component is only required on your primary ESA Server). **Windows Login** protection works only in a domain environment, which means both the the particular computer and the user account must belong to a domain established by Active Directory Domain Services.

3.5 Basic Configuration

Once you have installed the required components, some basic configuration is necessary. All configuration of the ESA system is performed via the ESA Management Console. The ESA Management Console is added as a Snap-In to the standard MMC console. The ESA Management Console may be accessed under Administrative Tools, as per the figure below.



The screenshot shows the Windows Administrative Tools console. The breadcrumb path is Control Panel > System and Security > Administrative Tools. The left sidebar shows navigation options like Favorites, Libraries, and Computer. The main pane displays a list of administrative tools. 'ESET Secure Authentication' is highlighted in blue.

Name	Date modified	Type	Size
Remote Desktop Services	2013-11-19 02:40 ...	File folder	
Active Directory Administrative Center	2012-07-25 10:19 ...	Shortcut	2 KB
Active Directory Domains and Trusts	2012-07-25 10:19 ...	Shortcut	2 KB
Active Directory Module for Windows Po...	2012-07-25 10:19 ...	Shortcut	2 KB
Active Directory Sites and Services	2012-07-25 10:19 ...	Shortcut	2 KB
Active Directory Users and Computers	2012-07-25 10:19 ...	Shortcut	2 KB
ADSI Edit	2012-07-25 10:19 ...	Shortcut	2 KB
Component Services	2012-07-25 10:22 ...	Shortcut	2 KB
Computer Management	2012-07-25 10:19 ...	Shortcut	2 KB
Defragment and Optimize Drives	2012-07-25 10:18 ...	Shortcut	2 KB
desktop.ini	2013-11-19 01:04 ...	Configuration sett...	5 KB
DNS	2012-07-25 10:19 ...	Shortcut	2 KB
ESET Secure Authentication	2013-11-28 05:12 ...	Shortcut	3 KB
Event Viewer	2012-07-25 10:20 ...	Shortcut	2 KB
Group Policy Management	2012-07-25 10:21 ...	Shortcut	2 KB
Internet Information Services (IIS) Manager	2012-07-25 10:15 ...	Shortcut	2 KB
iSCSI Initiator	2012-07-25 10:22 ...	Shortcut	2 KB
Local Security Policy	2012-07-25 10:19 ...	Shortcut	2 KB
ODBC Data Sources (32-bit)	2012-07-25 10:29 ...	Shortcut	2 KB
ODBC Data Sources (64-bit)	2012-07-25 10:25 ...	Shortcut	2 KB
Performance Monitor	2012-07-25 10:17 ...	Shortcut	2 KB
Resource Monitor	2012-07-25 10:17 ...	Shortcut	2 KB
Security Configuration Wizard	2012-07-25 10:30 ...	Shortcut	2 KB
Server Manager	2012-07-25 10:19 ...	Shortcut	2 KB
Services	2012-07-25 10:19 ...	Shortcut	2 KB
System Configuration	2012-07-25 10:18 ...	Shortcut	2 KB
System Information	2012-07-25 10:18 ...	Shortcut	2 KB
Task Scheduler	2012-07-25 10:20 ...	Shortcut	2 KB

First, you must activate your ESA system using an ESA license. This license can be obtained from your ESET distributor, or the demo license (in *License.txt*) shipped with the installer can be used.

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.
4. The ESA Server will obtain its license automatically and display the current license information.

Once your license is active, configure your token name under Basic Settings. This is your company's token name that will display in the Mobile Application on user's phones.

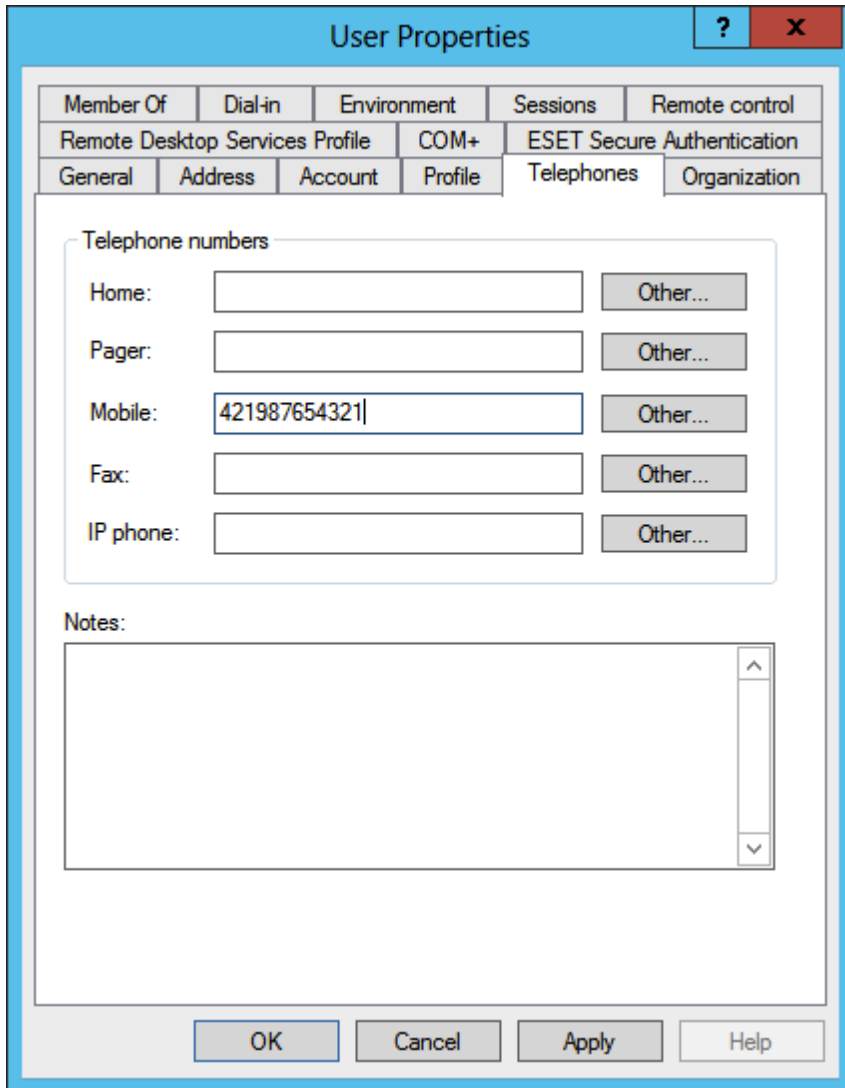
If you wish to configure a Web Application, jump to the [Web Application Protection](#) chapter. For configuring 2FA on your VPN, go to the [VPN Protection](#) chapter. To configure 2FA for Remote Desktop, see the [Remote Desktop Protection](#) chapter.

4. User Management - Provisioning

All user management is done via the Active Directory Users and Computers management interface. All ESA users must have valid mobile phone numbers in the **Mobile** field of the **Telephones** tab.

Provisioning a new Mobile App:

1. Open the normal ADUC user view.
2. Right-click a **User** and select **Properties**.
3. Type the user's mobile phone number into the **Mobile** field.



The screenshot shows the 'User Properties' dialog box with the 'Telephones' tab selected. The 'Telephone numbers' section contains five rows: Home, Pager, Mobile, Fax, and IP phone. Each row has a text input field and an 'Other...' button. The 'Mobile' field contains the number '421987654321'. Below this section is a 'Notes' text area. At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Member Of	Dial-in	Environment	Sessions	Remote control	
Remote Desktop Services Profile	COM+	ESET Secure Authentication			
General	Address	Account	Profile	Telephones	Organization

Telephone numbers

Home: Other...

Pager: Other...

Mobile: Other...

Fax: Other...

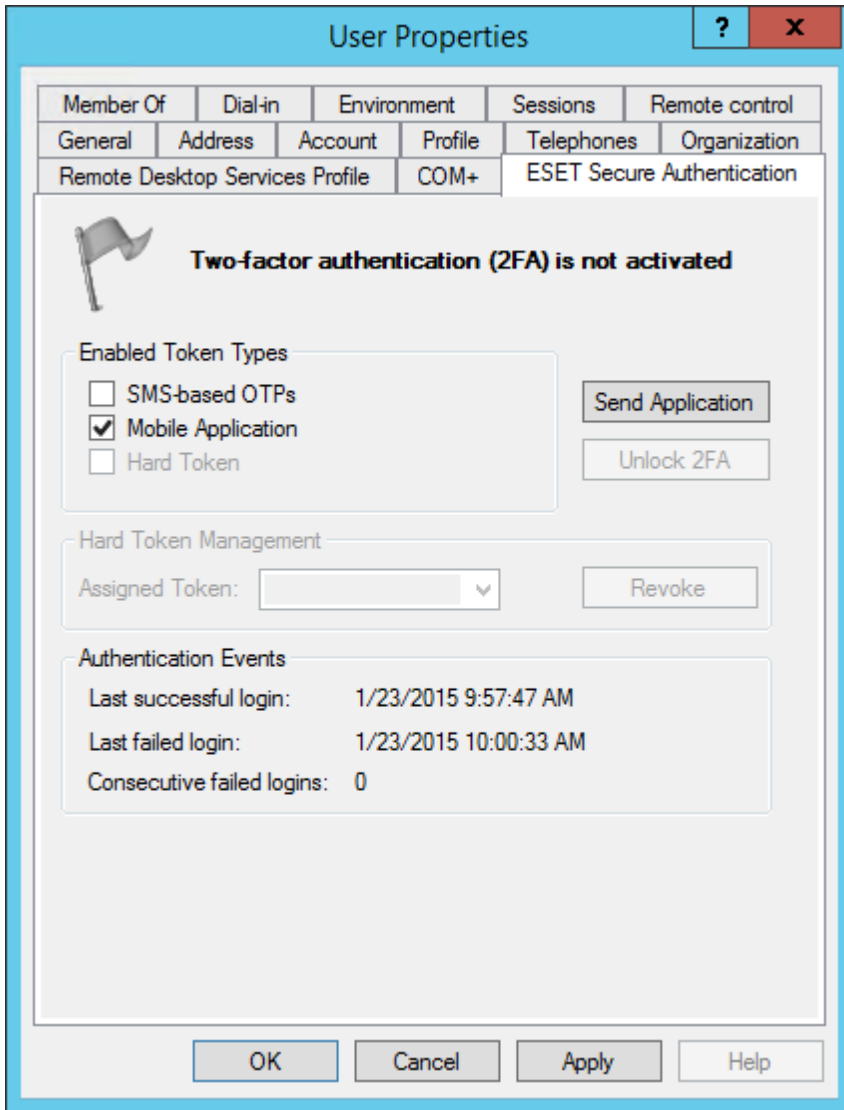
IP phone: Other...

Notes:

OK Cancel Apply Help

NOTE: Mobile numbers must consist entirely of digits (for example, they must be in the format 421987654321, where 4 is the country code and 21 is the area code).

Click the **ESET Secure Authentication** tab to manage ESET Secure Authentication settings for a specific user.



Enabling soft-token OTPs for a specific user:

1. Make sure that the check box next to **Mobile Application** is selected.
2. Click **Send Application**.
3. The user will receive an SMS message containing a link that can be used to install the application.

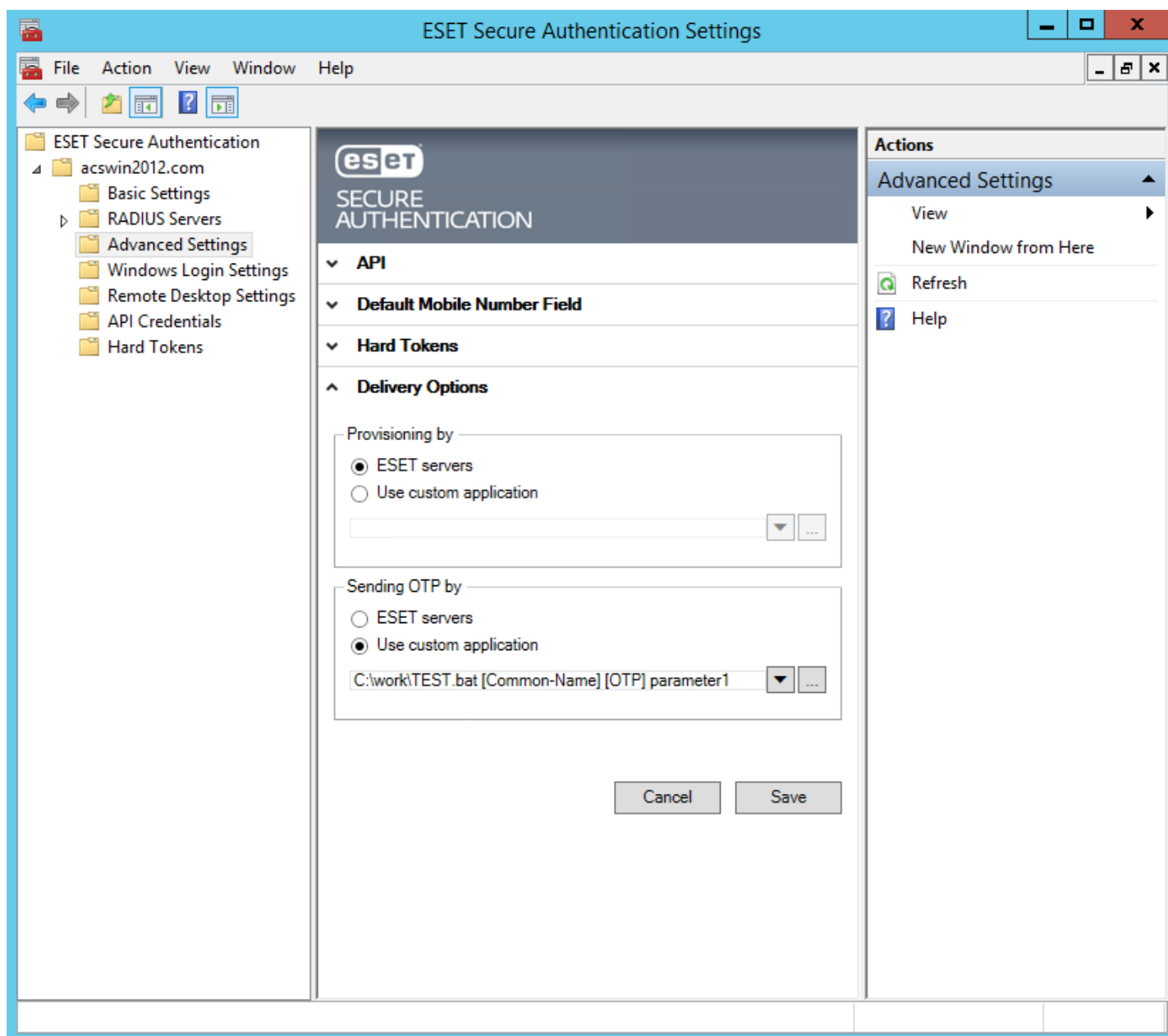
Instructions on installing and using the mobile application (click the desired mobile OS to be redirected to the corresponding article):



- [Android](#)
- [BlackBerry](#)
- [iPhone](#)
- [Windows Phone](#)

5. Custom delivery options

The default delivery options of OTP ([sms](#), [mobile app](#)) work perfect for most users, ESA can accommodate custom delivery options as well.

Open the ESA Management Console on your main computer, navigate to your domain node (in our example **acswin2012.com**), click **Advanced Settings** and then click **Delivery Options**.



Here you can specify the path to your custom script (or look up the custom script by clicking the  button) by which you wish to handle provisioning or delivery of OTP. Click  to view a list of parameters you can use to be passed to your custom script. For example, in order to deliver the OTP you must use the [OTP] parameter. You can also specify a custom string to be passed to your script (see **parameter1** in the screenshot above).

Sample scenario - delivering OTP via e-mail

Prerequisite:

- know the SMTP details of the email gateway we wish to use for sending the email message containing the OTP
- have a custom script for sending email messages
- have a custom .bat script we define the path to it in ESA Management Console as shown in the screenshot above, while this .bat script is going to call our custom script that is supposed to send the email message

- every 2FA-enabled user that receives OTP passwords via e-mail must have their e-mail address defined in the **E-mail** field of the **General** tab when viewing their details through the Active Directory Users and Computers management interface.

Sample python script for sending email - we name the file as **sendmail.py**:

```
import sys, smtplib
server = smtplib.SMTP('smtpserver:port')
server.starttls()
server.login('username', 'password')
server.sendmail(sys.argv[1], sys.argv[1], 'Subject: OTP is '+sys.argv[2])
server.quit()
```

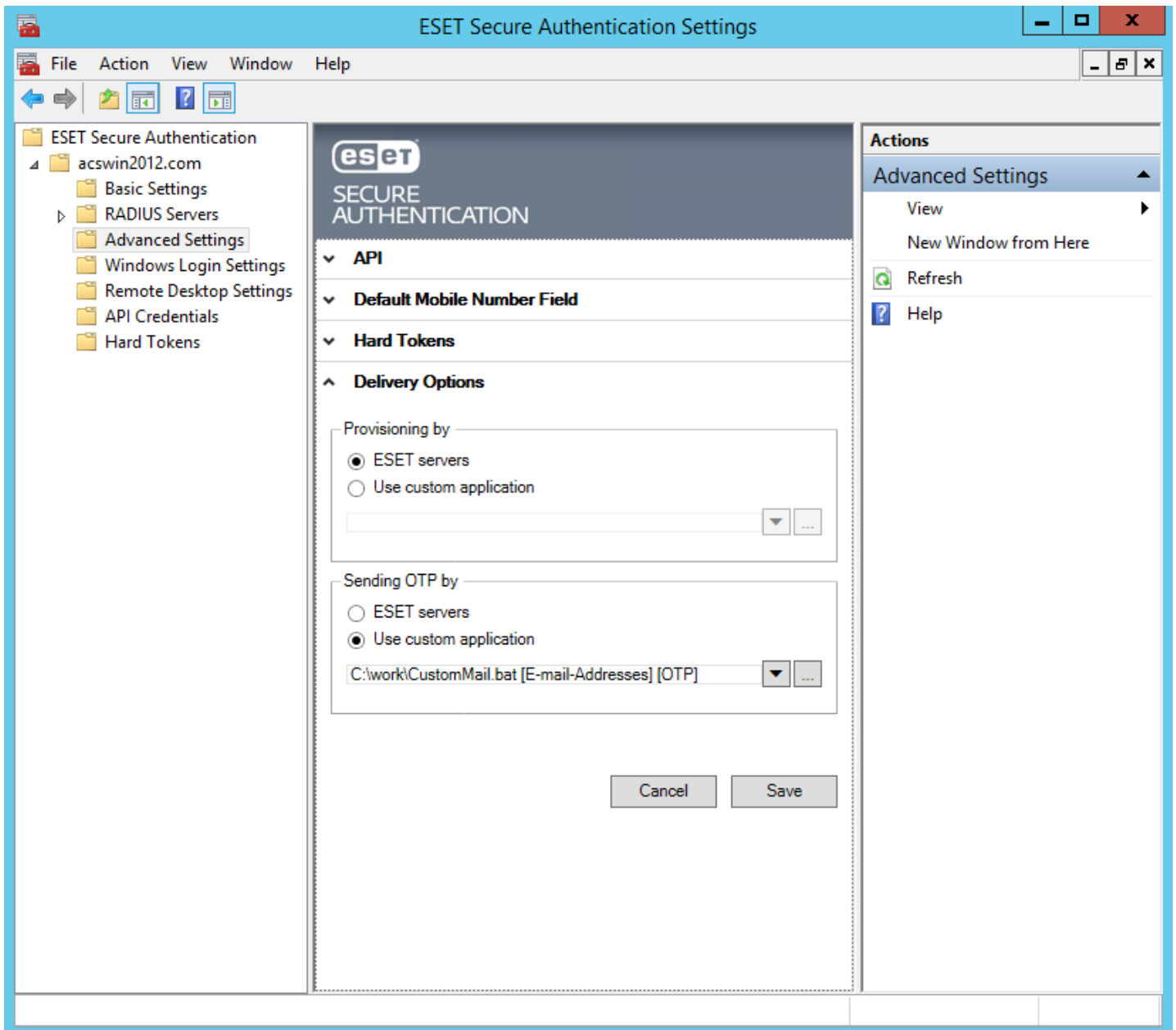
NOTE: In the sample python script above the smtpserver:port, username and password are supposed to be replaced with the corresponding SMTP details.

Sample .bat script for calling the sendmail.py script while passing the essential parameters to it - we name the file as **CustomMail.bat**:

```
c:\Python\python.exe c:\work\sendmail.py %1 %2
```

NOTE: This sample scenario assumes the python library is installed in your main computer where the ESA Core component is installed and you know the path to the python.exe file.

In the **Sending OTP by** field we define the path leading to our **CustomMail.bat** script, select the essential parameters such as [E-mail-Addresses] and [OTP] and then click **Save**

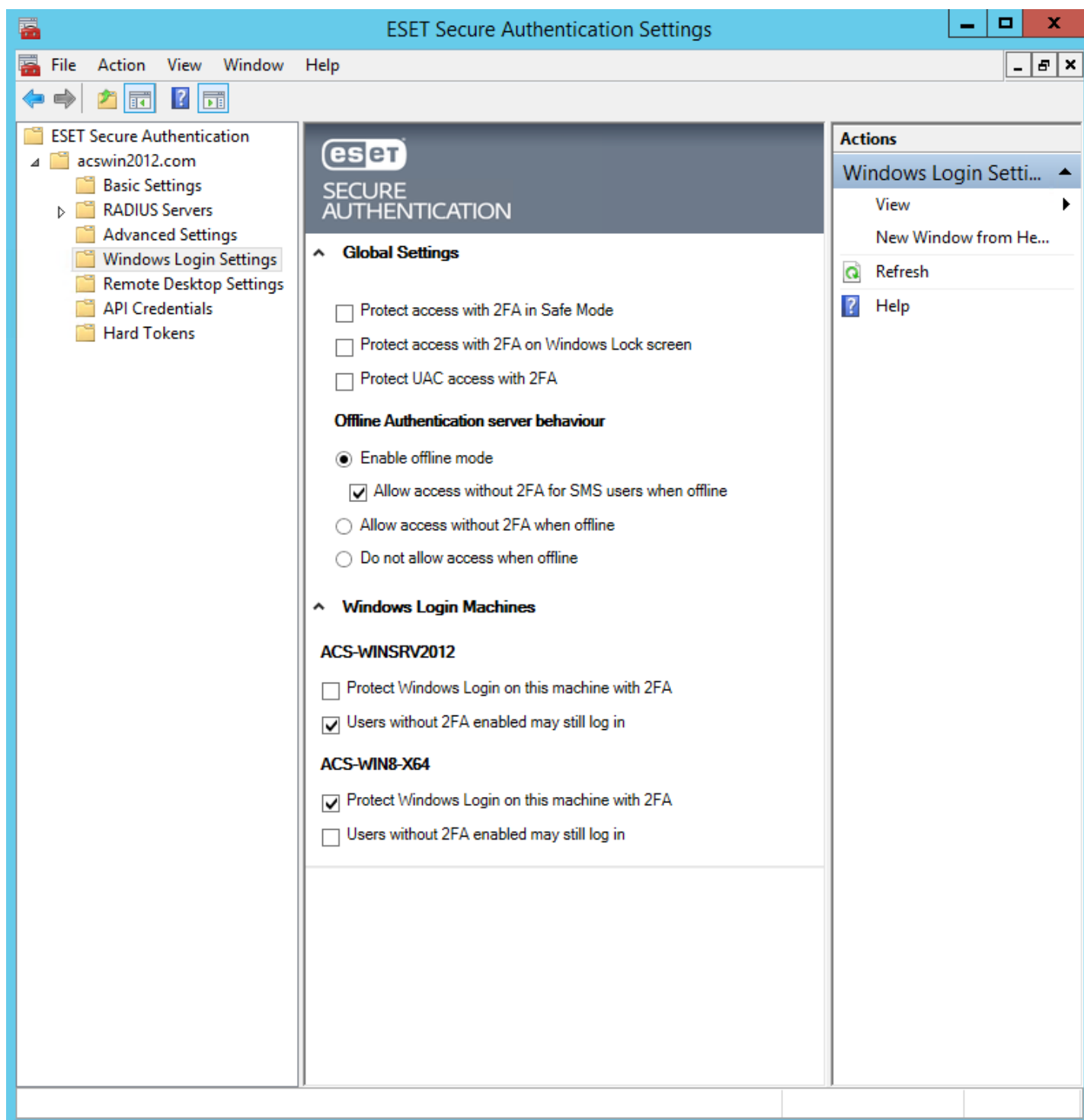


Provisioning (delivery of the [mobile application](#)) can be customized the same way using the essential parameters [PHONE] and [URL].

NOTE: Compared to SMS delivery (or usage of provisioned [mobile application](#)), the use of email as the means of OTP distribution is slightly less secure because the email message can be read on any device the user possesses. This method does not confirm that the intended recipient is in possession of the registered phone (phone number).

6. Windows Login protection

ESA features local login protection for Windows in a domain environment established by Active Directory Domain Services. To utilize this feature, it is essential to install the **Windows Login** component during [installation](#) of ESA. Once installation is finished, open the ESA Management Console on your main computer, navigate to your domain node (in our example acswin2012.com) and click **Windows Login Settings**.



From this screen you can see various options to apply 2FA, including the option to apply 2FA protection for Safe Mode, Windows lock screen and User Account Control (UAC). You can also view the list of computers where the **Windows Login** component of ESA is installed.

If the machine where the **Windows Login** component of ESA is installed, must be offline part of the time and you have users who have SMS authentication enabled, you can enable **Allow access without 2FA for SMS users when offline**.

If a user using SMS delivery for OTP wants to have an OTP re-sent, they can close the window requiring OTP and after 30 seconds enter their AD username and password again to receive a new OTP.

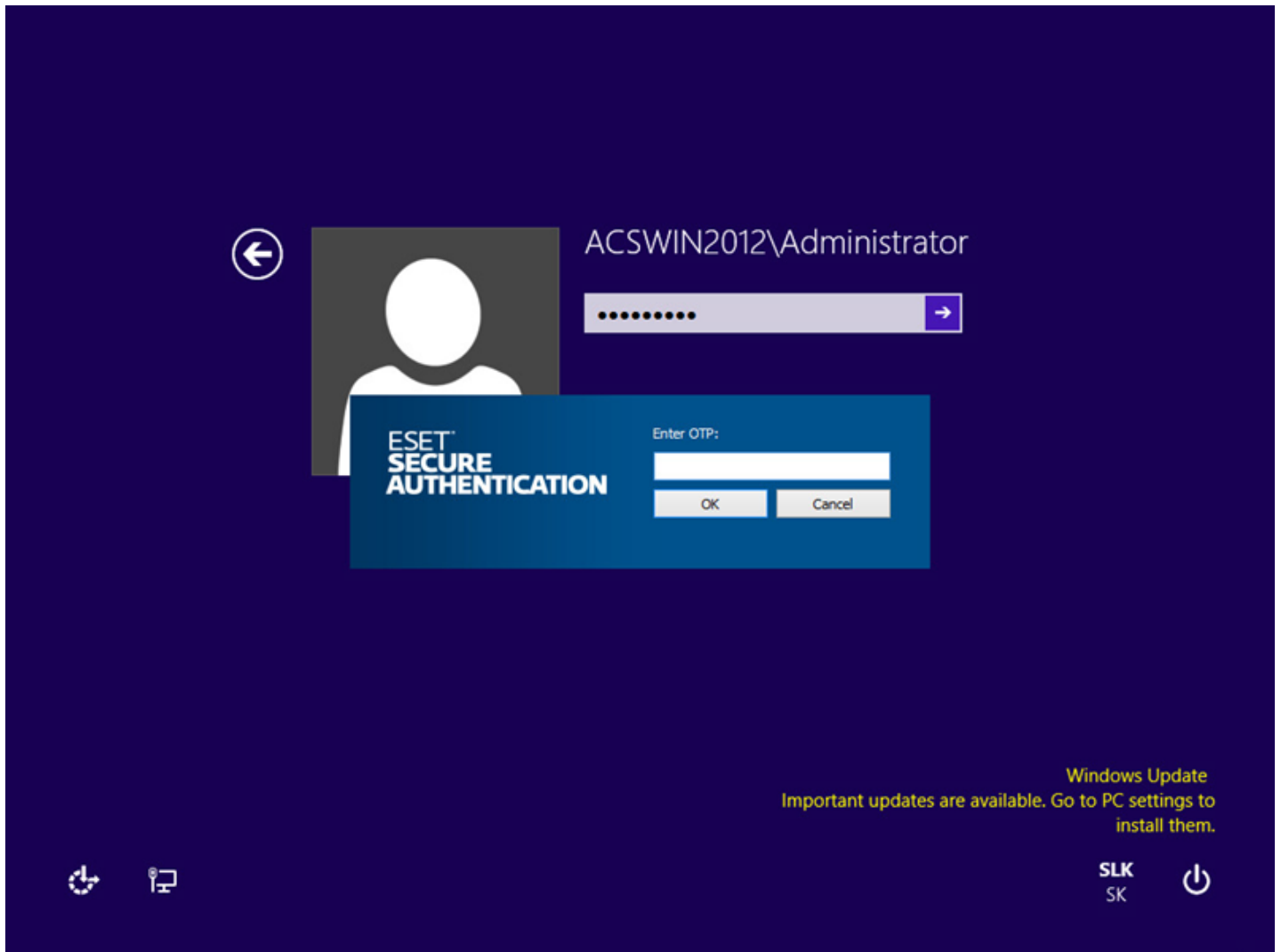
2FA protection cannot be bypassed by any attacker even if the attacker knew the AD username and password, thus providing better

protection of sensitive data. Of course, we assume the hard drive is not accessible by the attacker or the content of the drive is encrypted.

NOTE: If 2FA protection is enabled for offline mode, all users whose accounts are secured by 2FA and who want to use a 2FA-protected PC must log in to that PC for the very first time while the PC is online. By 'online' we mean that the main computer where [Core Components](#) of ESA are installed and the ESET Secure Authentication Service service is running and can be pinged from the 2FA-secured computer.

If the Windows Login component is installed on the same computer where ESA Core Components are installed and 2FA protection for Safe Mode is enabled on that computer while offline mode is disabled (*Do not allow access when offline* is selected), then the user will be allowed to log in to Safe Mode (without networking) without OTP.

Windows 8 login secured by ESA - after entering a valid AD username and password, users will be prompted for their OTP :

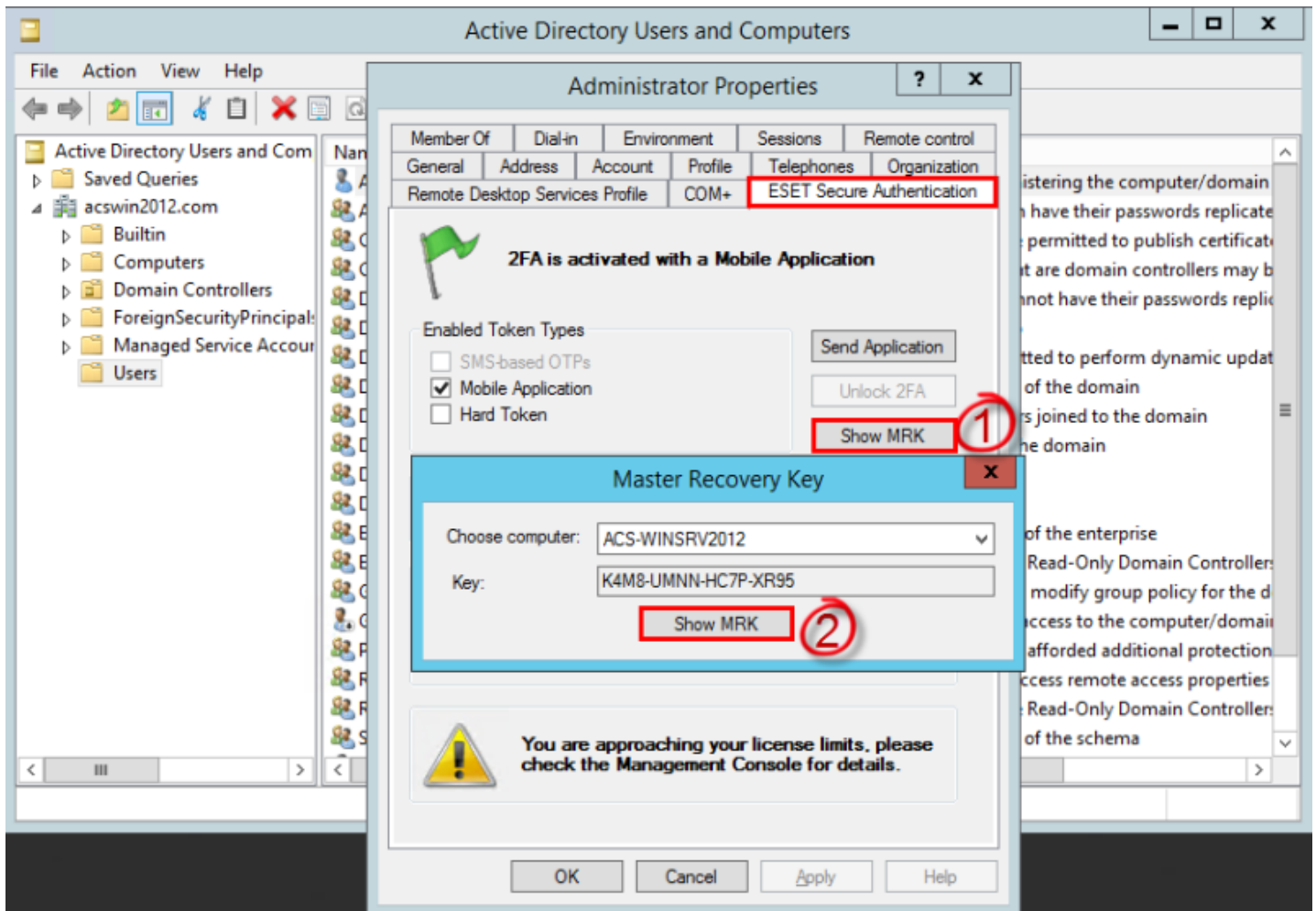


6.1 Master recovery key

A master recovery key (MRK) is an alternative OTP that can be used to log in to a Windows machine protected by 2FA in situations where the user can not enter a valid OTP. For example, the user lost his phone where the [ESA Mobile Application](#) was installed. An MRK is unique to a user and computer, meaning, User1 and User2 would have a different MRK for PC1. Access via MRK is available even in [online and offline mode](#). Offline use of MRK is available only if the offline mode for given computer is enabled in ESA Management Console in the section of [Windows Login Settings](#). If offline mode is enabled, MRK is also stored locally on the computer in the encrypted and protected cache.

To use MRK for authentication:

1. The user cannot obtain an OTP, so he calls the administrator.
2. The administrator opens the ADUC, navigates to the corresponding *Active Directory domain name* (in our example *acswin2012.com*) > *Users* > double-clicks the particular user > *ESET Secure Authentication* tab > clicks the *Show MRK* button > selects the particular computer from the *Choose computer* list-box and clicks *Show MRK*. At this point a MRK is generated.



3. The administrator provides the obtained MRK to the user and the user can log in entering the MRK instead of OTP.

While the computer is in [offline mode](#), an MRK may be used multiple times.

After first successful connection to [ESA core](#) the previously generated MRK is invalidated and can not be used anymore, even if it was not used at all.

7. VPN Protection

ESA ships with a standalone RADIUS server that is used to authenticate VPN connections. After installing the ESA RADIUS server component, the service will start automatically. Ensure that it is running by checking its status in the Windows Services console.

7.1 Configuration

To configure 2FA for your VPN, you must first add your VPN appliance as a RADIUS client. To do so, follow the steps shown below:

1. From the ESA Management Console, right-click the RADIUS server and select **Add Client**.
2. Select the new client and select **Properties** from the list of available actions.
3. Give the RADIUS client a memorable name for easy reference.
4. Configure the IP Address and **Shared Secret** for the Client so that they correspond to the configuration of your VPN appliance. The IP address is the internal IP address of your appliance. The shared secret is the RADIUS shared secret for the external authenticator that you will configure on your appliance.
5. Select "Mobile Application" as an authentication method. The optimal authentication method depends on your VPN appliance make and model. See the appropriate ESA VPN Integration Guide for details. [VPN integration guides](#) are available on the ESET Knowledgebase.
6. Optionally, you can allow any non-2FA users to use the VPN.

NOTE: Allowing non-2FA users to log in to the VPN without restricting access to a security group will allow all users in the domain to login via the VPN. Using such a configuration is not recommended.

7. Optionally restrict VPN access to an existing Active Directory security group.
8. Once you are finished making changes, click **OK**.
9. Re-start the RADIUS server.
 - a. Locate the ESA RADIUS Service in the Windows Services (under **Control Panel - Administrative Tools - View Local Services**).
 - b. Right-click the ESA Radius Service and select **Restart** from the context menu.

The following **VPN Type** options are available:

- **VPN does not validate AD user name and password**
- **VPN validates AD user name and password**
- **Use Access-Challenge feature of RADIUS**

The following RADIUS clients support the RADIUS Access-Challenge feature:

- Junos Pulse (VPN)
- Linux PAM module

The following RADIUS clients should not be used with the Access-Challenge feature:

- Microsoft RRAS -This appliance handles Access-Challenge as Access-Accept and does not prompt for an OTP, meaning, AD username and password are sufficient to log in.

7.2 Usage

Once you have configured your RADIUS client, it is recommended that you verify RADIUS connectivity using a testing utility such as NTRadPing before reconfiguring your VPN appliance. After verifying RADIUS connectivity, you may configure your appliance to use the ESA RADIUS server as an external authenticator for your VPN users.

Since both the optimal authentication method and usage are dependent on your appliance make and model, see the relevant ESET Secure Authentication VPN integration guide, available on the ESET Knowledgebase.

7.3 RADIUS PAM modules on Linux/Mac

Linux/Mac machines can use ESA for 2FA by implementing a Pluggable Authentication Module (PAM), which will serve as a RADIUS client communicating with the ESA RADIUS server.

PAM is a set of C dynamic libraries (.so) used for adding custom layers to the authentication process. They may perform additional checks and subsequently allow/deny access. In this case, we use a PAM module to ask the user for an OTP on a Linux or Mac computer joined to an Active Directory domain and verify it against an ESA RADIUS server.

The PAM Authentication and Accounting module by [FreeRADIUS](#) is used in this guide. Other RADIUS PAM clients can be used as well.

Basic configuration described here will use the Access-Challenge feature of RADIUS that is supported by both ESA RADIUS server and the used RADIUS PAM client. There are other options that do not use the Access-Challenge method briefly described in [Other RADIUS configurations](#) section of this manual.

First, [configure](#) the Linux/Mac RADIUS client in ESA Management Console. Type the IP address of your Linux/Mac computer in the **IP Address** field. Select **Use Access-Challenge feature of RADIUS** from the **VPN Type** drop-down menu.

Once you complete these steps, configuration your [Linux](#) or [Mac](#) computer based on the instructions in the following sub-chapters.

7.3.1 Mac OS - configuration

The steps below were performed on OS X - Yosemite 10.10.5.

Note: If you enable 2FA protection using the instructions in this guide, then by default local users who do not belong to your AD domain will not be able to log in. To allow local users to log in even if 2FA protection is enabled, please follow the additional steps described in the topic of [Other RADIUS configurations](#) - see [Non-2FA users \(user accounts not using 2FA\)](#).

To deploy 2FA protection on your Mac computer, make sure your computer is joined to the Active Directory domain. You can configure it under *System Preferences... > Users & Groups > Login Options*. Click *Join...* next to *Network Account Server* by entering your Active Directory credentials.

PAM Authentication Module

1. Download PAM RADIUS tar.gz from http://freeradius.org/pam_radius_auth/
2. Build the .so library by executing the following commands in a terminal window:

```
./configure  
make
```

3. Copy the built library to the PAM modules

```
cp pam_radius_auth.so /usr/lib/pam
```

On OS X El Capitan and later, this location is protected by System Integrity Protection. To use it, you have to [disable it](#) for the copy command.

4. Create a server configuration file named *server* at */etc/raddb/*. In it, enter the details of the RADIUS server in the following form:
<radius server>:<port> <shared secret> <timeout in seconds>

For example:
1.1.1.1 test 30

See [INSTALL](#) for security recommendations for the configuration file and [USAGE](#) for parameters that can be passed to the library. For example you can use the 'debug' parameter to identify potential problems.

Incorporating the PAM module

PAM modules may be incorporated into various login types, for example, login, sshd, su, sudo and so on. The list of login types available is located at `/etc/pam.d/`.

Modify the appropriate file in `/etc/pam.d/` to incorporate the RADIUS PAM module to specific login types.

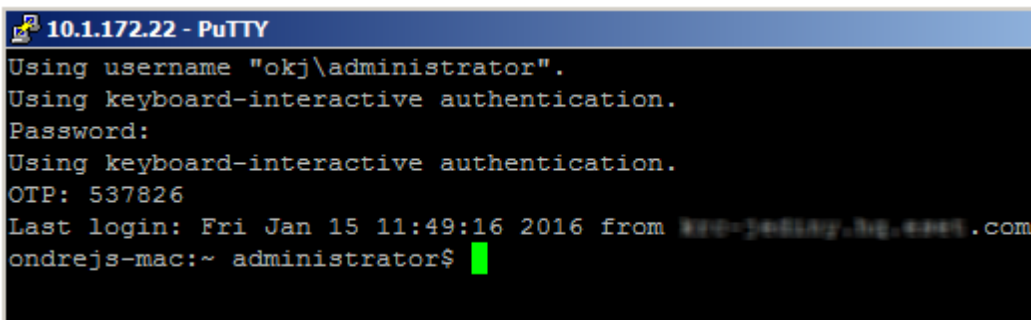
Incorporating the PAM module into SSH

To incorporate the PAM module into SSH, edit `/etc/pam.d/sshd` and add the following line at the end of the file:

```
auth required /usr/lib/pam/pam_radius_auth.so
```

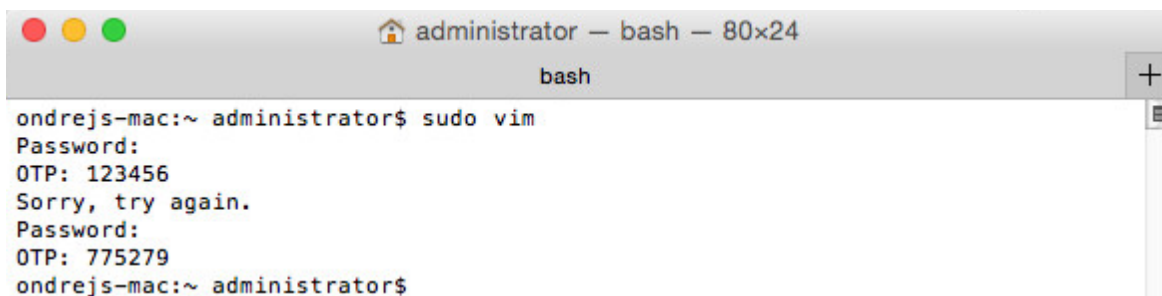
Next, enable SSH in OS X. Under *System Preferences... > Sharing*, enable **Remote Login**.

Below is an example of SSH login via ESA (PAM module incorporated in `/etc/pam.d/sshd`):



```
10.1.172.22 - PuTTY
Using username "okj\\administrator".
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
OTP: 537826
Last login: Fri Jan 15 11:49:16 2016 from 192-30-100-100.ng-eeet.com
ondrejs-mac:~ administrator$
```

Below is an example of sudo login via ESA (PAM module incorporated in `/etc/pam.d/sudo`):



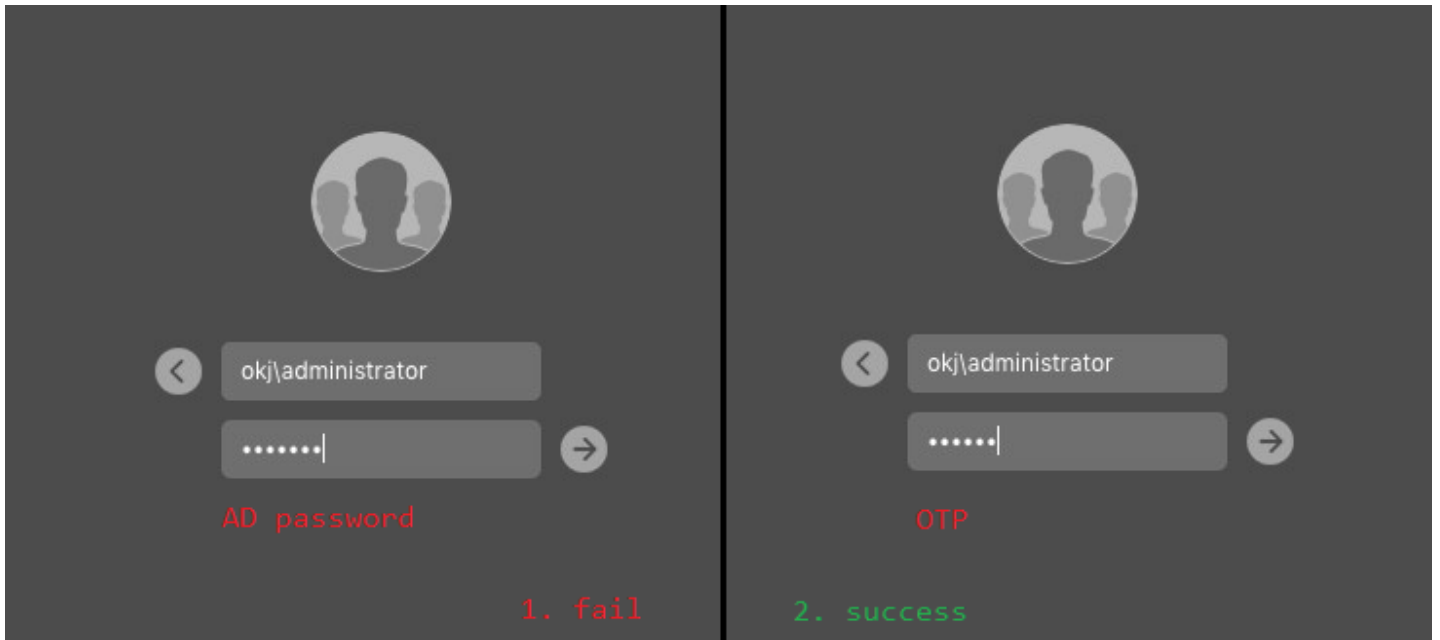
```
administrator - bash - 80x24
bash
ondrejs-mac:~ administrator$ sudo vim
Password:
OTP: 123456
Sorry, try again.
Password:
OTP: 775279
ondrejs-mac:~ administrator$
```

Incorporating the PAM module into Desktop Logins

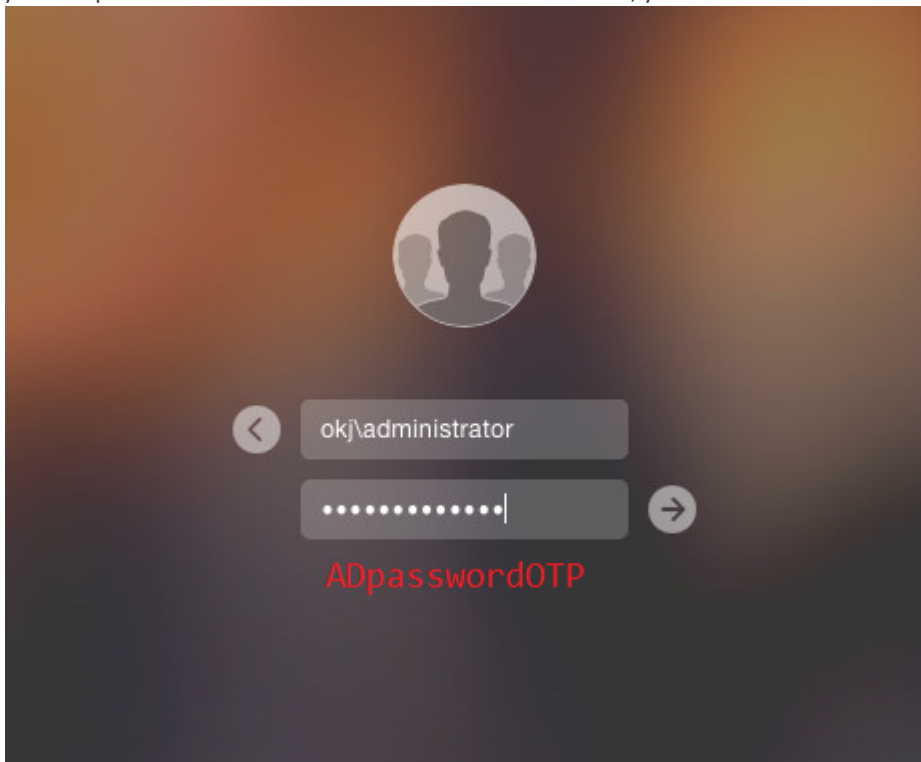
For Desktop login, we cannot use RADIUS Accept-Challenge like the VPN Type when configuring the RADIUS client in the ESA Management Tool. The RADIUS client configuration should be as shown in the **VPN Type - VPN does not validate AD username and password** section of the [Other RADIUS configurations](#) topic and the PAM module would be incorporated in the `/etc/pam.d/authorization` file.

Using these settings:

- OTP is delivered via SMS - at the first password prompt a user must enter their AD password. At the second password prompt, they must enter their OTP.



- Other type of OTP (compound authentication) - enter both the AD password and OTP at once as ADpasswordOTP. For example if your AD password is Test and the received OTP is 123456, you would enter Test123456.



7.3.2 Linux - configuration

The steps described here were accomplished on OpenSUSE Leap 42.1.

Note: If you enable 2FA protection using the instructions in this guide, then by default local users who do not belong to your AD domain will not be able to log in. To allow local users to log in even if 2FA protection is enabled, please follow the additional steps described in the topic of [Other RADIUS configurations](#) - see [Non-2FA users \(user accounts not using 2FA\)](#).

Make sure your Linux computer is joined to the Active Directory domain. Navigate to *YaST > Hardware > Network Settings > Hostname/DNS* and enter the IP address of the Domain Controller (DC) machine and the Active Directory domain name. Next, navigate to *YaST > Network Services > Windows Domain Membership*. Enter the AD domain name you want your Linux computer to join in the *Domain or Workgroup* field and click *OK*. You will be prompted to enter the domain administrator's username and password.

NOTE: The process of joining a domain will differ across Linux distributions.

PAM Authentication Module

1. Download PAM RADIUS tar.gz from http://freeradius.org/pam_radius_auth/
2. Build the .so library by executing the following commands in a terminal window:

```
./configure  
make
```

Depending on the output of the `configure` command, dependencies might have to be installed.

```
sudo zypper install gcc make pam-devel
```

3. Copy the built library to the PAM modules

```
sudo cp pam_radius_auth.so /lib/security/
```

4. Create a server configuration file at `/etc/raddb/` named `server`. In that file, enter the details of the RADIUS server in the following form:

```
<radius server>:<port> <shared secret> <timeout in seconds>
```

For example:
1.1.1.1 test 30

See [INSTALL](#) for security recommendations for the configuration file and [USAGE](#) for parameters that can be passed to the library. For example you can use the 'debug' parameter to identify potential problems.

Incorporating the PAM module

PAM modules may vary across Linux distributions. The incorporation scenarios also depend on the Desktop environment used on the particular Linux machine. In this example, Xfce was used on an OpenSUSE machine, therefore the PAM module was incorporated into `/etc/pam.d/xdm` (see examples below). It is possible that some modules may not prompt for a second factor as shown in the example below.

Incorporation of the PAM module into SSH in Linux is done similarly to the the way it is done in Mac OS - see [Incorporating the PAM module into SSH](#) in the Mac OS - configuration topic. However, the line of code to be added to the `/etc/pam.d/sshd` file is different:

```
auth required /lib/security/pam_radius_auth.so
```

Incorporating the PAM module into console login

In order to incorporate the PAM module into console login, edit `/etc/pam.d/login` and add the following line at the end of the file::

```
auth required /lib/security/pam_radius_auth.so
```

Below is an example of console login while secured via ESA :

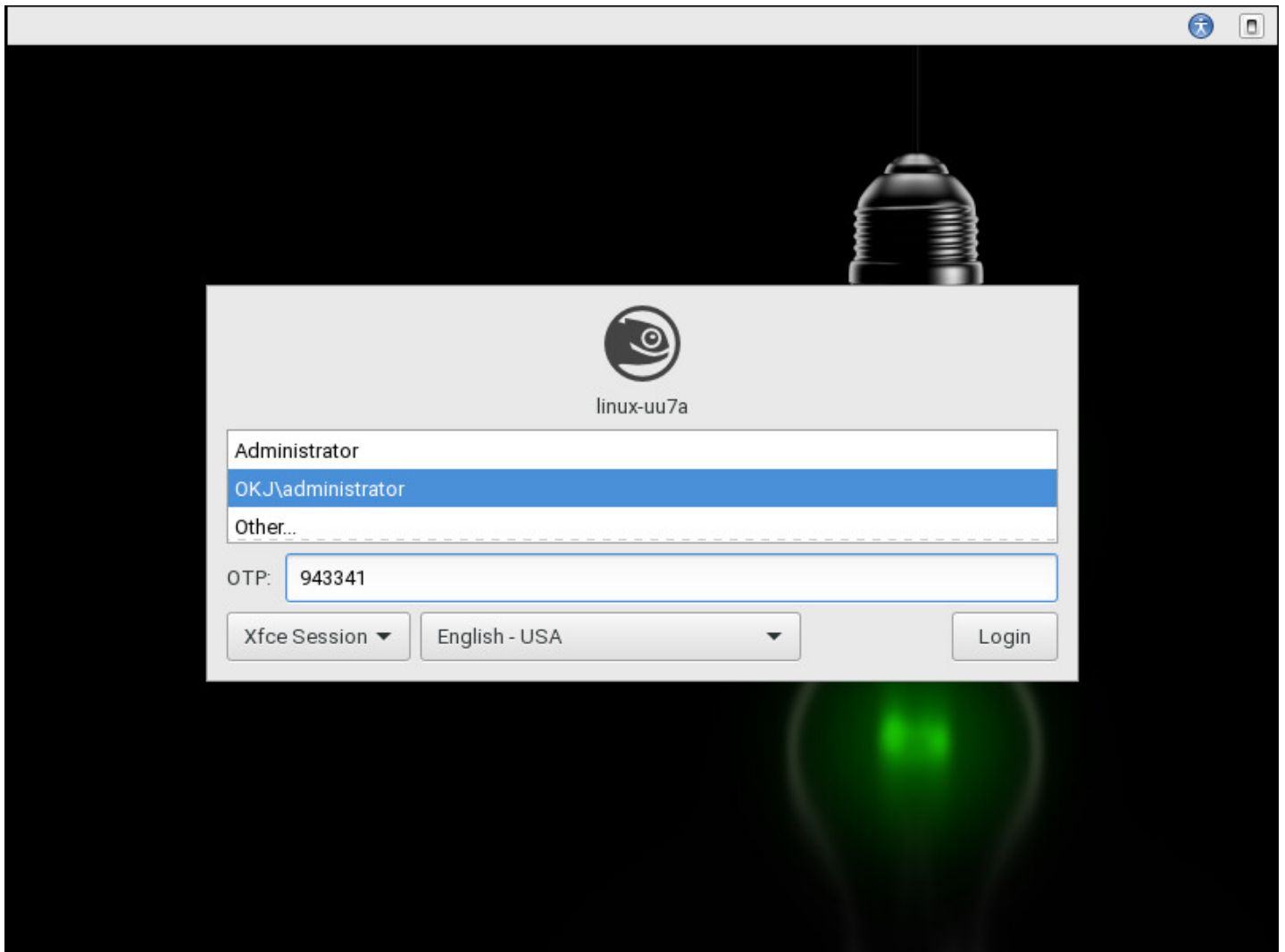
```
[ 2.552437] sd 0:0:0:0: [sda] Assuming drive cache: write through  
[ 8.922390] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!  
  
Welcome to openSUSE Leap 42.1 - Kernel 4.1.13-5-default (tty1).  
  
linux-uu7a login: okj\administrator  
Password:  
OTP: 421219  
Last login: Mon Jan 18 09:34:43 from console  
Have a lot of fun...  
OKJ\administrator@linux-uu7a:~> _
```

Incorporating the PAM module into Xfce desktop login

To incorporate the PAM module into Xfce desktop login, we have to edit `/etc/pam.d/xdm` and add the following line at the end of the file:

```
auth required /lib/security/pam_radius_auth.so
```

Below is an example of Xfce desktop login while secured via ESA:



7.3.3 Other RADIUS configurations

VPN Type - VPN does not validate AD username and password

If you set VPN Type to VPN does not validate AD username and password when [configuring](#) a RADIUS client in ESA Management Tool, both factors (AD username and password as first factor, and OTP as second factor) are verified by ESA:

The screenshot shows the 'UnixPAM Properties' dialog box with the 'RADIUS Client Configuration' tab selected. The 'Identification' section contains the following fields: Name: UnixPAM, IP Address: 10.1.172.22, and Shared Secret: test. The 'VPN Type:' dropdown menu is set to 'VPN does not validate AD user name and password'. The 'Authentication Methods:' section has the following checked options: SMS-based OTPs, Mobile Application, Hard Token OTPs, and Compound Authentication (passwordOTP). The 'Access Control:' section has the 'Restrict access to:' checkbox unchecked.

Afterward, in `/etc/pam.d/sshd` (or other integration), add the following line:

```
auth required /usr/lib/pam/pam_radius_auth.so
```

and comment (place a # tag at the beginning) all the other `auth` lines.

NOTE: The domain administrator must verify whether this scenario- specifically disabling all other modules - is suitable for their deployment.

In this case a SSH login process would look like this:

- SMS delivery of OTP - at the first password attempt, the user is prompted for an AD password. At the second password attempt, they enter their OTP.

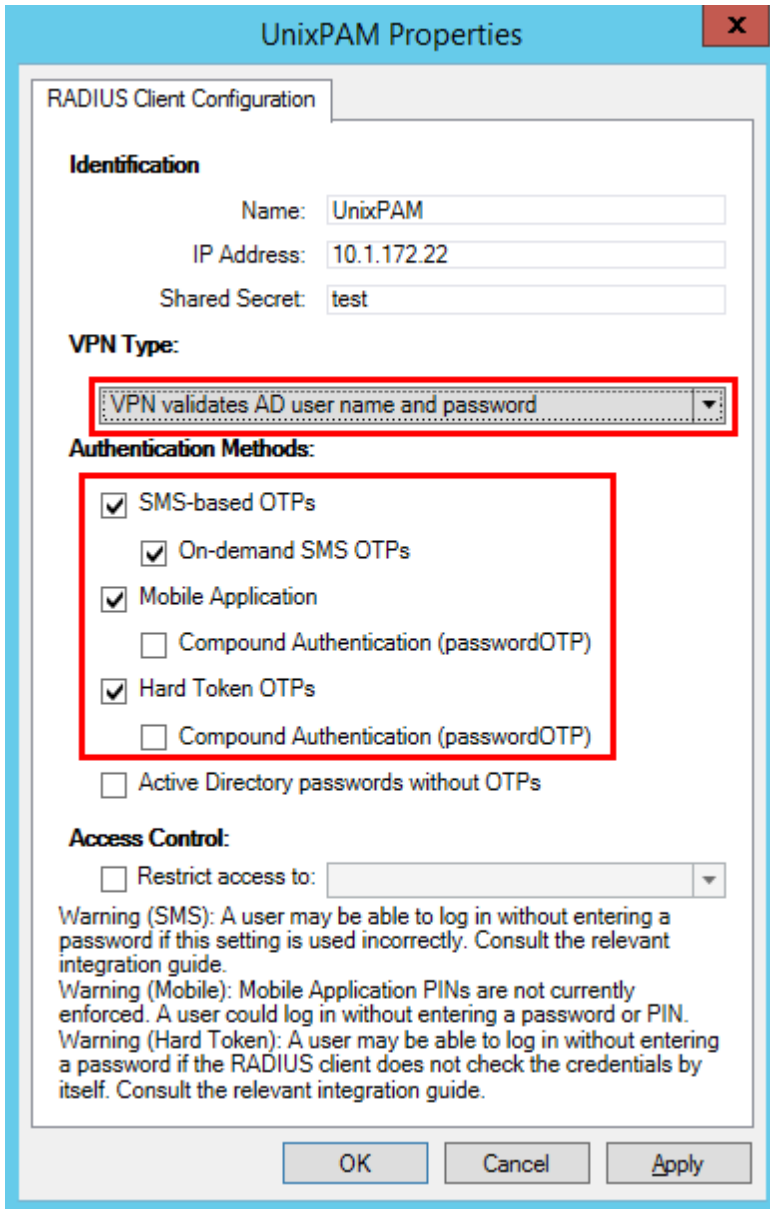

```
10.1.172.22 - PuTTY
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password: AD password
Access denied
Using keyboard-interactive authentication.
Password: OTP
Last login: Fri Jan 15 13:49:12 2016 from 192-168-1-100.100.100.com
ondrejs-mac:~ administrator$
```

- Other type of OTP (compound authentication) - the user must enter both the AD password and OTP at the same time as ADpasswordOTP. For example if your AD password is Test and the received OTP is 123456, you would enter Test123456.

```
10.1.172.22 - PuTTY
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password: ADpasswordOTP
Last login: Fri Jan 15 14:02:47 2016 from 192-168-1-100.100.100.com
ondrejs-mac:~ administrator$
```

VPN Type - VPN validates AD username and password

if you set **VPN Type** to **VPN validates AD username and password** when [configuring](#) a RADIUS client in ESA Management Tool, then the first factor (AD username and password) is validated by the other PAM module:



When configuring RADIUS in this manner, add the following line in `/etc/pam.d/ssh` (or the appropriate integration):

```
auth required /usr/lib/pam/pam_radius_auth.so force_prompt prompt=RADIUS
```

In this case a SSH login process would look like this:

- prompts that start with the string **Password:** are handled by other PAM modules. Prompts that begin with the string **RADIUS:** are handled by our PAM module. See the argument '**prompt=RADIUS**' in the sample code above
- SMS - at the first prompt, a user must enter their AD password. At the second prompt, they must enter the text 'sms' (without apostrophes). At the third prompt, they must enter their AD password. At the fourth prompt, they must enter the received OTP

```

10.1.172.22 - PuTTY
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password: AD password
Using keyboard-interactive authentication.
RADIUS: 'sms'
Access denied
Using keyboard-interactive authentication.
Password: AD password
Using keyboard-interactive authentication.
RADIUS: OTP
Last login: Fri Jan 15 14:36:00 2016 from 192-168-1-100.100.100.com
ondrejs-mac:~ administrator$ █

```

- Other type of OTP (OTP received via mobile application or a hard token) - enter the AD password at the first attempt. At the second attempt enter the OTP.

```

10.1.172.22 - PuTTY
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password: AD Password
Using keyboard-interactive authentication.
RADIUS: OTP
Last login: Mon Jan 18 13:12:13 2016 from 192-168-1-100.100.100.com
ondrejs-mac:~ administrator$ █

```

Non-2FA users (user accounts not using 2FA)

When configuring the PAM module for ESA, remember to consider the experience for non-2FA users - for example local Linux/Mac users as opposed to domain users.

Linux:

Using this configuration, a RADIUS server would fail authentication for local users unless the following code (or appropriate for your system) is added in `/etc/pam.d/ssh` (or the appropriate file for your PAM module):

```
auth sufficient pam_unix.so try_first_pass
```

This edit makes standard Unix authentication sufficient to log in, so any local user will be allowed after entering a local password. To allow domain users whose accounts are not secured with 2FA, enable **Active Directory Passwords without OTPs** when configuring the RADIUS client in ESA Management Console.

Mac:

There is no default PAM module to authenticate local users as on Linux (see above). To achieve this, another PAM module must be used. In this guide, we chose to download [a collection of modules for PAM](#) and then build the module by running the following commands in a terminal window:

```
./configure --disable-pgsql --disable-mysql --disable-ldaphome
make
make install
```

The next steps depend on whether 2FA integration is intended for use with desktop logins or non-desktop logins (for example ssh).

Mac non-desktop login integration:

- in the integration-specific `/etc/pam.d/` file, add the following line before `pam_radius_auth.so`:

```
auth sufficient /usr/local/lib/security/pam_regex.so sense=allow regex=user$
```

where **user** is a local **username** that we want to be allowed without the requirement of an OTP.

- make sure the default Mac modules (not added by us) are defined as "required" or "requisite", so that this added "sufficient" module does not cause a success if the first factor failed
- modules other than pam_regex from the [collection of Modules for PAM](#) may be used also. For example you could use pam_groupmember to allow groups of users instead of single users to log in.

Mac desktop login integration:

- change the /etc/pam.d/authorization file so it looks like this:

```
# authorization: auth account
auth    sufficient /usr/lib/pam/pam_radius_auth.so
auth    requisite /usr/local/lib/security/pam_regex.so sense=allow regex=^user$
auth    optional   pam_krb5.so use_first_pass use_kcminit
auth    optional   pam_ntlm.so use_first_pass
auth    required   pam_opendirectory.so use_first_pass nullok
account required   pam_opendirectory.so
```

Those changes ensure that:

1. our RADIUS PAM module is listed first as 'sufficient'
2. our regex PAM module is the second as 'requisite'
3. other modules that were in the file before follow later

8. Web Application Protection

The ESA Web Application Protection module automatically adds 2FA into the authentication process of all supported Web Applications. The module will be loaded the next time the protected Web Application is accessed after ESA has been installed.

Users will log in using the normal authentication process of the Web Application. After being authenticated by the Web Application, the user will be redirected to an ESA web page and prompted for an OTP. The user will only be allowed access to the Web Application if a valid OTP is entered.

The user's 2FA session will remain active until they log out of the Web Application or close their browser.

8.1 Configuration

The Web Application integration can be configured from the Basic Settings page of your domain in the ESET Secure Authentication management console.

The settings for the Exchange Server plugins, Outlook Web App and Exchange Control Panel, are global to the domain. The settings for all other Web Application plugins are per server.

The 2FA protection can be enabled or disabled for each Web Application. The 2FA protection is enabled by default after installation. The World Wide Web Publishing service will need to be restarted on all servers hosting the Web Application for changes to this configuration option to be reloaded.

8.1.1 Allowing Non-2FA Users

The module can be configured to either allow or to prohibit users that do not have 2FA enabled from accessing the Web Application through the "Users without 2FA enabled may still log in" configuration option.

This scenario occurs if the user is configured for neither SMS-based OTPs nor the Mobile Application and the Web Application configuration option to allow non-2FA users to log in is enabled. The configuration option to allow non-2FA users defaults to being enabled after installation.

In this configuration, a user can log into the Web Application with their Active Directory password.

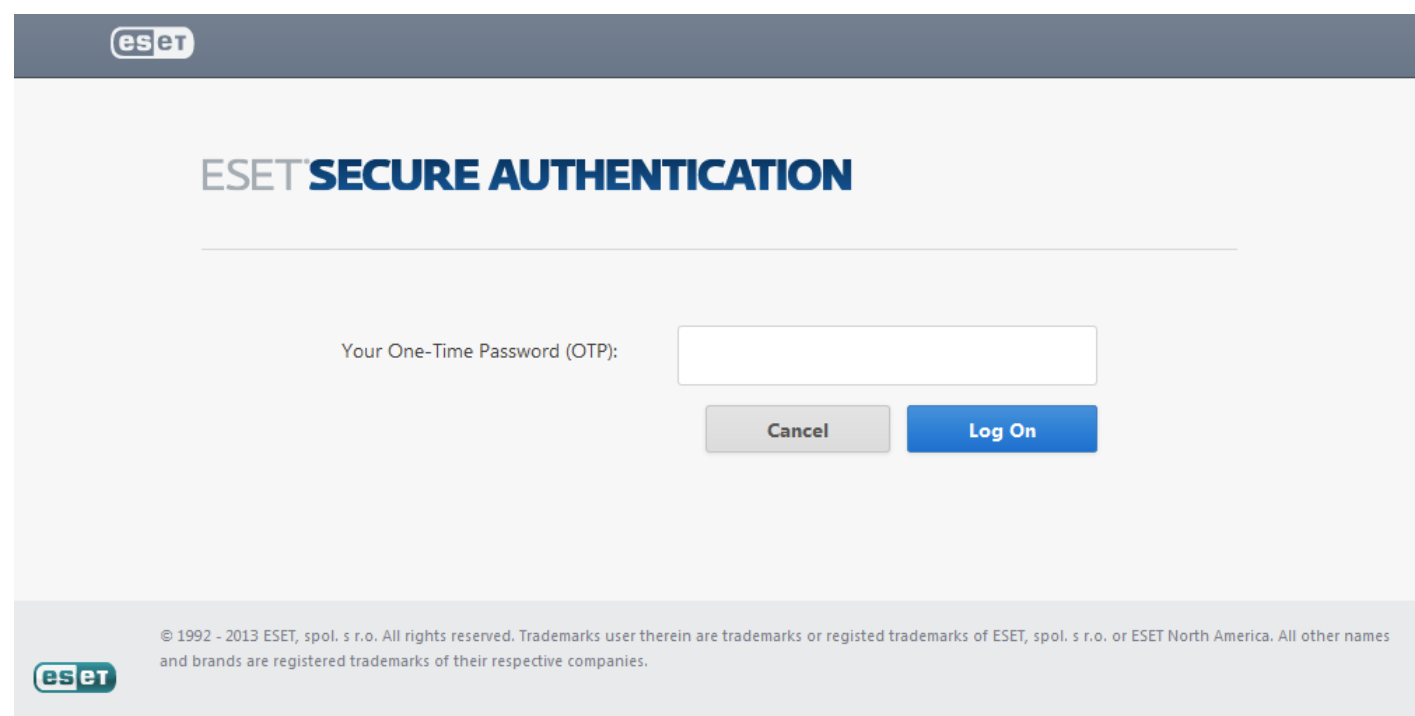
If the configuration option to allow non-2FA users is disabled, then the user will not be able to log into the Web Application.

8.2 Usage

The same 2FA process is followed for all supported Web Apps.

The operation of the Web Application Protection module can be verified as follows:

1. A user that has ESA 2FA enabled in the ADUC management tool is required for testing. The user must also be allowed to access the Web App.
2. Open the Web App in a desktop browser and authenticate as normal using the Active Directory credentials of the test user.
3. The ESA authentication page should now appear, as per the figure below. The Remote Desktop Web Access plugin on Windows Server 2008 and the Microsoft Dynamics CRM 2011 plugin will not display the "Cancel" button.
4. The ESA authentication page should now appear, as per the figure below. The Remote Desktop Web Access plugin on Windows Server 2008 and the Microsoft Dynamics CRM 2011 plugins will not display the "Cancel" button.



- a. If the user is enabled for SMS OTPs, an SMS will be sent containing an OTP that may be entered to authenticate.
 - b. If the user has installed the ESA mobile application on their phone, it may be used to generate an OTP to authenticate. OTPs are displayed in the mobile application with a space between the 3rd and 4th digits in order to improve readability. The Web Application Protection module strips whitespace, so a user may include or exclude whitespace when entering an OTP without affecting authentication.
5. If a valid OTP is entered, then the user will be redirected to the page they originally requested. The user will then be able to interact with the Web App.
 6. If an invalid OTP is entered, then an error message will be displayed and the user will not be allowed access to the web application, as per the figure below.

ESET[™] SECURE AUTHENTICATION

The OTP you entered could not be authenticated. Please try again.

Your One-Time Password (OTP):

© 1992 - 2013 ESET, spol. s r.o. All rights reserved. Trademarks user therein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.



7.

9. Remote Desktop Protection

The ESA Remote Desktop Protection module adds 2FA into the authentication process of Remote Desktop users. The module will be loaded the next time a 2FA-enabled user attempts to use Remote Desktop to log in to a remote computer on which the ESA Credential Provider has been installed.

Users will log in using the normal authentication process of Remote Desktop. After being authenticated by Remote Desktop, the user will be prompted for an OTP. The user will only be allowed access to his or her computer if a valid OTP is entered.

The user's 2FA session will remain active until they log out or disconnect from the Remote Desktop session.

NOTE: ESA cannot protect [RDP](#) clients that do not provide username and password, meaning, if there is an RDP client that does not have the username and password configured and it does not even request a username and password, then no OTP is going to be requested either.

9.1 Configuration

To configure Remote Desktop 2FA for ADUC users, you must enable 2FA for the desired user(s). They must also be allowed Remote Desktop users.

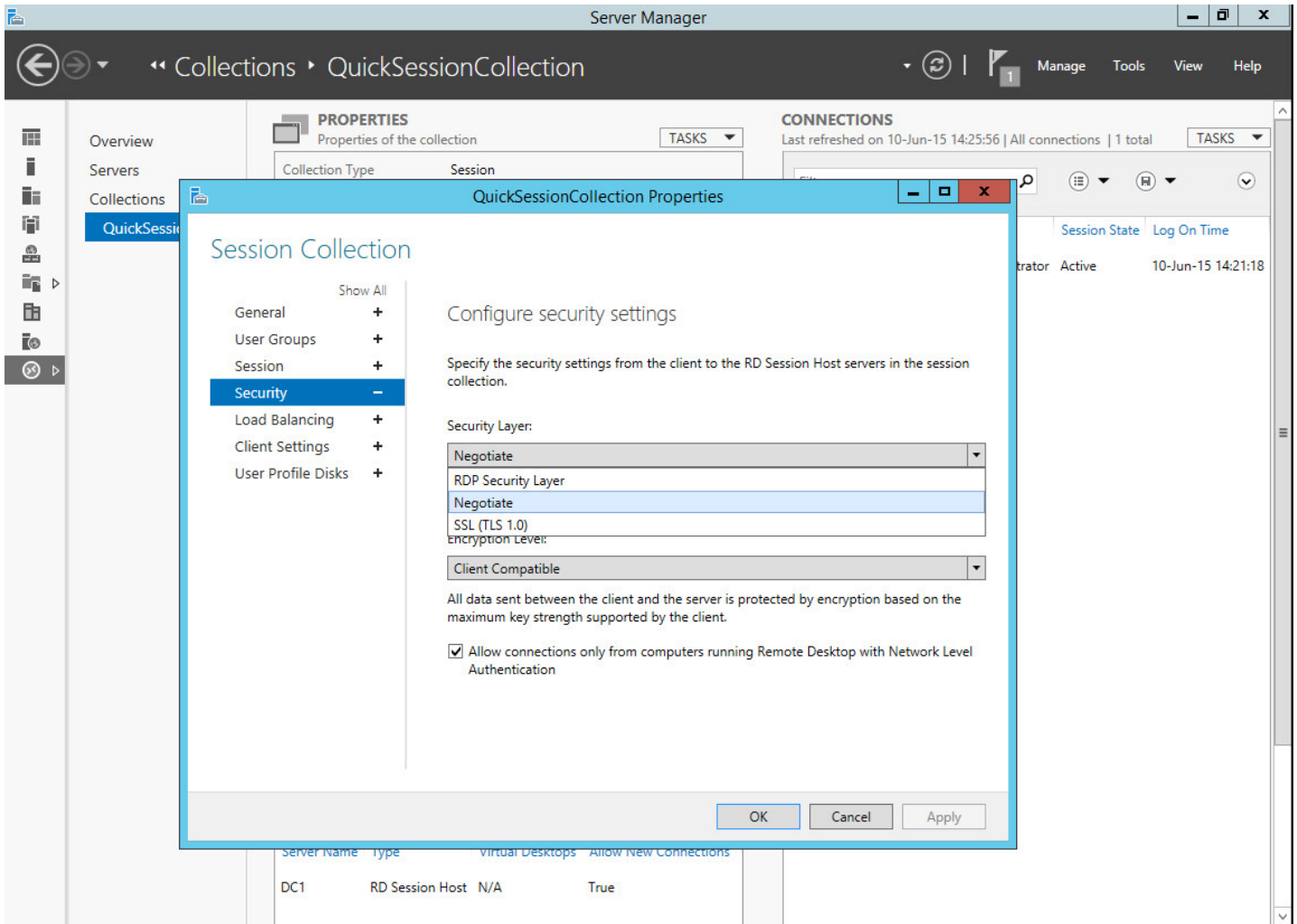
In order to use Remote Desktop protection, RD Session Host must be configured to use *SSL (TLS 1.0)* or *Negotiate*.

To modify the settings on Windows Server 2008 or earlier, follow these steps:

1. Go to the **Start** menu > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**
2. In the **Connections** section, open **RDP-Tcp**
3. Click the **General** tab
4. In the **Security** section, the **Security Layer** setting must be set to *SSL (TLS 1.0)* or *Negotiate*

To modify the settings on Windows Server 2012, follow these steps:

1. Open **Server Manager**
2. Click **Remote Desktop Services** from the left pane
3. Open the **Collections** properties
4. In the **Security** section, the **Security Layer** setting must be set to *SSL (TLS 1.0)* or *Negotiate*



9.1.1 Allowing Non-2FA Users

The module can be configured to either allow or to prohibit users that do not have 2FA enabled from logging in to remote computers with Remote Desktop Protocol through the "Users without 2FA enabled may still log in" configuration option.

This scenario occurs if the user is configured for neither SMS-based OTPs nor the Mobile Application and the Remote Desktop configuration option to allow non-2FA users to log in is enabled. The configuration option to allow non-2FA users defaults to being enabled after installation.

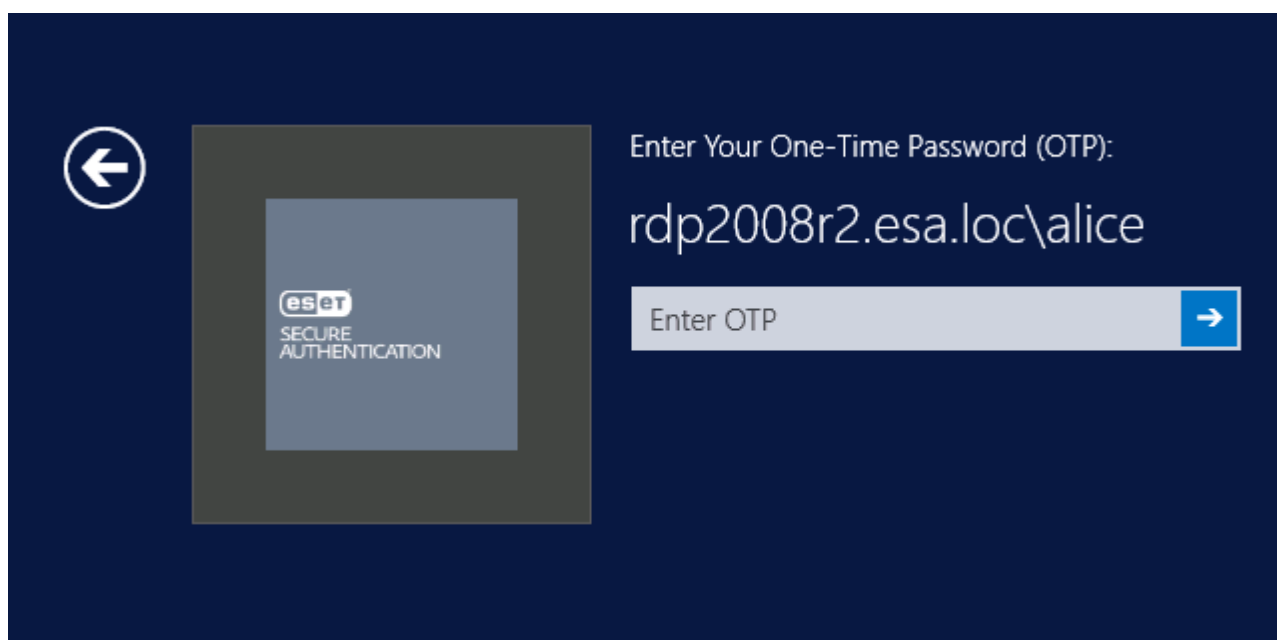
In this configuration, a user can log into the remote computer with their Active Directory password.

If the configuration option to allow non-2FA users is disabled, then the user will not be able to log into remote computers with Remote Desktop Protocol.

9.2 Usage

The operation of the Remote Desktop Protection module can be verified as follows:

1. A domain user that has ESA 2FA enabled in the ADUC management tool is required for testing. This user must be added as an allowed Remote Desktop user on the remote computer.
2. A computer that has Remote Desktop Access enabled is also required.
3. Connect to the remote computer using a Remote Desktop client, and authenticate as normal using the Active Directory credentials of the test user.
4. The OTP prompt screen should now appear, as per the figure below.



- a. If the user is enabled for SMS OTPs, an SMS will be sent containing an OTP that may be entered to authenticate.
 - b. If the user has installed the ESA mobile application on their phone, it may be used to generate an OTP to authenticate. OTPs are displayed in the mobile application with a space between the 3rd and 4th digits in order to improve readability. The Remote Desktop Protection module strips whitespace, so a user may include or exclude whitespace when entering an OTP without affecting authentication.
5. If a valid OTP is entered, then the user will be granted access to the computer they attempted to connect to.
 6. If an invalid OTP is entered, then an error message will be displayed and the user will not be allowed access to the remote computer.

9.3 Remote Desktop Web Access

If you utilize 2FA protection of RDP on your server where [Remote Desktop Web Access](#) (RDWA) is hosted, default settings require 2FA authentication for the launch of applications available in your RDWA.

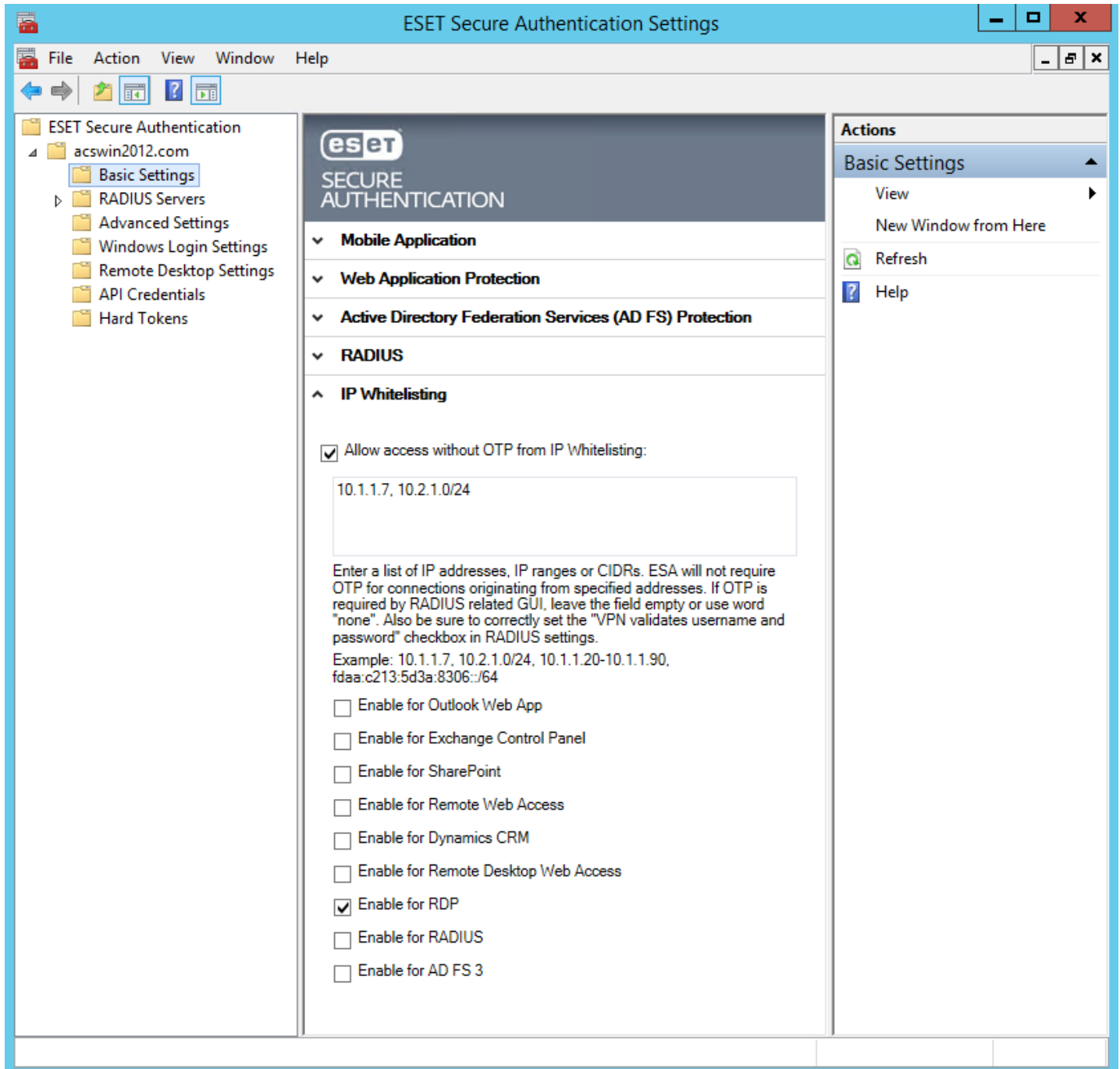
This means, if a user tries to access your RDWA web site, the user is prompted for an OTP. Once the user provides a valid OTP, logs in and tries to launch an application available in your web site, the user will be prompted again to provide an OTP.

If you do not want an authenticated user (used a valid OTP to enter your RDWA web site) to be prompted for an OTP when launching an application in your web site, take the following steps:

1. In the ESA Management Console navigate to **ESET Secure Authentication** > <domain> > **Basic Settings** > **Trusted Networks**
2. Click the [IP Whitelisting](#) row
3. Enter the localhost IP address: 127.0.1.0,::1 in the text box
4. Select the check-box next to **RDP**
5. Click **Save**.

10. IP address whitelisting

If there are certain users for whom you want to grant access to Remote Desktop or [Supported Web Applications](#) secured by 2FA without the need to enter an OTP, you can whitelist their IP addresses. To do so, open the ESA Management Console in the **ESET Secure Authentication Settings** application and navigate to **ESET Secure Authentication > <domain> > Basic Settings > Trusted Networks**.



The screenshot displays the ESET Secure Authentication Settings application window. The title bar reads "ESET Secure Authentication Settings". The menu bar includes "File", "Action", "View", "Window", and "Help". The left sidebar shows a tree view with "ESET Secure Authentication" expanded to "acswin2012.com", where "Basic Settings" is selected. The main content area features the ESET logo and "SECURE AUTHENTICATION" header. Below this, several sections are visible: "Mobile Application", "Web Application Protection", "Active Directory Federation Services (AD FS) Protection", "RADIUS", and "IP Whitelisting". The "IP Whitelisting" section is expanded, showing a checked checkbox for "Allow access without OTP from IP Whitelisting:". Below this is a text input field containing "10.1.1.7, 10.2.1.0/24". A descriptive paragraph explains that users can enter IP addresses, ranges, or CIDRs, and provides an example: "10.1.1.7, 10.2.1.0/24, 10.1.1.20-10.1.1.90, fd00:c213:5d3a:8306::/64". A list of services follows, with "Enable for RDP" checked and others unchecked. The right sidebar, titled "Actions", shows "Basic Settings" selected, with options for "View", "New Window from Here", "Refresh", and "Help".

Select the check box next to **Allow access without OTP from trusted networks**, define the desired IP addresses, select the services to whitelist and click **Save**.

NOTE:

When analyzing RDP connections to find out if the user (IP address) is whitelisted or not, we review IP addresses that connect through the RDP port. This may present an issue if multiple RDP connections are in place at one time, because we cannot identify the IP address of users who are already connected as opposed to trying to connect. To eliminate the OTP prompt, all connecting IP addresses must be whitelisted. Therefore, if a non-whitelisted user is already connected and a whitelisted user is establishing a

connection, the whitelisted user will be asked to enter an OTP.

If your VPN is secured by 2FA utilizing and you want the users whose IP addresses you whitelisted to be able to access your VPN without an OTP, the following criteria must be met:

- in the [configuration of RADIUS client](#) select the check boxes next to **VPN validates username and password** and **Active Directory passwords without OTPs**
- make sure the user the whitelisted IP address belongs to does not have any 2FA options enabled - see [user management](#)

If these criteria are met, the user can access the VPN without entering a password or using the word **none** as password

Do not confuse [Remote Web Access](#) with [Remote Desktop Web Access](#).

11. Hard Tokens

A hard token is a device that generates an OTP and can be used in conjunction with a password as an electronic key to access something. Hard tokens come in many different device types, it could be a key fob which can be clipped onto a keyring or in a credit card form which can be stored in a wallet.

ESA supports all OATH compliant HOTP hard tokens but ESET does not supply them. The hard token HOTPs can be used in the same way as the OTPs generated by the mobile app or sent to the user via SMS. Scenarios where this may be useful is to support legacy token migration, for compliance or if it fits with the company policy. Note that OATH TOTP (time-based OTPs) are not supported.

11.1 Hard Token Management

This section describes how to enable hard tokens and manage them using the ESA Management Console.

This mainly consists of three functions:

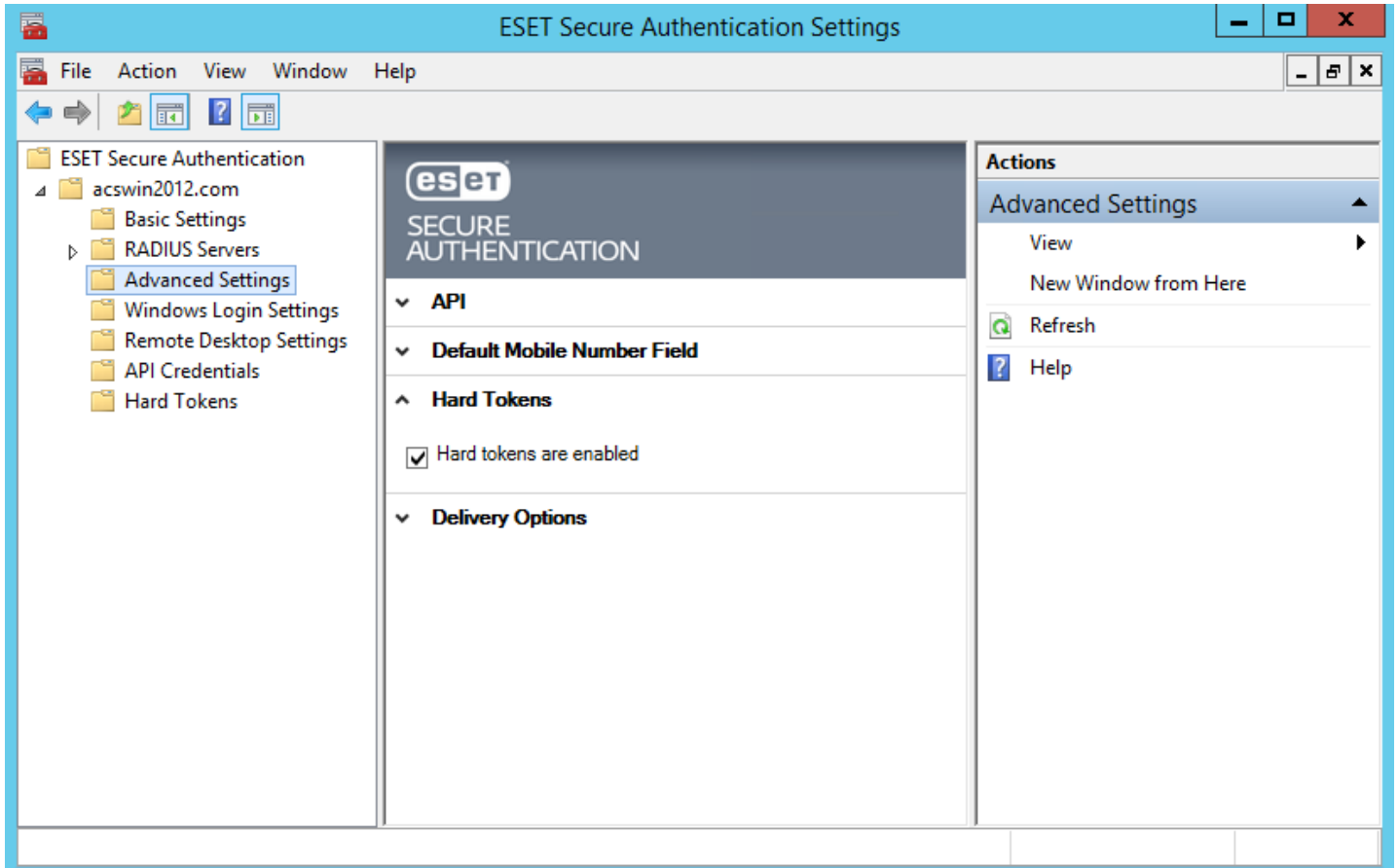
1. Importing the hard tokens into the system
2. Deleting hard tokens
3. Resynchronizing hard tokens

11.1.1 Enable

Hard tokens are disabled by default and must be enabled before use. Once enabled, hard tokens will need to be imported before the full functionality is available.

Hard tokens can be enabled as follows:

1. Launch the ESET Secure Authentication Management Console and navigate to the "Advanced Settings" node for your domain.
2. Expand the "Hard Tokens" section and check the "Hard tokens are enabled" check box. Save the changes.
3. If successful a "Hard Tokens" node will appear. Hard token management can be done here.

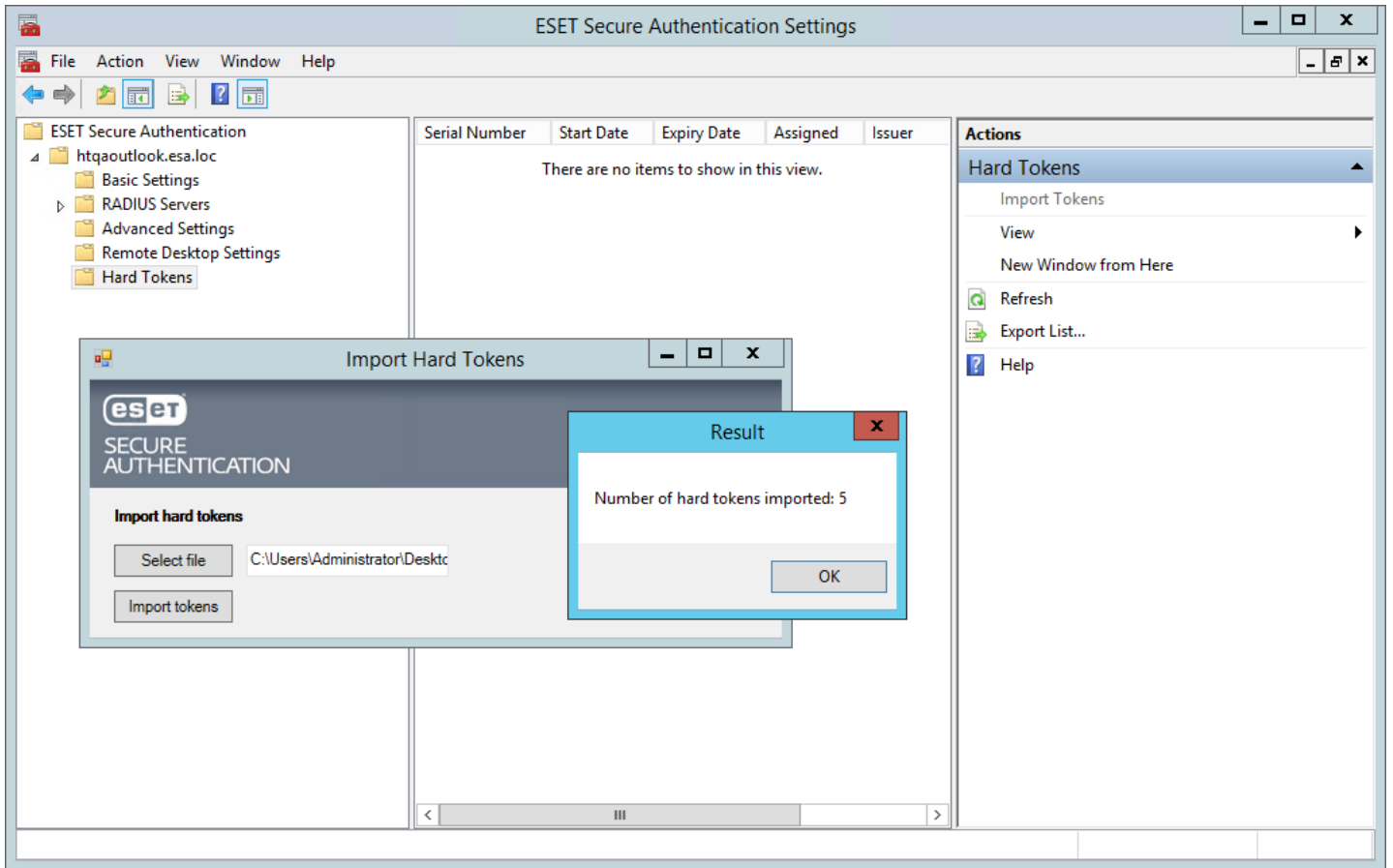


11.1.2 Import

To fully utilize hard token functionality, hard tokens need to be imported. Once done these hard tokens will be available to assign to users.

Tokens can be imported as follows:

1. Launch the ESET Secure Authentication Management Console and navigate to the "Hard Tokens" node for your domain.
2. Click the "Import Tokens" action.
3. Select the file to import. This should be an XML file in the PSKC format. NOTE: If such a file was not received from the hard token vendor, please contact ESA support.
4. Click the Import tokens button.
5. A result window will pop up indicating how many hard tokens were imported.
6. On clicking OK the windows will close and the imported hard tokens will be displayed.

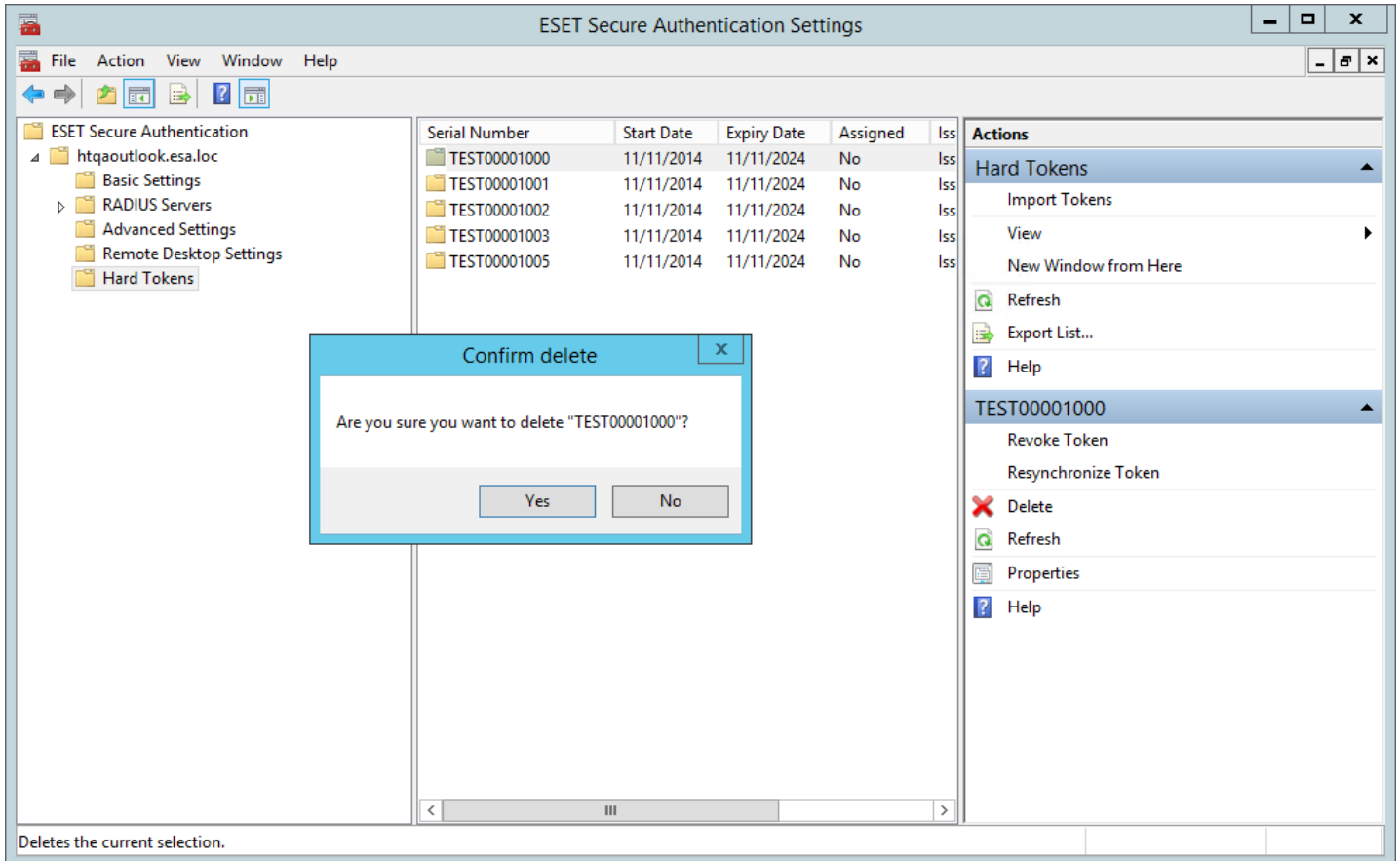


11.1.3 Delete

It may be necessary to delete a token from the system.

Tokens can be deleted as follows:

1. Launch the ESET Secure Authentication Management Console and navigate to the "Hard Tokens" node for your domain.
2. Select the hard token to delete.
3. Click the Delete action for that hard token.
4. Click the "Yes" button on the confirmation box.

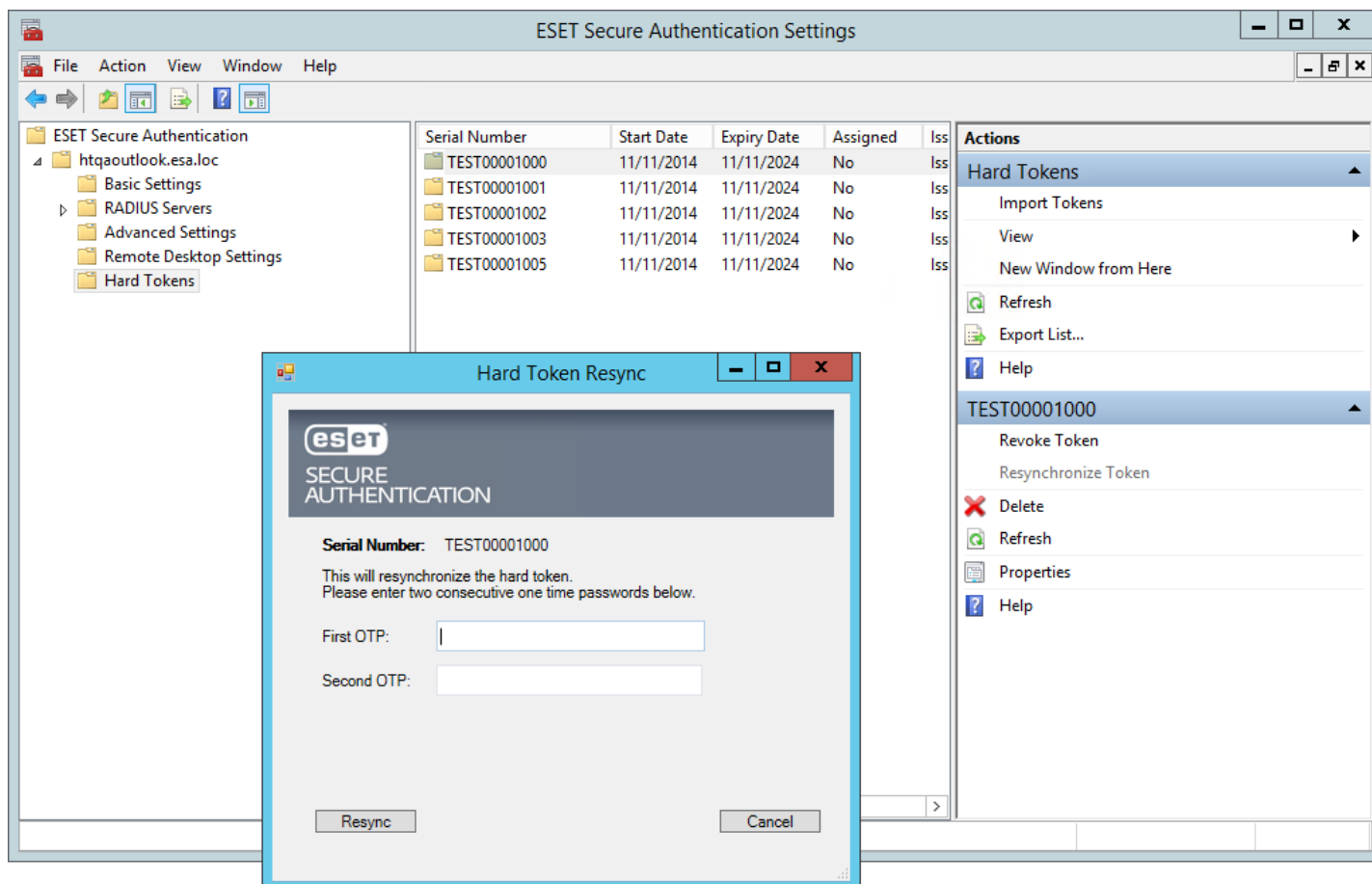


11.1.4 Resynchronize

There is a possibility that a hard token becomes out of sync with the system. This can happen if a user generates many new OTPs in a short space of time. In this scenario a resynchronization will be required.

A token can be resynchronized as follows:

1. Launch the ESET Secure Authentication Management Console and navigate to the "Hard Tokens" node for your domain.
2. Select the hard token to resynchronize.
3. Click the "Resynchronize Token" action for that hard token.
4. This opens the Hard Token Resync window.
5. Generate and enter two consecutive OTPs using the selected hard token.
6. Click the Resync button.
7. A successful message should display.



11.2 Hard Token User Management

This section deals with the user management of hard tokens. For this functionality to work hard tokens need to be enabled on the system and hard tokens need to have been imported.

User management takes place through the ESET Secure Authentication tab in the ADUC tool.

There are two functions available:

1. Enable hard token authentication for a user and assign a hard token.
2. Revoke a hard token linked to a user.

11.2.1 Enable and Assign

When hard tokens are enabled for a user a hard token needs to be assigned before proceeding.

Enable and assign as follows:

1. Open the user's profile from the ADUC.
2. Navigate to the ESET Secure Authentication tab.
3. Enable the Hard Token token type.
4. In the Hard Token Management group select a token to assign.
5. Click the Apply button. The hard token is now assigned to the user.

User Properties

? X

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile			COM+	
General	Address	Account	Profile	Telephones
Attribute Editor		ESET Secure Authentication		



Two-factor authentication (2FA) is not activated

Enabled Token Types

- SMS-based OTPs
- Mobile Application
- Hard Token

Send Application

Unlock 2FA

Hard Token Management

Assigned Token: Not assigned ▼

Revoke

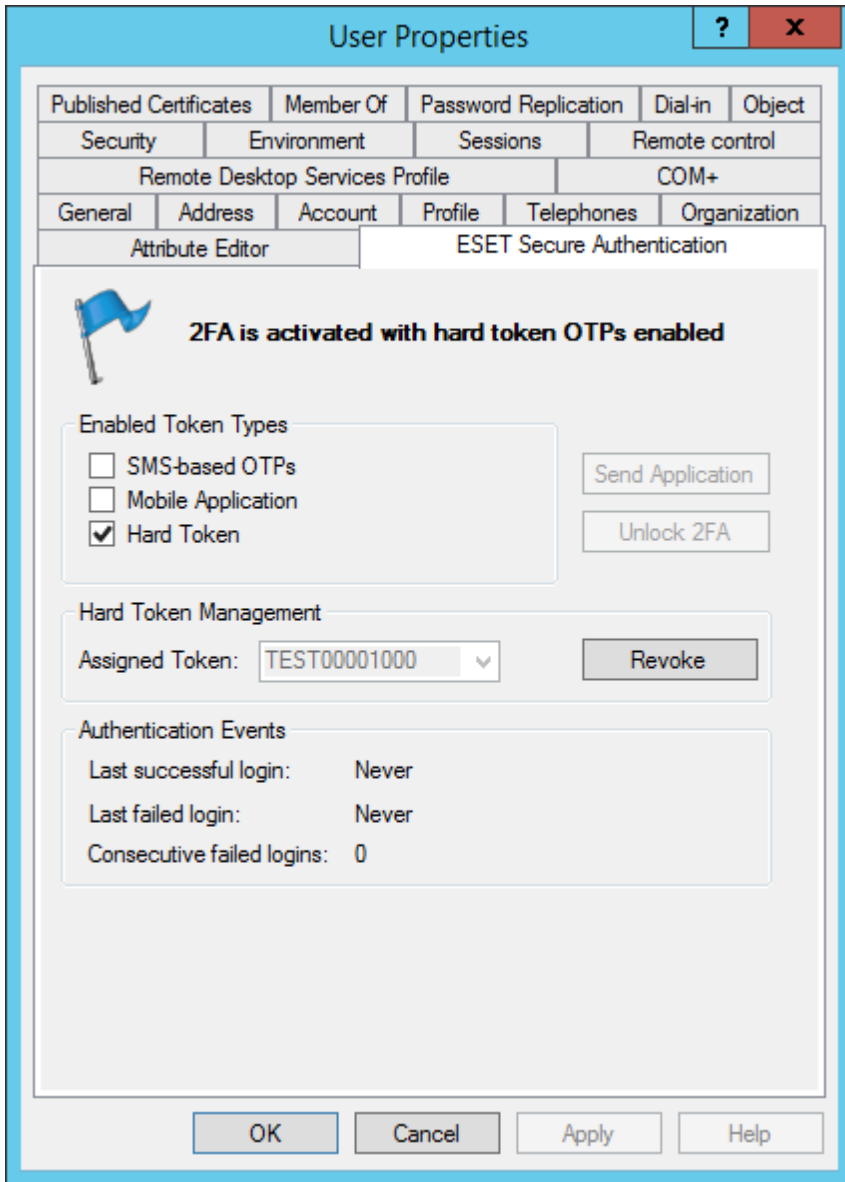
Authentication Eve
TEST00001000
Last successful lo
TEST00001001
Last failed login:
TEST00001002
TEST00001003
Consecutive failed logins: 0

OK

Cancel

Apply

Help



11.2.2 Revoke

Revoking a hard token for a user will also disable that user for hard token authentication.

A hard token can be revoked as follows:

1. Open the user's profile from the ADUC tool.
2. Navigate to the ESET Secure Authentication tab.
3. Click the Revoke button.

12. API

The ESA API is a REST-based web service that can be used to easily add 2FA to existing applications.

In most web-based applications users are authenticated before being granted access to protected resources. By asking for an additional authentication factor during the logon process, such applications can be made more resilient to attack.

The full API documentation for developers is available in the [API User Guide](#).

12.1 Integration Overview

The API consists of two endpoints, which are both called by POSTing JSON-formatted text to the relevant API URLs. All responses are also encoded as JSON-formatted text, containing the method result and any applicable error messages. The first endpoint (the Authentication API) is for user authentication and the second endpoint (the User Management API) is for user management.

The API is available on all servers where the Authentication Core component is installed and runs over the secure HTTPS protocol on port 8001.

The Authentication API is available on URLs of the form <https://127.0.0.1:8001/auth/v1/> and the User Management API is available on URLs of the form <https://127.0.0.1:8001/manage/users/v1/>. Both endpoints are protected from unauthorized access via standard HTTP Basic Authentication, requiring a valid set of API Credentials before processing any request.

The ESET Secure Authentication installer automatically uses an appropriate SSL security certificate installed on the machine, or generates a new self-signed certificate if another cannot be found.

12.2 Configuration

The API is disabled by default and must be enabled before use. Once enabled, API credentials must be created to authorize requests:

1. Launch the ESET Secure Authentication Management Console and navigate to the “Advanced Settings” node for your domain.
2. Expand the “API” section and check the “API is enabled” check box. Save the changes.
3. Open the standard Windows Services Console and restart the ESET Secure Authentication Core service for the change to take effect.
4. Navigate to the newly visible “API Credentials” node for your domain.
5. Click the “Add Credentials” action to create a new set of credentials.
6. Double-click on the newly created credentials to get the username and password that are to be used for API authentication.
7. Check the “Enabled for Auth API” check box, the “Enabled for User Management API” check box or both.

Many sets of API credentials may be created. It is recommended to create different sets for each application being protected, as well as for testing.

If the API is enabled, all servers with the Authentication Core component installed will respond to authorized API requests after they are restarted. There is no need to restart the Authentication Core service when credentials are created or deleted.

12.3 Replacing the SSL Certificate

The API utilizes an SSL certificate to secure API communications from eavesdropping. The installer automatically selects an appropriate certificate installed on the machine, or generates a new self-signed certificate if another cannot be found.

This section explains how to replace the certificate with another of your choosing. It will first help you to import your new certificate into Windows, and then use it for ESA.

12.3.1 Prerequisites

In order to follow this guide you will need:

- All operating systems:
 - An installation of the ESET Secure Authentication Core component
 - Administrator access to the computer where ESET Secure Authentication is installed
 - The SSL certificate you wish to use in PKCS12 format (.pfx or .p12)
 - The certificate file needs to contain a copy of the private key as well as the public key
- Windows 2003 only:
 - The httpcfg.exe tool from the Windows Support Tools pack (either on the installation CD or downloadable from <http://www.microsoft.com/en-us/download/details.aspx?id=18546>)

NOTE: The ESA Authentication API does not have to be enabled in order to replace the certificate.

12.3.2 Importing the New Certificate

The new certificate needs to be placed in the Local Machine\Personal store before it can be used.

1. Launch the Microsoft Management Console (MMC):
 - Windows Server 2003: Start -> Run -> Type "mmc.exe" and press the "Enter" key
 - Windows Server 2008+: Start -> Type "mmc.exe" and press the "Enter" key
2. Add the Certificates snap-in:
 - Windows Server 2003:
 - Click "File" -> "Add/Remove Snap-in" -> "Add" button
 - Select "Certificates" from the list
 - Click the "Add" button
 - Select "Computer account"
 - Click "Next"
 - Select "Local computer"
 - Click "Finish"
 - Click "Close"
 - Click "OK"
 - Windows Server 2008+:
 - Click "File" -> "Add/Remove Snap-in"
 - Select "Certificates" from the left-hand column
 - Click the "Add >" button
 - Select "Computer account"
 - Click "Next"
 - Select "Local computer"
 - Click "Finish"
 - Click "OK"
3. Optionally save the snap-in for future use ("File" -> "Save")
4. Select the "Certificates (Local Computer)" -> "Personal" node in the tree
5. Right-click -> "All tasks" -> "Import"
6. Follow the Import Wizard, taking care to place the certificate in the "Personal" certificate store location
7. Double-click the certificate and make sure the line "You have a private key that corresponds to this certificate" is displayed

12.3.3 Replacing the ESA Certificate

NOTE: The ESA Core Authentication service will not start up without a certificate configured. If you remove the certificate, you must add another before the Core service will run correctly.

Determine the correct certificate to use:

1. Open the MMC Certificates Manager using the steps above
2. Find the certificate you wish to use in the "Personal" folder and double-click it
3. Make sure you see "You have a private key that corresponds to this certificate" on the "General" tab
4. On the "Details" tab, select the "Thumbprint" field
5. The certificate thumbprint is displayed in the bottom pane (sets of two hex digits separated by spaces)

Windows Server 2003:

1. Click "Start" -> "All Programs" -> "Windows Support Tools" -> "Command Prompt"
2. Type "httpcfg query ssl -i 0.0.0.0:8001" and press the "Enter" key
3. Copy and paste the "Hash" field somewhere safe, in case you want to re-add the existing certificate
4. Type "httpcfg delete ssl -i 0.0.0.0:8001" and press the "Enter" key
5. You should see "HttpDeleteServiceConfiguration completed with 0."
6. Type "httpcfg set ssl -i 0.0.0.0:8001 -g {BA5393F7-AEB1-4AC6-B759-1D824E61E442} -h <THUMBPRINT>", replacing <THUMBPRINT> with the values from the certificate thumbprint without any spaces and press the "Enter" key
7. You should see "HttpSetServiceConfiguration completed with 0"
8. Restart the ESET Secure Authentication Core service for the new certificate to take effect

Windows Server 2008+

Click "Start" -> Type "cmd.exe"

In the list of programs, right-click the "cmd.exe" item and select "Run as administrator"

Type "netsh http show sslcert ipport=0.0.0.0:8001" and press the "Enter" key

Copy and paste the "Certificate Hash" field somewhere safe, in case you want to re-add the existing certificate

Type "netsh http delete sslcert ipport=0.0.0.0:8001" and press the "Enter" key

You should see "SSL Certificate successfully deleted"

Type "netsh http add sslcert ipport=0.0.0.0:8001appid={BA5393F7-AEB1-4AC6-B759-1D824E61E442}certhash=<THUMBPRINT>", replacing <THUMBPRINT> with the values from the certificate thumbprint without any spaces and press the "Enter" key

You should see "SSL Certificate successfully added"

Restart the ESET Secure Authentication Core service for the new certificate to take effect

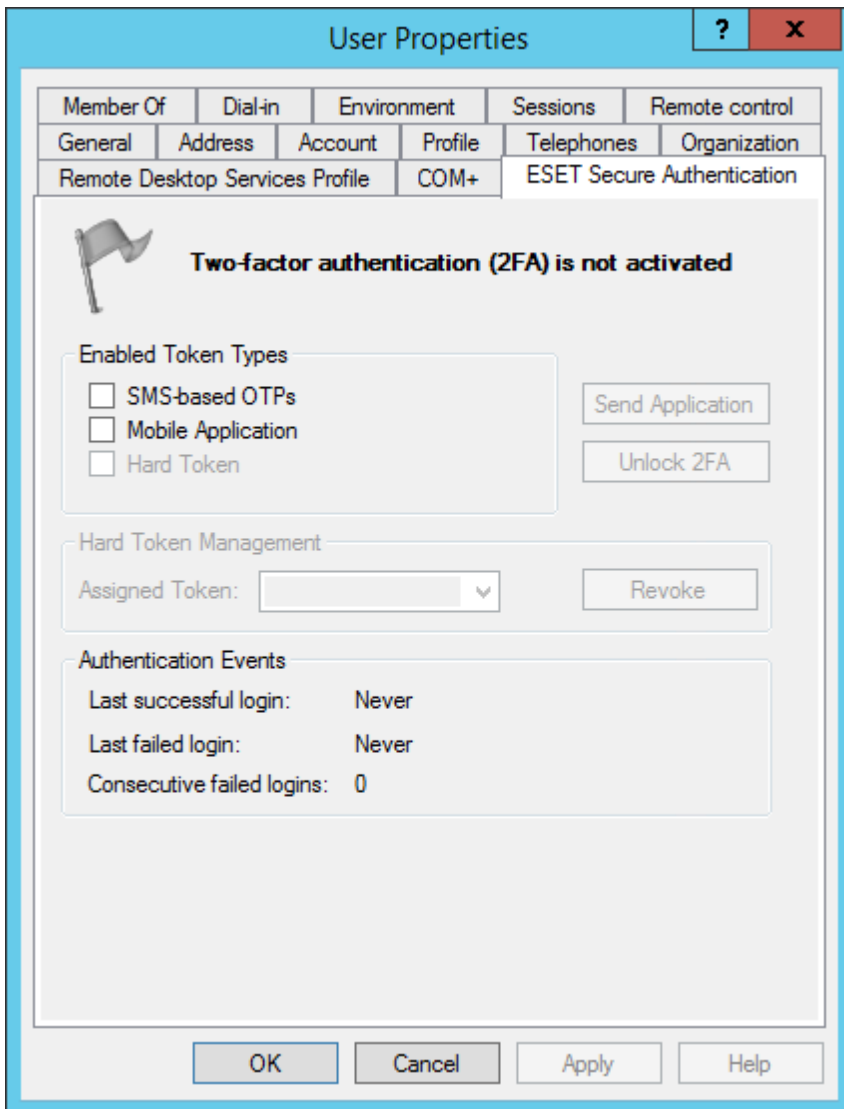
13. Advanced User Management

The ESET Secure Authentication tab for a user in the ADUC is divided into four sections:

- User State (indicated by a colored flag for quick reference)
- Enabled Token Types (check boxes)
- Administrator Actions (buttons)
- Auditing Data (text data indicating authentication events)

13.1 User States

A user may be in various states during regular operation. Before enabling a user for 2FA, they are in an uninitialized state:



The screenshot shows the 'User Properties' dialog box with the 'ESET Secure Authentication' tab selected. The main content area displays a message: 'Two-factor authentication (2FA) is not activated' with a flag icon. Below this, there are three sections: 'Enabled Token Types' with three unchecked checkboxes (SMS-based OTPs, Mobile Application, Hard Token) and two buttons ('Send Application', 'Unlock 2FA'); 'Hard Token Management' with a dropdown menu for 'Assigned Token' and a 'Revoke' button; and 'Authentication Events' with three rows of data: 'Last successful login: Never', 'Last failed login: Never', and 'Consecutive failed logins: 0'. At the bottom, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Member Of	Dial-in	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones	Organization
Remote Desktop Services Profile		COM+	ESET Secure Authentication		

Two-factor authentication (2FA) is not activated

Enabled Token Types

- SMS-based OTPs
- Mobile Application
- Hard Token

Buttons: Send Application, Unlock 2FA

Hard Token Management

Assigned Token: [Dropdown]

Button: Revoke

Authentication Events


Last successful login:	Never
Last failed login:	Never
Consecutive failed logins:	0

Buttons: OK, Cancel, Apply, Help

A user may then be enabled for either SMS-based OTPs, Mobile Application OTPs, or both. If they are enabled for both, they are in what is known as the transitioning state:

User Properties [?] [X]

Member Of	Dial-in	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones	Organization
Remote Desktop Services Profile	COM+	ESET Secure Authentication			

 **2FA is activated; user will transition to a Mobile Application once app is sent**

Enabled Token Types

- SMS-based OTPs
- Mobile Application
- Hard Token

Buttons: Send Application, Unlock 2FA

Hard Token Management

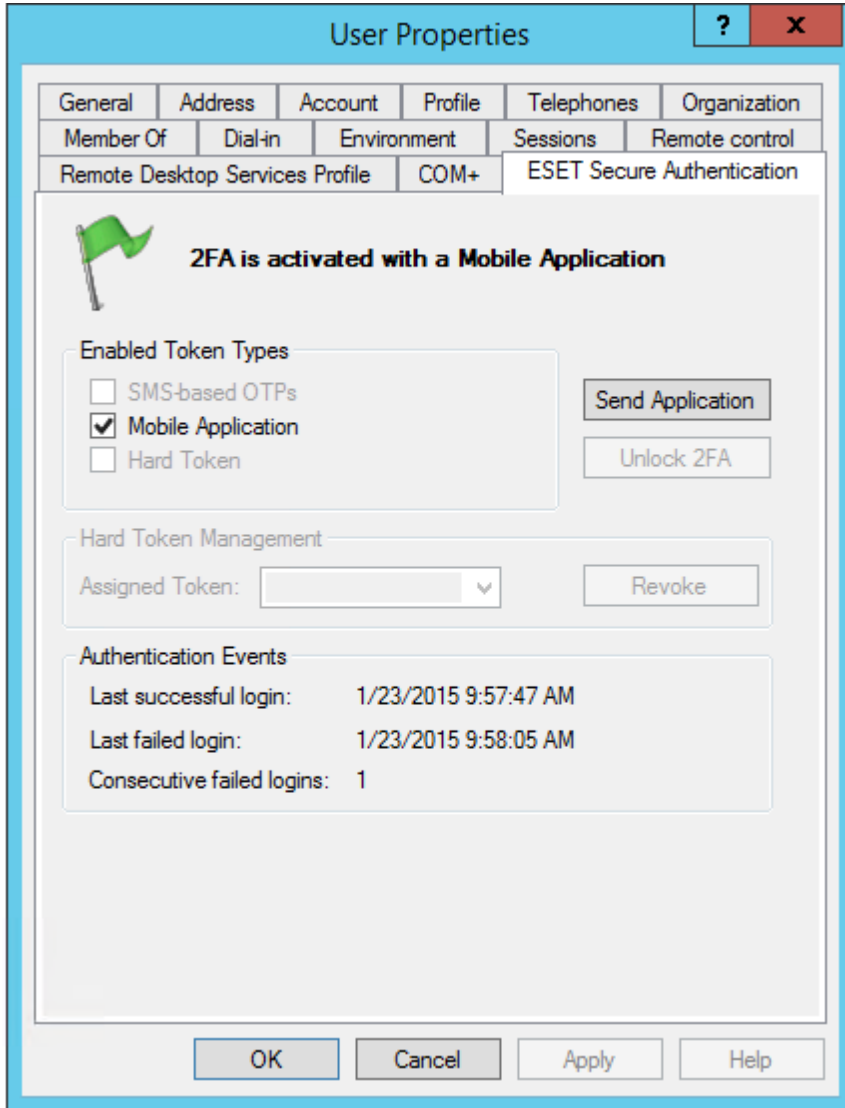
Assigned Token: [] [v] [Revoke]

Authentication Events

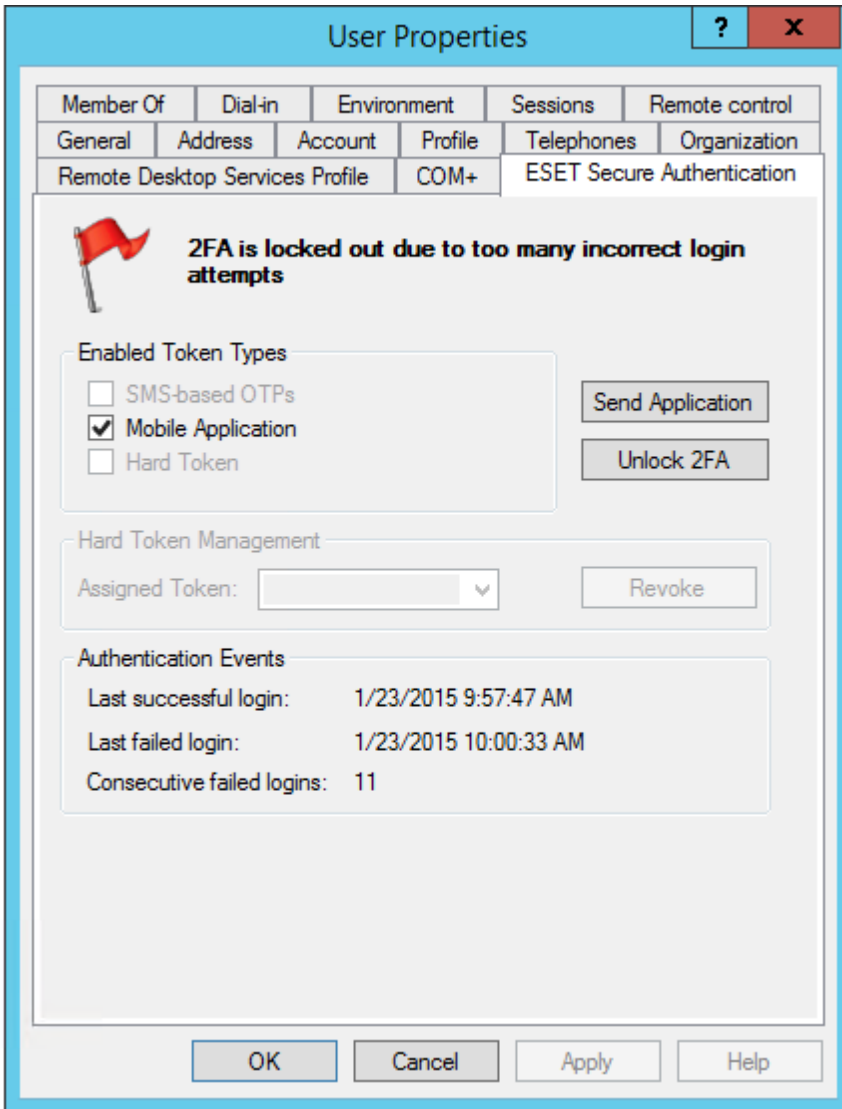
- Last successful login: Never
- Last failed login: Never
- Consecutive failed logins: 0

Buttons: OK, Cancel, Apply, Help

In this state, a user will receive SMS OTPs when authentication attempts are initiated, but as soon as a valid mobile OTP is used for authentication, SMS OTPs will be disabled, and the user will only be able to authenticate using mobile OTPs. When a user has successfully authenticated using a mobile app OTP, a green flag is displayed:



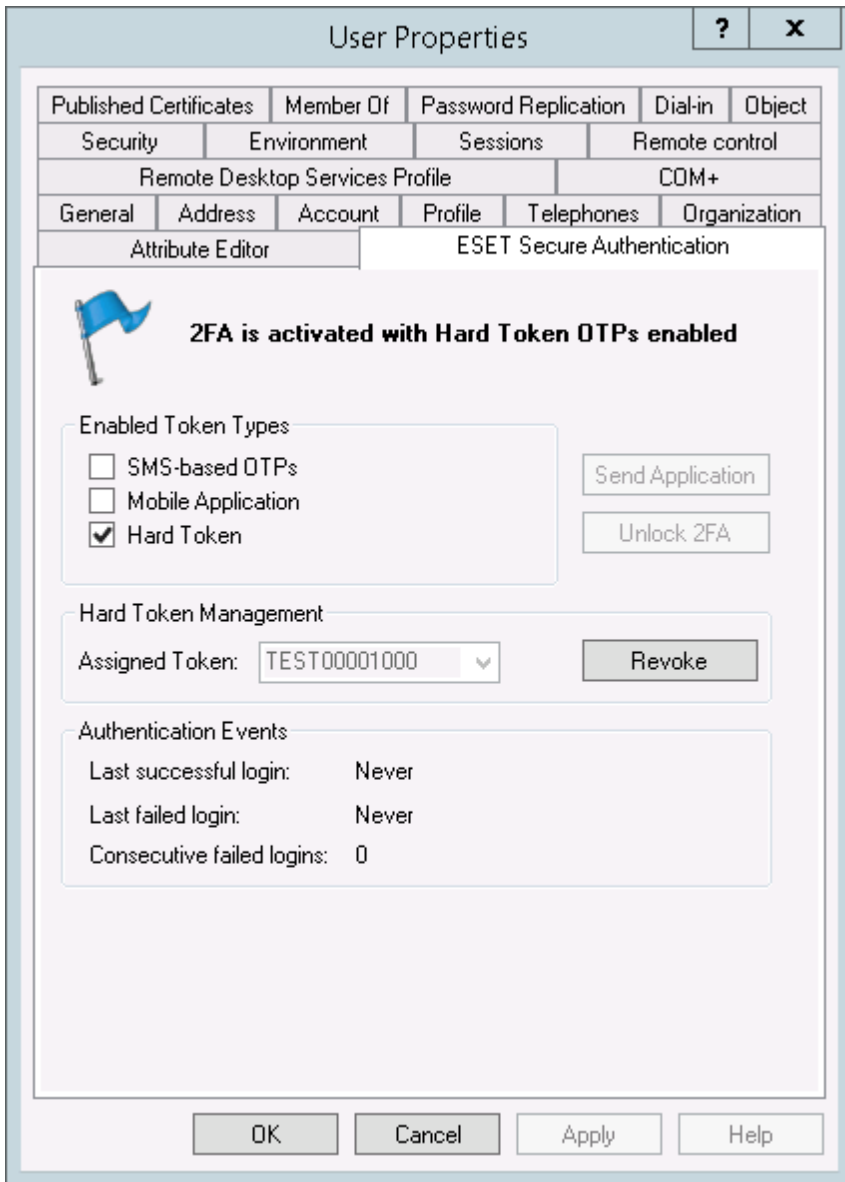
When authenticating OTPs, a user has 10 opportunities to enter an incorrect OTP. On the 11th failed OTP, a user's 2FA gets locked. This is to prevent brute force guessing of OTPs. When a user's 2FA is locked, a red flag is displayed:



If it has been confirmed that the user's identity is not under attack, clicking on the Unlock 2FA button will unlock the user's 2FA.

If Hard Token OTPs have been enabled in the MMC, then the Hard Token check-box will become available. There are then more states in which the user may potentially find him or herself. The user can be enabled for any combination of the three OTP types, including a transitioning state. The different possibilities are listed below.

The user may be in a Hard Token OTP only state:




Or the user may be in a transitioning state where all three OTP types are enabled. In this state, a user will receive SMS OTPs when authentication attempts are initiated, but as soon as a valid mobile OTP is used for authentication, SMS OTPs will be disabled, and the user will only be able to authenticate using mobile or Hard Token OTPs:

User Properties [?] [X]

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile			COM+		
General	Address	Account	Profile	Telephones	Organization

Attribute Editor | ESET Secure Authentication

 **2FA activated; user transitioning from SMS-based OTPs to a Mobile App; Hard Token OTPs enabled**

Enabled Token Types

- SMS-based OTPs
- Mobile Application
- Hard Token

Buttons: Send Application, Unlock 2FA

Hard Token Management

Assigned Token: TEST00001000 [v] [Revoke]

Authentication Events

- Last successful login: Never
- Last failed login: Never
- Consecutive failed logins: 0


Buttons: OK, Cancel, Apply, Help

In the following state the user is enabled for both Hard Token and mobile OTPs:

User Properties [?] [X]

Published Certificates | Member Of | Password Replication | Dial-in | Object
Security | Environment | Sessions | Remote control
Remote Desktop Services Profile | COM+
General | Address | Account | Profile | Telephones | Organization

Attribute Editor | **ESET Secure Authentication**

 **2FA is enabled; application must be sent to user;
Hard Token OTPs are enabled**

Enabled Token Types

- SMS-based OTPs
- Mobile Application
- Hard Token

Buttons: Send Application, Unlock 2FA

Hard Token Management

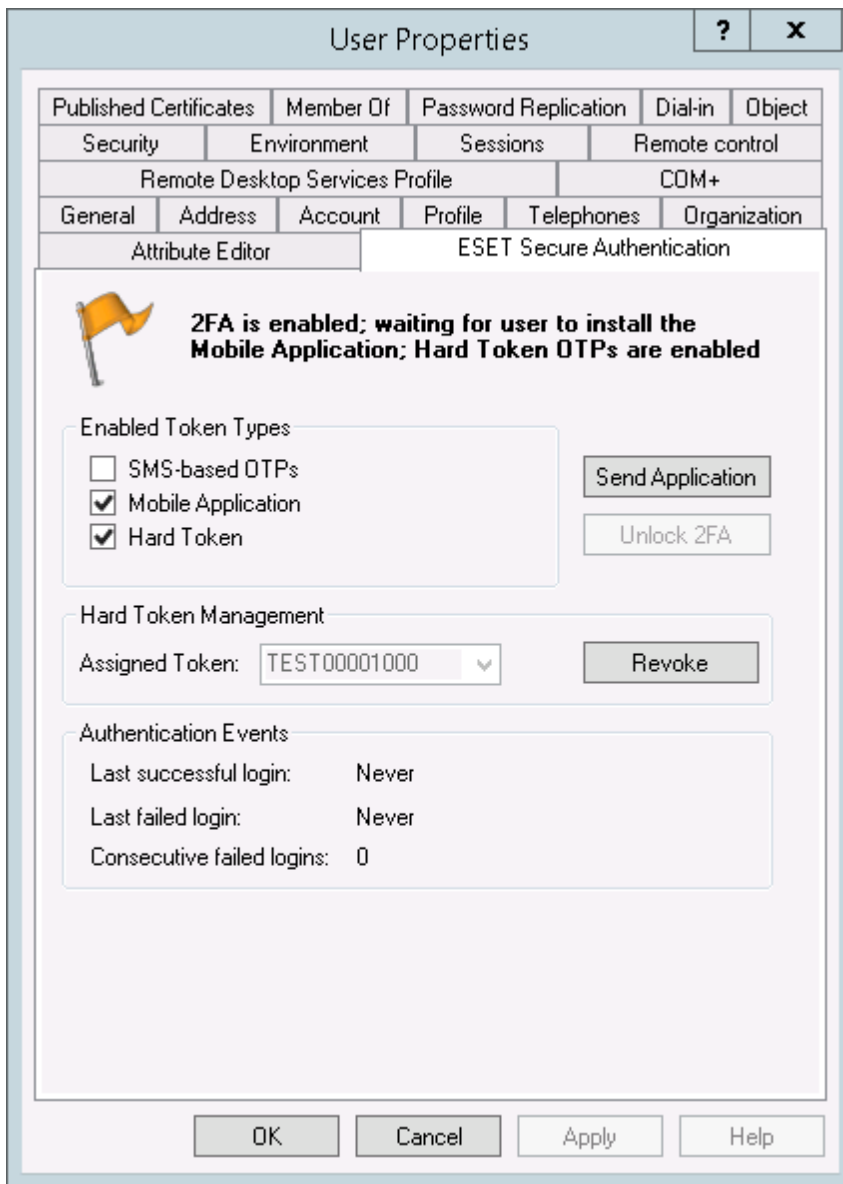
Assigned Token: TEST00001000 [v] Revoke

Authentication Events

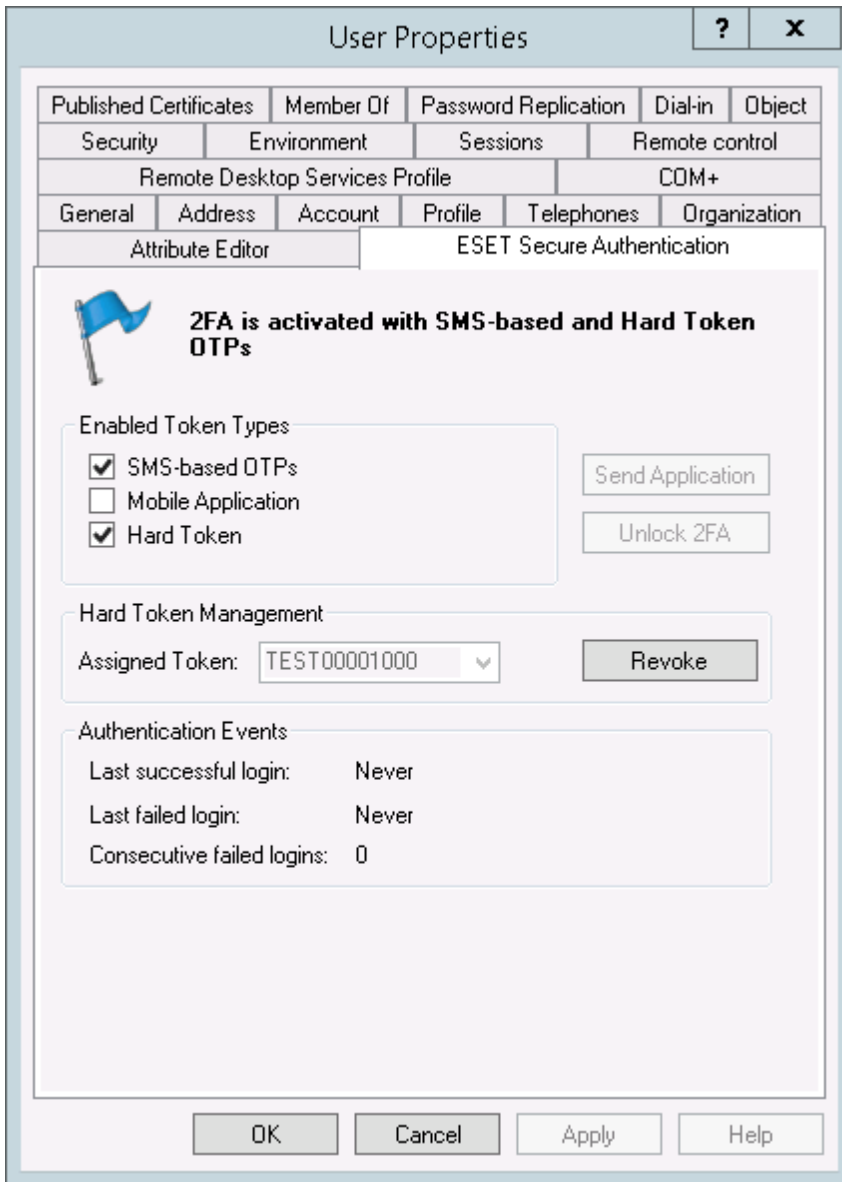
- Last successful login: Never
- Last failed login: Never
- Consecutive failed logins: 0

Buttons: OK, Cancel, Apply, Help

If the Mobile Application has been sent but not yet installed, the user will be in the following state:



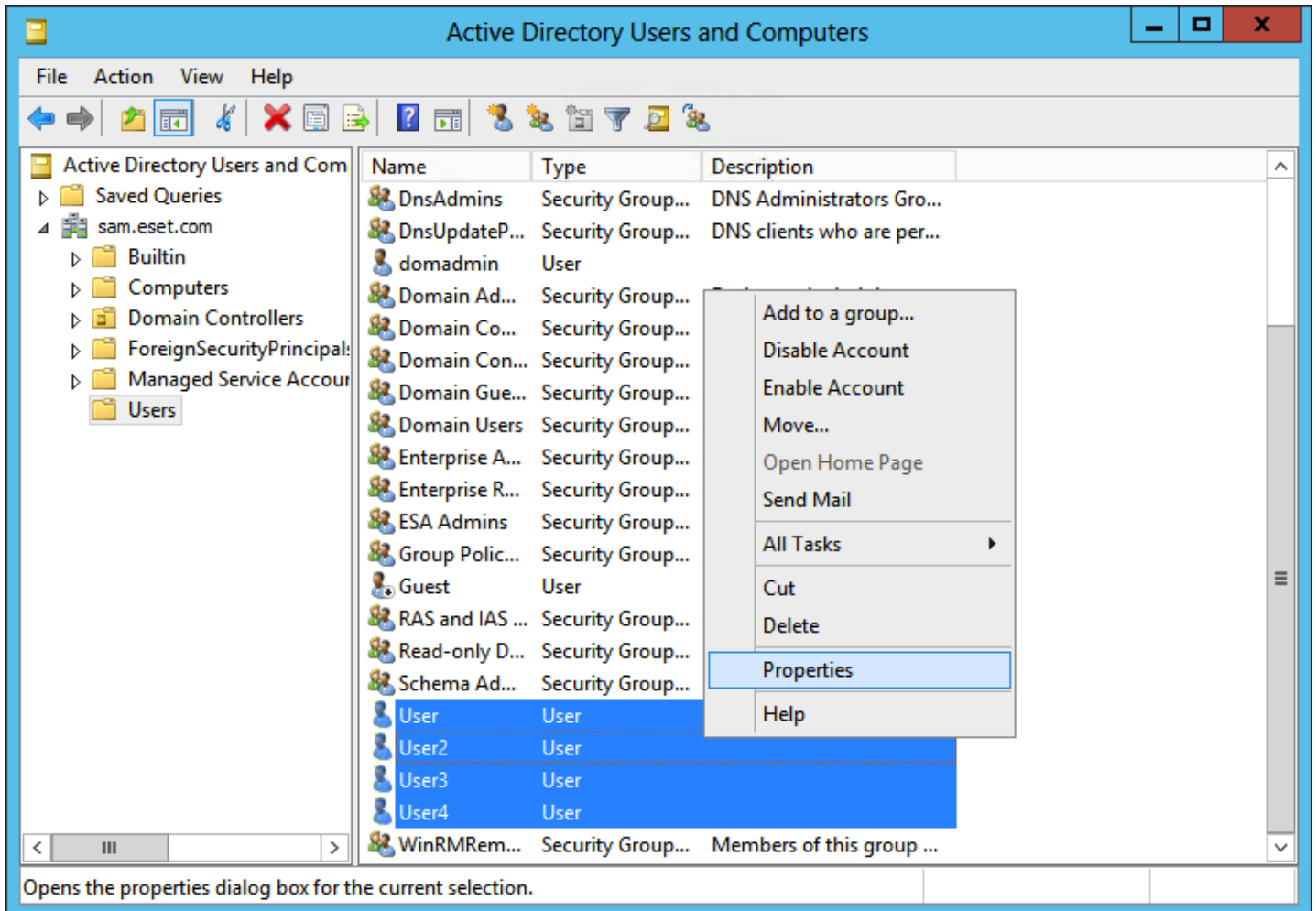
The user can also be in the state where both SMS and Hard Token OTPs are allowed:



13.2 Provisioning Multiple Phones

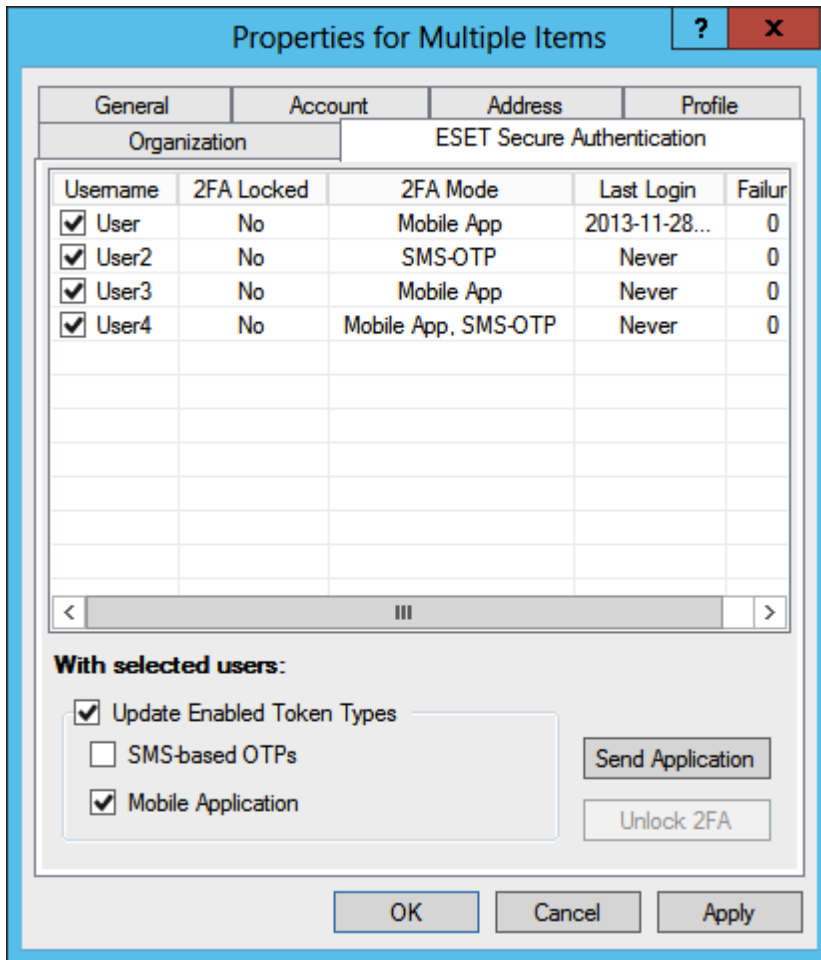
You can distribute the ESET Secure Authentication mobile app or SMS text messaging service to multiple mobile phones using the ADUC. For provisioning to multiple phones to be successful, all users must have a valid mobile phone number entered in User Properties under 'Mobile' (see the section [User Management](#) for instructions on how to enter a user's mobile phone number into User Properties).

1. Open the normal ADUC user view.
2. Hold **CTRL** and click to select the users you want to provision.
3. Right-click the group of users that you want to provision and select **Properties** from the context menu.



4. In the **Properties for Multiple Items** window, click the **ESET Secure Authentication** Tab.
5. Select the check boxes next to **Update Enabled Token Types** and **Mobile Application** (leave the check box next to **SMS-based OTPs** deselected).

6. Click **Send Application**. Your client phones will receive a text message containing a link to the ESA mobile app download page.



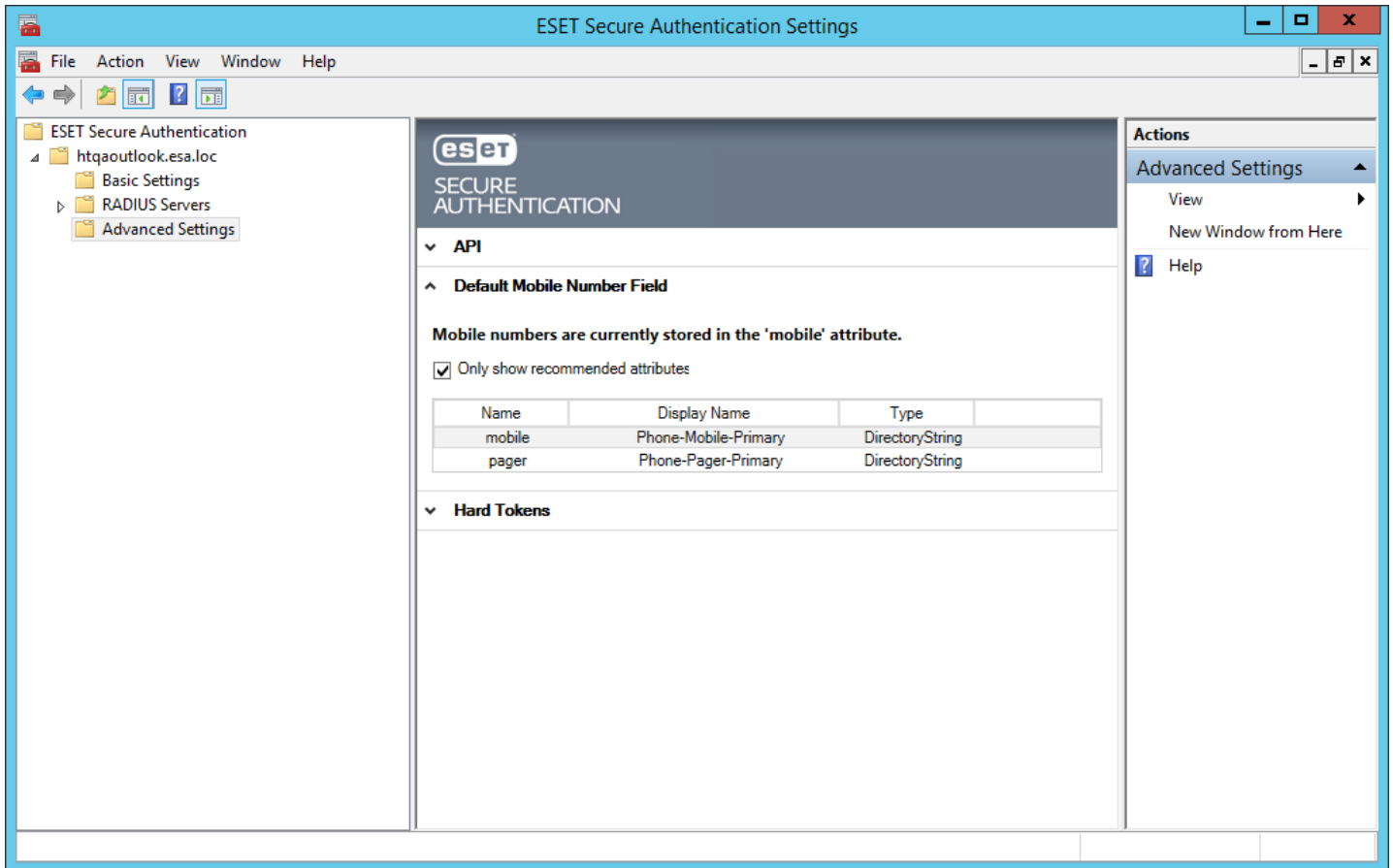
Instructions on installing and using the mobile application (click the desired mobile OS to be redirected to the corresponding article):

- [Android](#)
- [BlackBerry](#)
- [iPhone](#)
- [Windows Phone](#)

13.3 Override Mobile Number Field

You can specify the Active Directory field from which a user's mobile number is loaded. The "Mobile" field is used by default. To change the mobile number field:

1. Launch the ESA Management Console.
2. Expand the node for your domain.
3. Navigate to the Advanced Settings node.
4. Expand the Default Mobile Number Field panel.



5. You will be able to select a different field to be used for loading a user's mobile number.
6. After you have selected a different field to use, click on Save.
7. Restart the ESET Secure Authentication Core Authentication Service:
 - a. Locate the ESET Secure Authentication Core Service in the Windows Services (under **Control Panel - Administrative Tools - View Local Services**).
 - b. Right Click on the ESET Secure Authentication Radius Service and select **Restart**.

13.4 Groups Based User Management

Keeping track of which users in your domain are activated for two-factor authentication becomes hard in large domains. To solve this problem, ESET Secure Authentication provides automatic bookkeeping for your 2FA users by means of Active Directory groups membership.

Concretely, three active directory groups are created at installation time:

- ESA Users

The ESA Users group does not contain any users directly, but contains the ESA SMS Users and ESA Mobile App Users group. Transitive Group Membership may therefore be used to locate all 2FA users in your domain using this group.

- ESA SMS Users

The ESA SMS Users group contains all users in your domain that have been enabled for SMS OTPs

- ESA Mobile App Users

The ESA Mobile App Users group contains all users that have been enabled for mobile application OTPs.

Group membership is updated in real-time when users are configured in the ADUC. Finding all users that have been enabled for SMS OTPs (for example), is simple:

1. Launch the ADUC
2. Right-click on your domain node, and select Find
3. Type in "ESA SMS" and hit Enter - the group will be displayed in the Search Result section
4. Double click on the group and select the Members tab to view all users in your domain that have been enabled for SMS OTPs.

14. Advanced VPN Topics

This chapter contains the detail of all the options available when configuring two factor authentication for your VPN.

14.1 VPN Authentication Options

This section contains the detail of the options available when configuring a RADIUS client using the ESA Management Console.

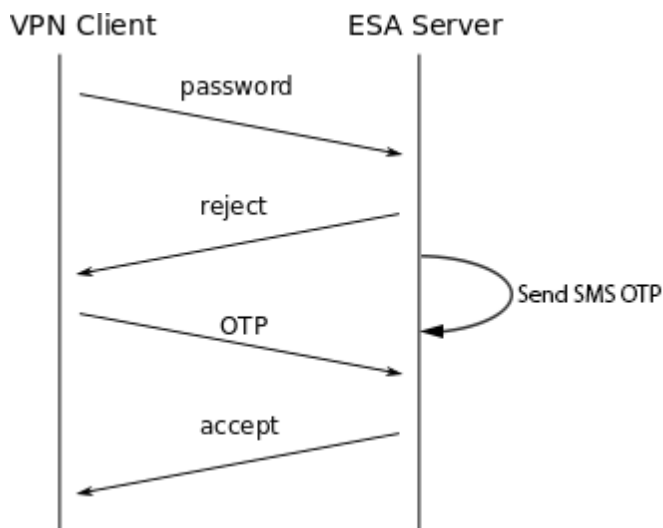
14.1.1 SMS-based OTPs

This scenario occurs if the user is configured to use only SMS-Based OTPs and the RADIUS client is configured to use SMS-based OTP authentication.

In this configuration, a user logs in with their Active Directory password. The first authentication attempt by the VPN client will fail to authenticate and the user will be prompted to enter their password again. At the same time, the user will receive an SMS with their OTP. The user then logs in with the OTP contained in the SMS. The second authentication attempt will grant access if the OTP is correct.

This sequence is depicted in Figure 1: RADIUS SMS OTP Authentication.

Supported authentication protocols: PAP, MSCHAPv2.



14.1.2 On-demand SMS-based OTPs

ESET Secure Authentication supports "On-demand SMS OTPs" for certain systems that support primary authentication against Active Directory and secondary authentication against a RADIUS server. In this scenario, users that have already been authenticated against Active Directory have to type the letters 'sms' (without apostrophes) into the **ESA OTP** field to receive a One Time Password via SMS.

NOTE: This feature should only be used when instructed to do so by an official ESET Secure Authentication Integration Guide, as it may allow users to authenticate with only an OTP if used incorrectly.

14.1.3 Mobile Application

This scenario occurs if the user is configured to use only the Mobile Application and the RADIUS client is configured to use Mobile Application-based OTP authentication.

The user logs in with an OTP generated by the Mobile Application. Note that PIN enforcement is strongly recommended in this configuration to provide a second authentication factor.

Supported PPTP Protocols: PAP, MSCHAPv2.

NOTE: If the Mobile Application has PIN protection enabled, it will allow a user to log in using an incorrect PIN code to protect the correct PIN code from brute-force attacks. For example, if an attacker attempts to log into the Mobile Application using an incorrect PIN code, they might be granted access, but no OTP will work. After entering several wrong OTPs, the 2FA of the user account (which the Mobile Application belongs to) will be automatically locked. This represents a minor issue for a general user: If the user happens to log into the Mobile Application using an incorrect PIN code, then changes the PIN code to a new one, all the tokens included in the Mobile Application will become unusable. There is no way to repair such tokens—the only solution is to re-provision tokens to the Mobile Application. Therefore, we advise users to try an OTP before changing their PIN code—if the OTP works, it is safe to change the PIN code.

Compound Authentication Enforced

This scenario occurs if the RADIUS client is configured to use **Compound Authentication**. This authentication method is restricted to users who are configured to use the Mobile Application.

In this scenario, a user logs into the VPN by entering their Active Directory (AD) password concatenated with an OTP generated by the Mobile Application. For example, given an AD password of 'password' and an OTP of '123456', the user enters 'password123456' into the password field of their VPN client.

Supported authentication protocols: PAP.

14.1.4 Hard Tokens

This scenario occurs if both the user and the RADIUS client are configured to use Hard Token OTPs.

Based on the configuration of your VPN client, you can either use single Hard Token authentication or compound Hard Token authentication.

When using compound Hard Token authentication a user logs into the VPN by entering their Active Directory (AD) password concatenated with an OTP generated by their Hard Token. For example, given an AD password of 'password' and an OTP of '123456', the user enters 'password123456' into the password field of their VPN client.

Supported authentication protocols: PAP.

14.1.5 Migration from SMS-Based OTPs to Mobile Application

This scenario occurs if the user is configured to use both SMS-based OTPs and the Mobile Application, and the RADIUS client is configured to use OTP authentication.

In this configuration, the user may use either the SMS-based OTP or Mobile Application OTP scenarios (as described above) to log in.

If the user logs in with an OTP generated with their Mobile Application, SMS OTP authentication will automatically be disabled. On subsequent attempts, SMS based OTPs will not be accepted as log-in credentials.

Supported authentication protocols: PAP, MSCHAPv2.

14.1.6 Non-2FA Pass-through

This scenario occurs if the user is not configured for SMS-, Mobile Application- or Hard Token-based OTPs, and the RADIUS client configuration option to allow **Active Directory passwords without OTPs** is selected.

In this configuration the user logs in with their Active Directory password.

Supported authentication protocols: PAP, MSCHAPv2.

NOTE: For Microsoft Routing & Remote Access Server (RRAS) PPTP VPNs, encryption of the VPN connection is not performed when the PAP authentication protocol is used, and is therefore not recommended. Most other VPN providers encrypt the connection regardless of the authentication protocol in use.

14.1.7 Access Control Using Group Membership

ESA supports the ability to only allow members of a specific AD security group to log in to the VPN using 2FA. This is configured on a per RADIUS client basis under the **Access Control** heading.

14.2 OTPs and Whitespace

OTPs are displayed in the mobile application with a space between the 3rd and 4th digits in order to improve readability. All authentication methods except MS-CHAPv2 strip whitespace from the provided credentials, so a user may include or exclude whitespace without affecting authentication.

14.3 ESA Authentication Methods and PPP Compatibility

This section explains which PPP authentication methods are compatible with which ESA authentication methods. The VPN server must be configured to allow all protocols that clients might want to use. End-user VPN clients need only be configured for a single protocol.

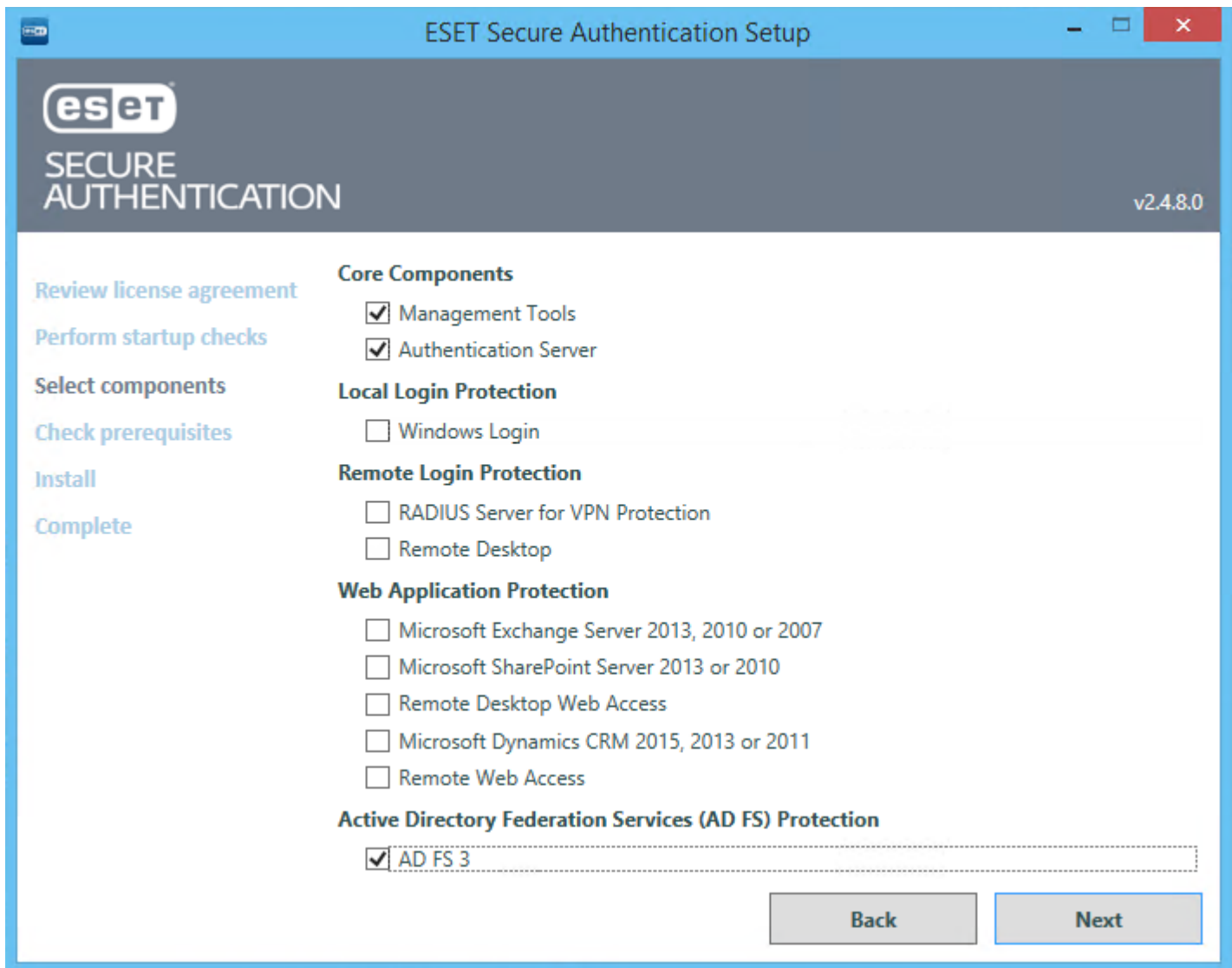
Whenever more than one protocol is supported, VPN clients should be configured to use MS-CHAPv2 with 128-bit MPPE. This means that PAP is only recommended for Compound Authentication.

Authentication Method	PAP	MS-CHAPv2	MS-CHAPv2 with MPPE
SMS-Based OTPs	Supported	Supported	Supported
On-demand SMS-Based OTPs	Supported	Not supported	Not supported
Mobile-Application (OTP Only)	Supported	Supported	Supported
Mobile Application (Compound Authentication)	Supported	Not supported	Not supported
Hard Token OTPs	Supported	Not supported	Not supported
Active Directory passwords without OTPs	Supported	Supported	Supported

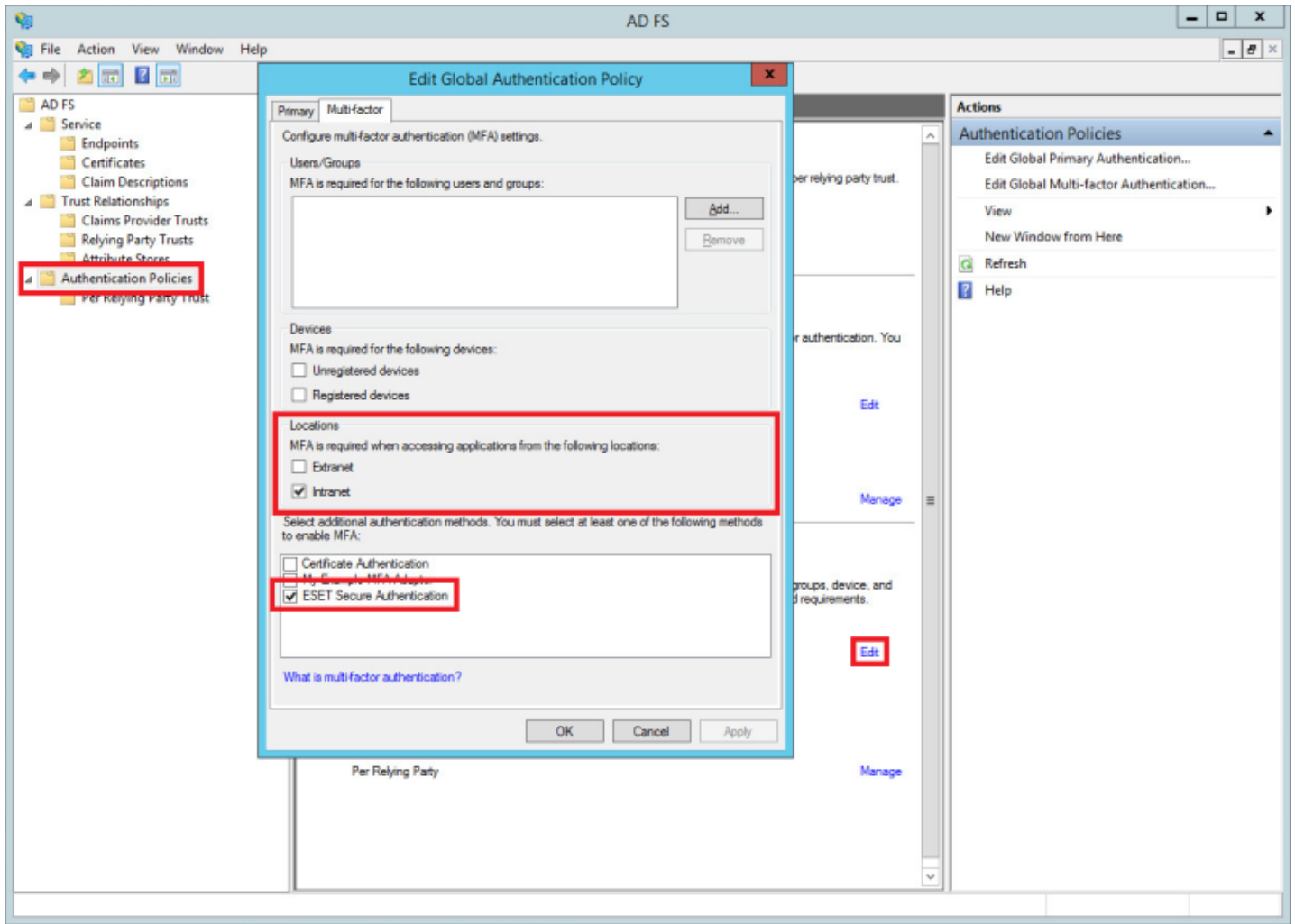
15. AD FS 3

ESA is a great choice for security if you are using Active Directory Federation Services (AD FS) 3 and want to secure it with 2FA.

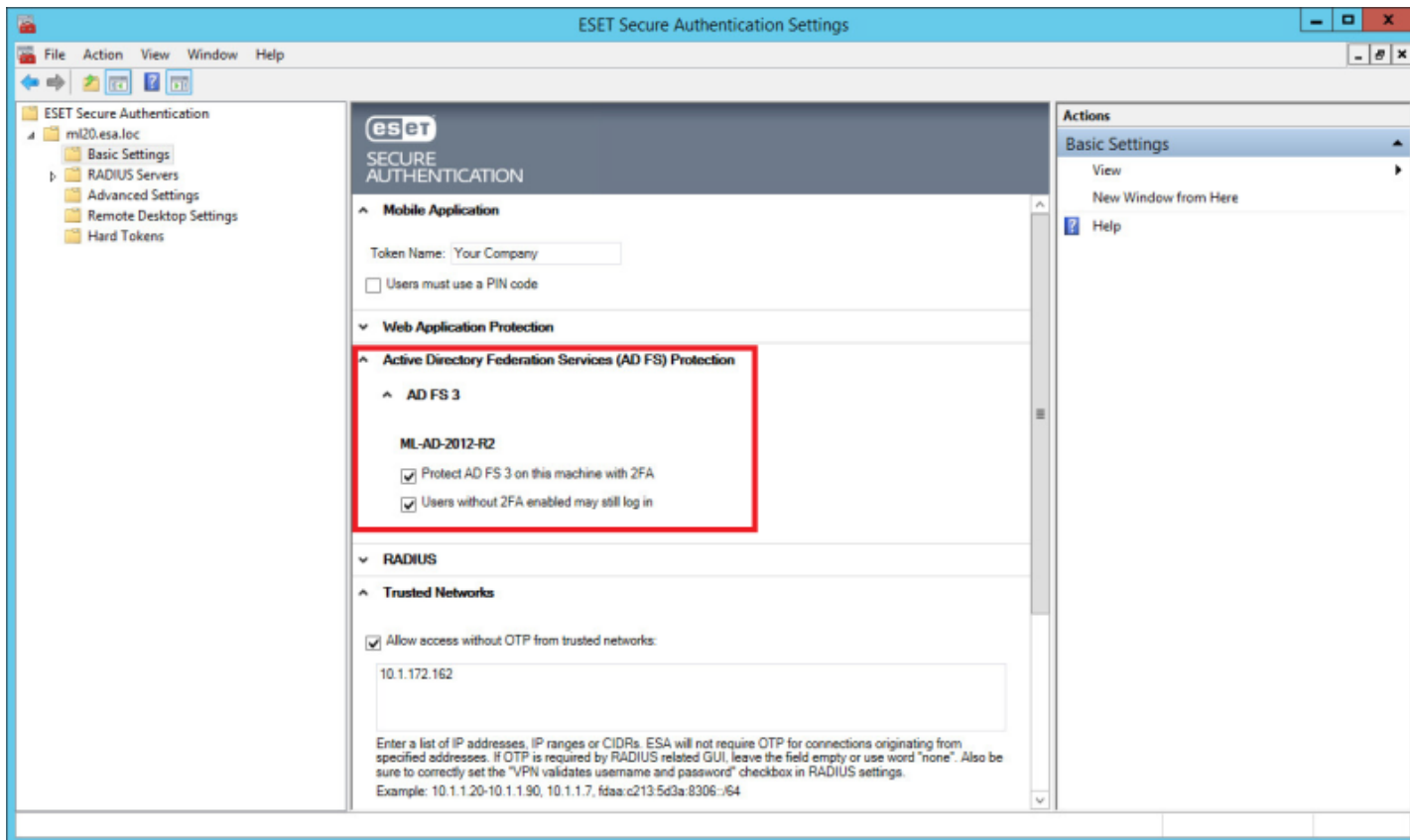
During the installation of ESA on the computer running AD FS 3, select the AD FS 3 component and complete the installation.



During the installation of AD FS configuration is modified - the ESET Secure Authentication authentication method is added and if no location is specified both Intranet and Extranet locations will be included. The image below shows the configuration changes with the Intranet location selected prior to installation of the AD FS 3 component of ESA.



Once the installation is complete, open the ESA Management Console, navigate to **Basic Settings**, expand **Active Directory Federation Services (AD FS) Protection** and you will see the **Protect AD FS 3 on this machine with 2FA** and **Users without 2FA enabled may still log in** options enabled.



If a website requiring authentication verifies the identity against AD FS 3, and 2FA protection through ESA is applied to the particular AD FS 3, you will be prompted to enter an OTP upon successful verification of identity:

ESET SECURE AUTHENTICATION

Enter OTP:

16. Auditing and Licensing

16.1 Auditing

ESA records audit entries in the Windows event logs - specifically the Application log in the Windows Logs section. The Windows Event Viewer can be used to view the audit entries.

Audit entries fall into the following categories:

- User auditing
 - Successful and failed authentication attempts
 - Changes to 2FA state, for example, when a user account becomes locked
- System auditing
 - Changes to ESA settings
 - When ESA services are started or stopped

The use of the standard Windows event logging architecture facilitates the use of third-party aggregation and reporting tools such as LogAnalyzer.

16.2 Licensing

16.2.1 Overview

Your ESA license has three parameters:

- User Total
- Expiry Date
- SMS Credits

The details of the license are obtained from the ESET Licensing system, and the ESA system automatically checks for license validity.

The ESA Provisioning server may perform license enforcement by limiting SMS OTPs and user provisioning. In addition, the ESA authentication server performs license enforcement by limiting user management actions and (in extreme cases) disabling user authentication.

16.2.2 Warnings

Warnings are communicated to the ESA Administrator in the User Management plugin in the ADUC console and in the ESA Management Console.

During User Management

When the license is not in the normal state, a warning message will be displayed in the ADUC (user management) interface. This warning indicates the severity of the problem, but not the details, due to limited space.

During System Administration

The full license state is displayed in the system management interface. This will include the overall state of the license as well as the details of usage (user numbers, remaining SMS credits, remaining license days).

16.2.3 License States

The license of an ESA server can be in one of the following six possible states:

1. **OK:** all license parameters are within the prescribed limits
2. **Warning:** At least one license parameter is close to the allowed limit
3. **SMS Credits Expired:** SMS credits have run out and no OTP or Provisioning SMSes will be sent.
4. **Violation (full functionality):** One of the licensed parameters has exceeded allowed limits, but no enforcement is imposed
5. **Violation (limited functionality):** A license parameter has been exceeded for more than 7 days, certain user management functions are disabled
6. **ESA Disabled:** The ESA license expiry date has passed more than 30 days ago and authentication is disabled. In this case all authentication calls will fail, will lock out all authentication until ESA is uninstalled, disabled by the admin or re-licensed.

Details of License States

The following table summarizes how each of the license parameters may cause the license to be in one of the warning or error states listed above.

	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
License Expiry	less than 30 days before expiration	N/A	0 more than the license expiry date more than/equals 7 days	more than 7 days after expiration	more than 30 days after expiration
User Numbers	less than 10% or 10 seats available,	N/A	Active users exceed licensed users	more than 7 days after active users exceed license	Never

	whichever is lowest			
SMS Credits	less than 10 SMS credits remaining (Onboarding + Top-up)	0 SMS credits remain	Never	Never
				Never

16.2.4 License Enforcement


The following table describes how license enforcement is performed on the ESA authentication server. In all cases, an administrator will be able to disable ESA authentication for a subset of the users (by disabling 2FA for those users) or for all users (by means of system configuration or uninstalling the product).

	OK	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
Enable Users for 2FA	Allowed	Allowed	Allowed	Allowed	Disabled	Disabled
Provision Users	Allowed	Allowed	Disabled	Allowed	Disabled	Disabled
Authenticate with SMS OTP	Allowed	Allowed	Disabled	Allowed	Allowed	Disabled
Authenticate with mobile app	Allowed	Allowed	Allowed	Allowed	Allowed	Disabled
Authenticate with hard token	Allowed	Allowed	Allowed	Allowed	Allowed	Disabled
Manage system configuration	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Disable Users for 2FA	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed

17. High Availability View


All installed servers are displayed in the “servers” panel of the ESA management console. When more than one core service is detected on the network, all servers are displayed. Online and active servers are shown in green, and offline servers are shown in red.

^ Servers



E0N0BG5ER4V
Online

Endpoint: e0n0bg5er4v.smoke08r2.esa.loc:8000
Version: 2.0.735.0619c21



8TOQQFO0JOH
Active

Endpoint: 8toqqfo0joh.smoke08r2.esa.loc:8000
Version: 2.0.735.0619c21

Each ESA Authentication Service that gets installed on the domain registers itself in AD DNS using an SRV record (as `_esetsecauth._tcp`). When an endpoint (such as a web application or a VPN appliance) begins authentication, it first checks its internal list of known servers. If the list is empty, it performs an SRV lookup. The SRV lookup will return all Authentication Servers on the domain. The endpoint then chooses an Authentication Server to connect to. If the connection fails, it selects another server from the list and attempts to connect again.

If network redundancy is a concern when protecting your VPN with ESA, it is recommended to configure primary and secondary RADIUS authenticators on your VPN appliance. You should then install two ESA RADIUS servers on your network, and configure them accordingly.

18. Glossary

ADUC - Active Directory Users and Computers management interface

COS - Client operating system

ESA - ESET Secure Authentication

ESA core - Authentication Server that verifies the validity of an entered OTP.

MRK - [Master recovery key](#)

Online (Online mode) - A machine where the [core components](#) of ESA (at least the Authentication Server) are installed and the ESET Secure Authentication Service service is running. Available via TCP/IP connection.

Offline (Offline mode)- A machine where the [core components](#) of ESA are installed, the ESET Secure Authentication Service service is not running on that machine, or connection via TCP/IP is not available.

OTP - an one time password with limited time validity

RDP - Remote Desktop Protocol. A proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.

SOS - Server operating system