

ESET

Secure Authentication

Product Manual

(intended for product version 2.8)

[Click here to navigate to the online version of product documentation](#)

ESET SECURE AUTHENTICATION

Copyright © 2019 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. 3/28/2019

Contents

1. Overview	5
2. Requirements	6
2.1 Supported Operating Systems.....	6
2.2 Supported Web Browsers and Resolution.....	7
2.3 Supported Web Applications.....	7
2.4 Supported Mobile Phone Operating Systems.....	8
2.5 Installation Requirements.....	9
2.6 Supported Active Directory Environments.....	11
2.7 Firewall exceptions.....	12
2.8 Policies.....	12
3. Installation	13
3.1 Installation of Authentication Server	13
3.2 Installation of Reporting Engine (Elasticsearch).....	16
3.3 Installation of the Remote Desktop plugin.....	18
3.4 Installation of the Web App plugin.....	19
3.5 Installation of Windows Login plugin.....	20
3.6 Change, repair, remove installation.....	21
3.7 Installation of Windows Login and RDP protection via GPO.....	22
3.7.1 Startup script.....	24
3.7.2 Software Installation task.....	26
3.7.3 MSI arguments.....	32
3.8 Upgrade installation.....	33
3.8.1 Compatibility.....	34
4. Using reverse proxy	36
4.1 Configure proxy for ESA.....	36
5. Getting started with ESET Secure Authentication Web Console	39
5.1 Activate ESET Secure Authentication.....	41
5.2 User Management - Provisioning.....	41
5.2.1 User Status.....	45
5.2.2 Synchronizing with LDAP.....	47
5.2.3 Import users from file.....	48
5.2.4 Self-enrollment.....	49
5.3 Invitations.....	50
5.4 Use domain authentication.....	52
6. Authentication options	54
6.1 Mobile Application.....	54
6.2 Push Authentication.....	56
6.3 Custom delivery options.....	60
6.3.1 Sample PowerShell scripts.....	64
6.4 Hard Tokens	65
6.5 FIDO	68
7. Windows Login Protection	70
7.1 Master recovery key.....	72
8. VPN Protection	74
8.1 Configuration.....	74
8.2 Usage.....	76
8.3 VPN Authentication Options.....	76
8.3.1 SMS-based OTPs.....	77
8.3.2 On-demand SMS-based OTPs.....	77
8.3.3 Mobile Application.....	77
8.3.4 Hard Tokens.....	78
8.3.5 Migration from SMS-Based OTPs to Mobile Application.....	78
8.3.6 Non-2FA Pass-through.....	79
8.3.7 Access Control Using Group Membership.....	79
8.4 ESA Authentication Methods and PPP Compatibility.....	79
9. RADIUS PAM modules on Linux/Mac	80
9.1 Mac OS - configuration.....	80
9.2 Linux - configuration.....	83
9.3 Other RADIUS configurations.....	86
10. Web Application Protection	91
10.1 Configuration.....	91
10.2 Usage.....	91
11. Remote Desktop Protection	94
11.1 Configuration in an Active Directory environment.....	94
11.2 Allowing Non-2FA Users.....	95
11.3 Usage.....	95
11.4 Remote Desktop Web Access.....	96
12. IP address whitelisting	98
13. AD FS	100
14. API	103
14.1 Integration Overview.....	103
14.2 Configuration.....	104
14.3 Replacing the SSL Certificate.....	105
14.4 Generate custom SSL Certificate.....	106
15. Auditing and Licensing	108
15.1 Reports.....	108
15.2 Auditing.....	109
15.3 License Overview.....	110

15.4 License States.....	110
15.5 License Enforcement.....	111
16. High Availability View.....	112
17. Troubleshooting.....	113
18. Glossary.....	114

1. Overview

ESET Secure Authentication (ESA) adds Two Factor Authentication (2FA) to Microsoft Active Directory domains or local area network, that is, an one-time password (OTP) is generated and has to be supplied along the generally required username and password, or a push notification is generated and has to be approved on the user's cell phone running Android OS, iOS or Windows once the user has successfully authenticated using their general access credentials.

Push notifications require Android 4.0.3 and later along with Google Play services 10.2.6 and later, or iOS.

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 Windows Login plug-in provides 2FA for Windows computers.
- 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 installed in an Active Directory environment:
 - 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.



2FA enabled for Domain Admin user

If a Domain Admin user has 2FA enabled during their ESA 2.7.x upgrade, access to the Active Directory Users and Computers > **ESET Secure Authentication** screen and ESA Management Console will be removed. The [ESA Web Console](#) must be used instead.

Alternatively, disable 2FA for the Domain Admin user, create another user with 2FA disabled and add the user to the ESA Admins group, or [disable 2FA for the ESA Webconsole](#).

- ESA Web Console, an all-in-one management tool, can also be used to configure ESET Secure Authentication and manage users.
- ESA installed in standalone mode:
 - ESA Web Console, an all-in-one management tool, is used to configure ESET Secure Authentication and manage users.

If ESA is installed in an Active Directory environment, it stores data in the Active Directory data store. Since ESA data is automatically included in your Active Directory backups, there is no need for additional backup policies.

2. Requirements

An Active Directory domain or local area network is required to Install ESET Secure Authentication (ESA). The minimum supported functional level for an Active Directory domain is Windows 2000 Native. Only Windows DNS is supported.

If you use a custom DNS in your Active Directory environment, you must create an SRV record in your DNS prior to installing the Authentication Server using the following information:

- **Type:** SRV
- **Name:** `_esetsecauth`
- **Protocol:** `_tcp`
- **Port number:** Use the port number you configured for the Domain port during the [installation of the Authentication Server](#). The default Domain port number is 8000.
- **Host:** `<hostname>:<domain>`. If ESA's prerequisite check regarding Active Directory DNS fails, the correct name will be displayed.

Verify the availability of an SRV record by running the following command from a Windows computer within your Active Directory environment:

```
nslookup -type=SRV _esetsecauth._tcp
```

At least one instance of Authentication Server is essential in your domain/network, select it during the first installation of ESA on your server (main computer). Should you select a component that cannot be installed, the installer will inform you of the exact prerequisites that are not met.

[ESA components](#) can communicate with the Authentication Server via both IPv4 and IPv6.

2.1 Supported Operating Systems

Below is a list of supported operating systems (OS) in general. For component-specific [OS](#) support, refer to [installation requirements](#).

Server operating systems (SOS)


- 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
- Windows Server 2016
- Windows Server 2016 Essentials
- Windows Server 2019
- Windows Server 2019 Essentials

Client operating systems (COS)

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10 (including version 1809 / Redstone 5)

RADIUS Server on Windows Small Business Server

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`

 Installing ESA Core (Authentication Server) and RADIUS Server on a [COS](#) in the list of [Supported Operating Systems](#) might not be in alignment with Microsoft's licensing policy. Consult Microsoft's licensing policy or your software supplier for details. Moreover, a [COS](#) may present other limitations (for instance number of maximum concurrent TCP connections) compared to a [SOS](#).

2.2 Supported Web Browsers and Resolution

ESET Secure Authentication Web Console has optimal functionality in the following browsers:

Microsoft Internet Explorer	11
Google Chrome	latest
Mozilla FireFox	latest
Microsoft Edge	latest
Safari	latest

Note

The execution of JavaScript needs to be enabled in your web browser.

Domain authentication is not supported in Safari.

The minimum resolution required is 1024x768.

2.3 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 Access - Exchange Client Access Server (CAS)
 - Exchange Control Panel
- Microsoft Exchange 2013
 - Outlook Web App - Exchange Mailbox Server Role (MBX)

- Exchange Admin Center
- Microsoft Exchange 2016
 - Outlook Web App - Exchange Mailbox Server Role (MBX)
 - Exchange Admin Center



ESA adds 2FA protection only to web-based interface of Outlook Web Access. Login to Microsoft Outlook and similar email clients cannot be protected by ESA, due to the nature of their protocol, also known as RPC over HTTPS. We recommend not to expose such email clients to external access. See how to control access to Exchange Web Services: [https://msdn.microsoft.com/en-us/library/office/dn467892\(v=exchg.150\).aspx](https://msdn.microsoft.com/en-us/library/office/dn467892(v=exchg.150).aspx)

- Microsoft Dynamics CRM 2011
- Microsoft Dynamics CRM 2013
- Microsoft Dynamics CRM 2015
- Microsoft Dynamics CRM 2016
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016
- Microsoft SharePoint Foundation 2010
- Microsoft SharePoint Foundation 2013
- Microsoft Remote Desktop Web Access
- Microsoft Terminal Services Web Access
- Microsoft Remote Web Access



Note

Along the [supported web browsers](#), Internet Explorer version 9 and 10 are also supported.

2.4 Supported Mobile Phone Operating Systems

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

- iOS 9 to iOS 12
- Android™ 4.1 to Android 9.0 - Google Play Services 10.2.6 are required for both push notifications and [provisioning](#)
 - The permission to access the camera and flashlight is required to scan the QR code
- Windows Phone 8.1 to Windows 10 Mobile

2.5 Installation Requirements

Secure installation requires outbound connectivity to esa.eset.com on TCP port 443. If installing in an Active Directory environment, the installer must be run by a member of the "Domain Administrators" security group, or by a user with administrator privileges. Another requirement for running the installer is to have .NET Framework Version 4.5 (Full Install). The installer will automatically attempt to install .NET 4.5 if it is not already installed.

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

Windows Firewall exceptions that are essential for the proper function of ESET Secure Authentication will be added automatically as part of the installation. If you are using 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 Server 2008 or later [SOS](#) in the list of [Supported Operating Systems](#)
- If installing in an Active Directory environment, the installer must be run by 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 Server 2008 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)



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.

- **Reporting Engine (Elasticsearch):**

- Server JRE ([Java SE Runtime Environment](#)) version 1.8.0_131 and later, or [OpenJDK](#) 10.0.2 and later
- JAVA_HOME and PATH system environment variables contain the path to your installation of Server JRE or OpenJDK
- .NET Framework version 4.7.2

- **RADIUS Server:**

- Windows Server 2008 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 4.5

- **Web App Plug-in for Microsoft Dynamics CRM:**
 - Microsoft Dynamics CRM 2011, 2013 or 2015
 - .NET Framework version 4.5
- **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 4.5
- **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 4.5
- **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 4.5
- **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 or 4.0 protection:**
 - Windows Server 2012 R2

.NET Requirements:

- All components: .NET 4.5 Full Install
- Core Server: .NET 4.5 Full Install
- RADIUS Server: .NET 4.5 Full Install
- Management Tools: .NET 3.5 (4 on Windows Server 2012)
- Web App Plugin: .NET 4.5, however, IIS Filters require .Net version 3.5
- Reporting Engine (Elasticsearch) and FIDO: .NET Framework version 4.7.2

 Installing ESA Core (Authentication Server) and RADIUS Server on a [COS](#) in the list of [Supported Operating Systems](#) might not be in alignment with Microsoft's licensing policy. Consult Microsoft's licensing policy or your software supplier for details. Moreover, a [COS](#) may present other limitations (for instance number of maximum concurrent TCP connections) compared to a [SOS](#).

2.6 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 its 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.

2.7 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

2.8 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 new window will display the **Computer name**.

3. Installation

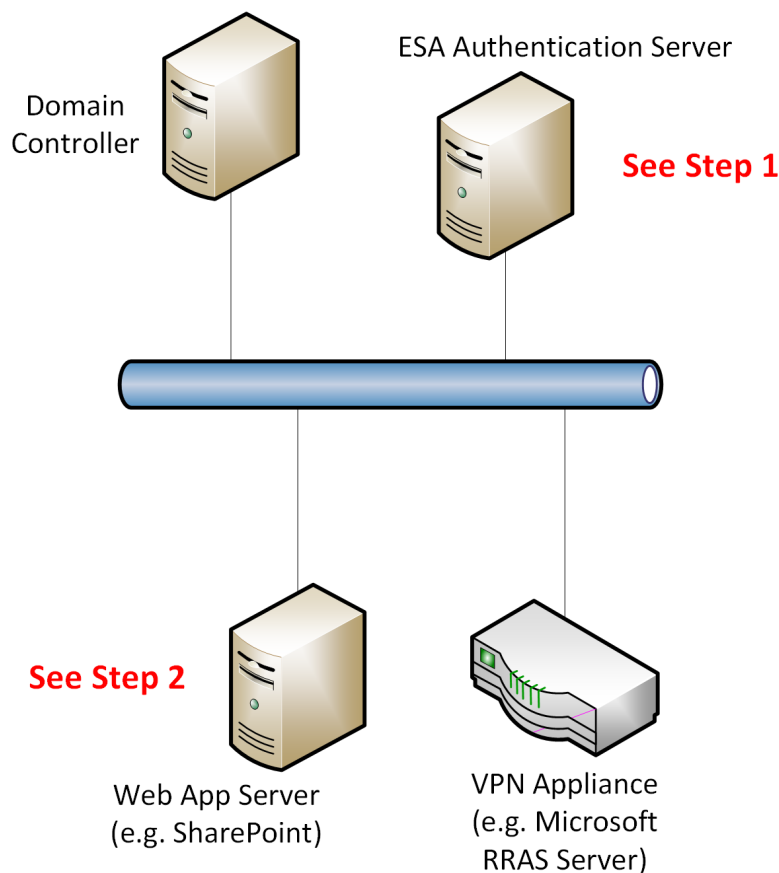
All of the following components are required for your first ESA installation:

- At least one instance of the Authentication Server
- At least one of the authentication endpoints (API, Windows Login, 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, except for ESA Web Console, which is part of the Authentication Server. As is the case with distributed systems, there are many possible installation scenarios.

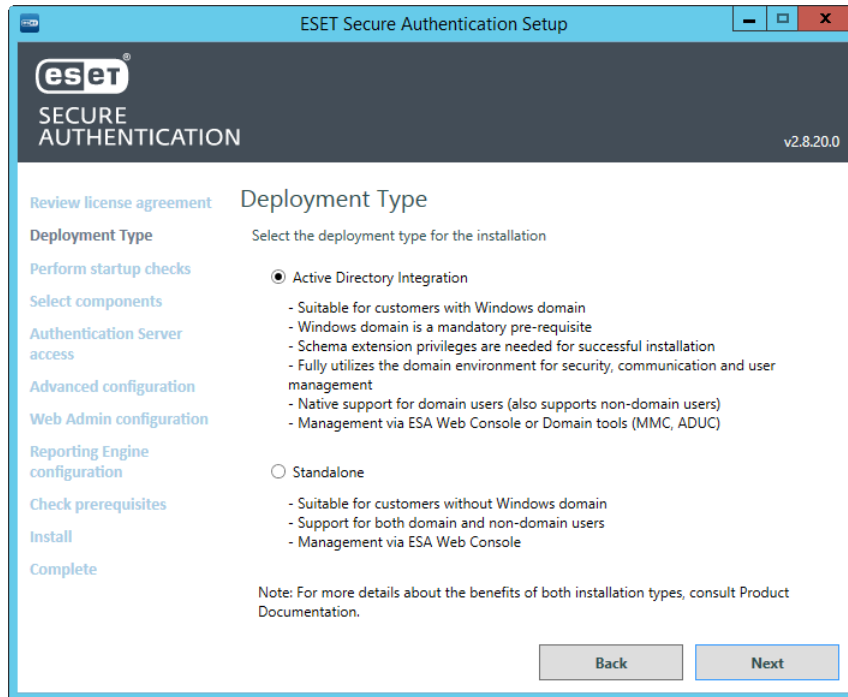
You do not have to install [ESA Authentication Server](#) on the domain controller specifically, it can be installed on any other machine within your Active Directory network.

The example below illustrates a generic installation scenario in an Active Directory environment; 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.

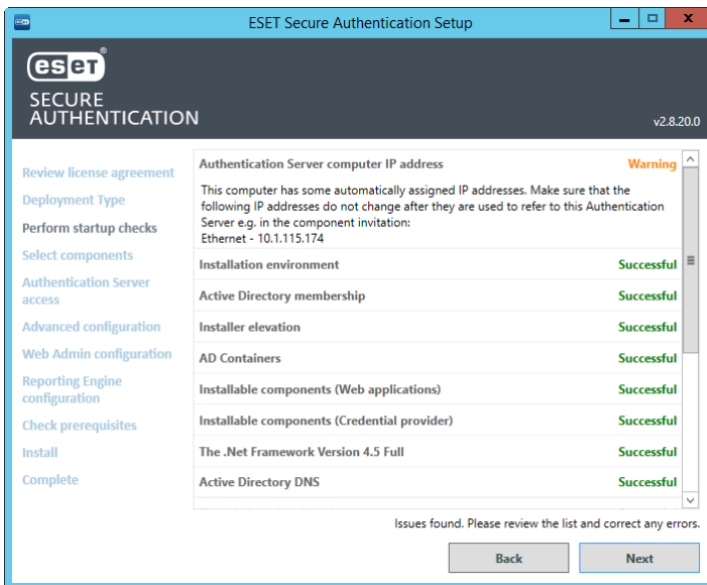


3.1 Installation of Authentication Server

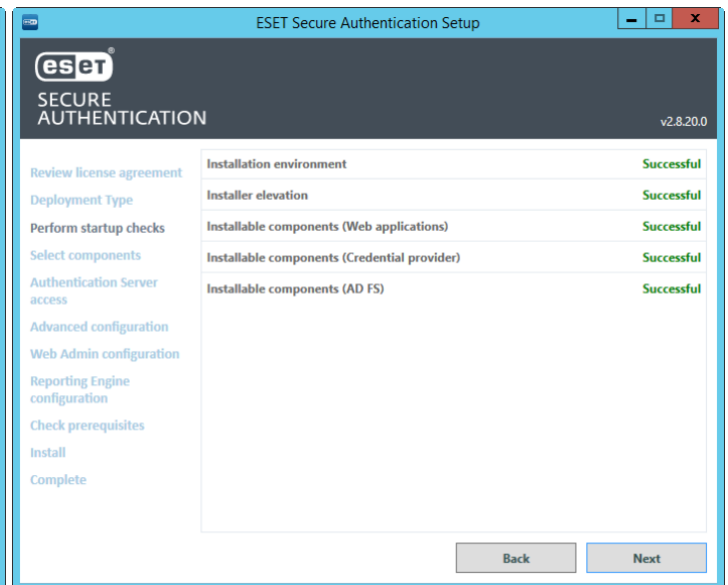
1. Run the supplied .exe file to start installation of Authentication Server on the machine that is about to host the ESA Authentication Service. The .NET Framework version 4.5 will be installed automatically if it is not detected.
2. Select deployment type
 - a. **Active Directory Integration** - This type of deployment is suitable for customers running a Windows domain network. They are not limited to protect with 2FA computers belonging to their Windows domain only, but they can invite computers from outside their network also, as long as the the Authentication Server is available [online](#).
 - b. **Standalone** - Suitable for customers not using a Windows domain. They can invite computers from their local network and other networks also. ESA related services run under SYSTEM user.



A number of prerequisite checks will be performed to ensure that the domain or installation environment 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.



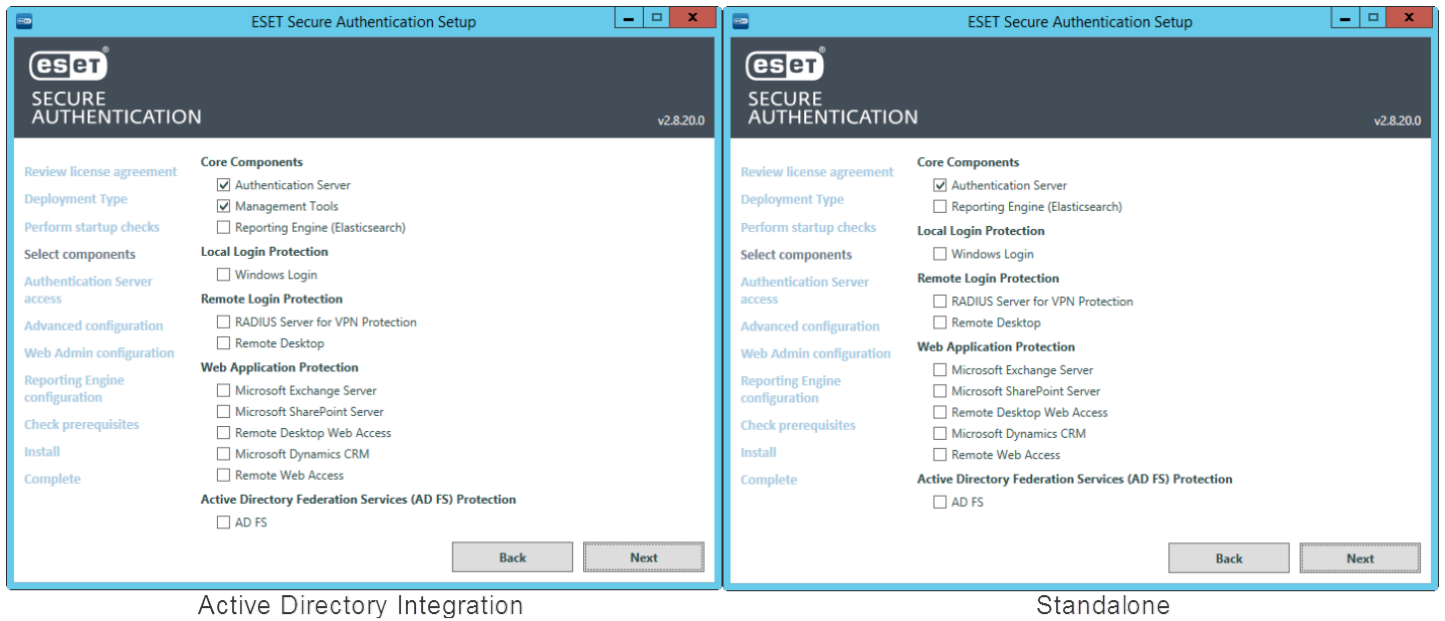
Active Directory Integration



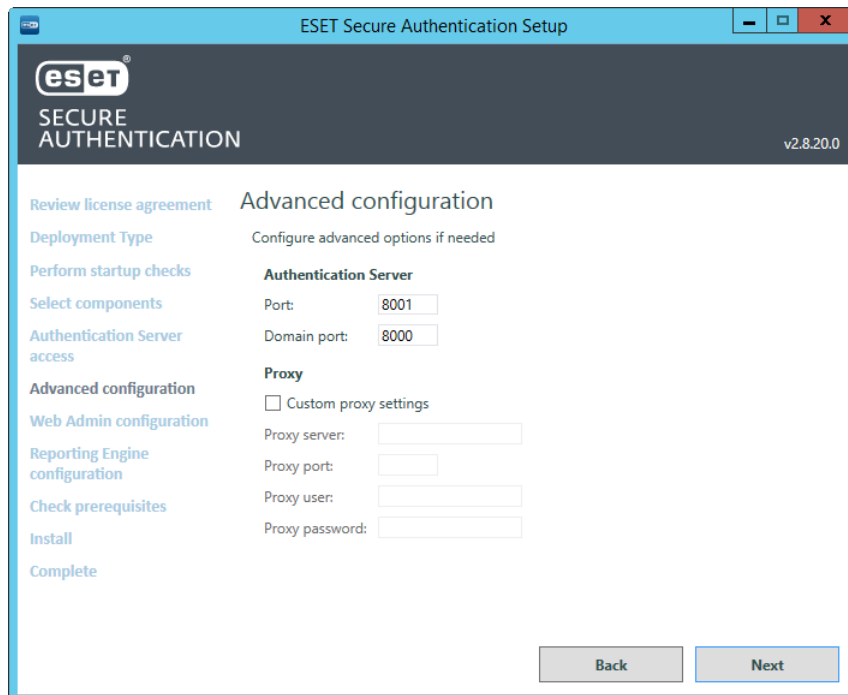
Standalone

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

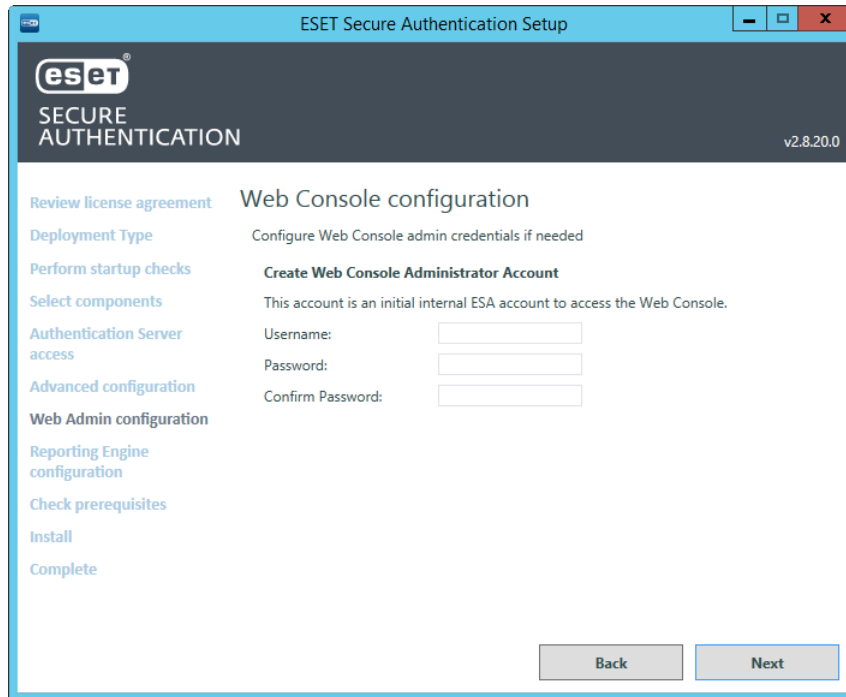
3. When prompted, make sure that **Authentication Server** component is selected, as per the figure below. If Active Directory Integration type of deployment was selected initially, then both **Authentication Server**, **Management Tools** (Microsoft Management Console for ESA) and **Reporting Engine (Elasticsearch)** will be selected automatically.



If port number 8000 (Active Directory Integration only) or 8001 is already in use on your network, select a different port for ESA Web Console. If you prefer to use a transparent proxy, select **Use proxy** and type in the corresponding values. Click **Next**. Port number 8001 is also used for [API](#).



Set the Username and Password. Click **Next**.



The subsequent **Check prerequisites** screen will reveal if the selected port(s) is (are) available.

4. Go through the remainder of the steps as prompted by the installer and close the installer when complete.
5. Use [ESA Web Console](#) to configure your installation of ESET Secure Authentication and related components, users.

3.2 Installation of Reporting Engine (Elasticsearch)

To be able to see reports inside ESA Web Console, it is essential to install Elasticsearch.

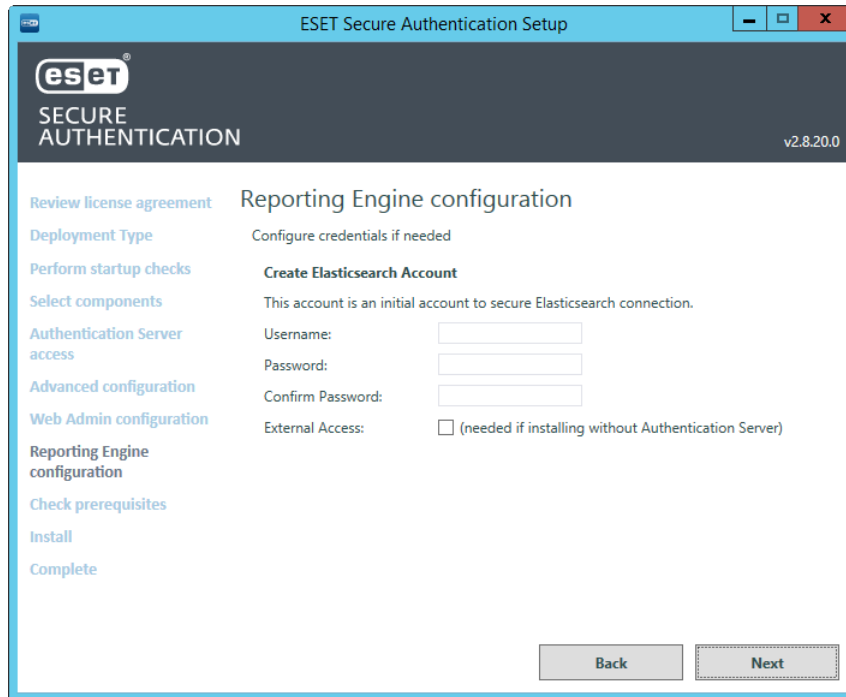
You can either install the **Reporting Engine (Elasticsearch)** component in the ESA installer, or use your existing 3rd party Elasticsearch component.

Installation from ESA installer

The Reporting Engine (Elasticsearch) component of the ESA installer can be installed along with the [Authentication Server](#) on the same computer, or separately on a different computer.

Installing both Authentication Server and Elasticsearch on the same computer

1. Follow the instructions in the [installing the Authentication Server](#) topic and make sure to leave the **Reporting Engine (Elasticsearch)** component selected along with the **Authentication Server** component.
2. In the **Reporting Engine configuration** screen, set a username and password. Click **Next**.



If the installer warns you about missing [requirements](#), make sure to fulfill the requirements before proceeding with the installation.

3. Follow the instructions in the installer to complete the remainder of the steps and close the installer when you are finished.

Installing Elasticsearch separately

If you have already installed the [Autheticnication Server](#) and you are now installing Elasticsearch separately, run the supplied .exe file again.

1. Click **Change**, select **Reporting Engine (Elasticsearch)** and click **Next**.
2. In the **Reporting Engine configuration** screen, set a username and password. Click **Next**.
3. If the installer warns you about missing requirements, make sure to fulfill the requirements before proceeding with the installation.
4. Follow the instructions in the installer to complete the remainder of the steps and close the installer when you are finished.



Note

Silent mode installation in an Active Directory environment is available via the [.msi installer](#).

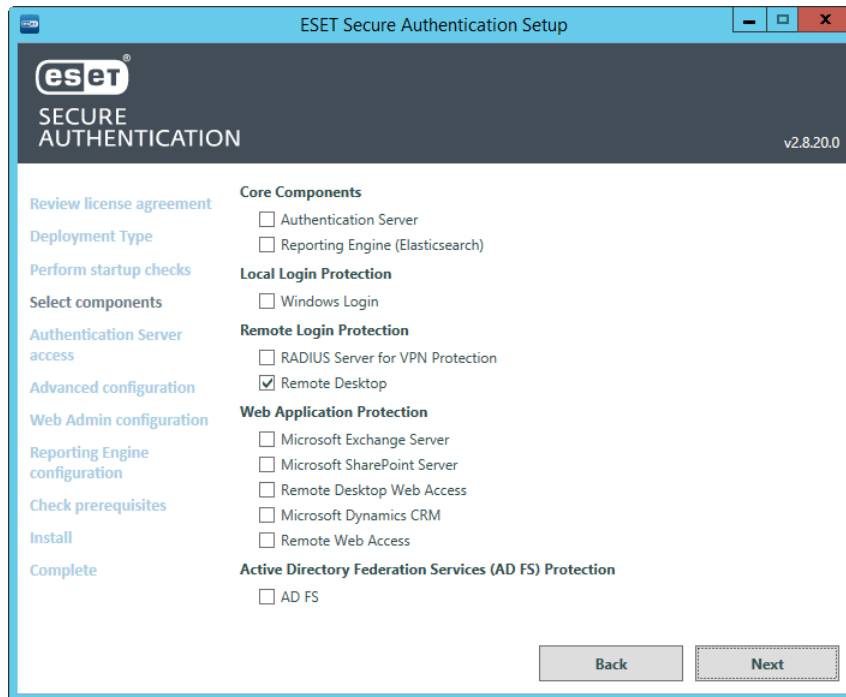
Using 3rd party installation of Elasticsearch

If you are using a 3rd party installation of Elasticsearch and want to use Reports in ESA Web Console, add the information about your Elasticsearch installation in the ESA Web Console at **Settings > Reports**.

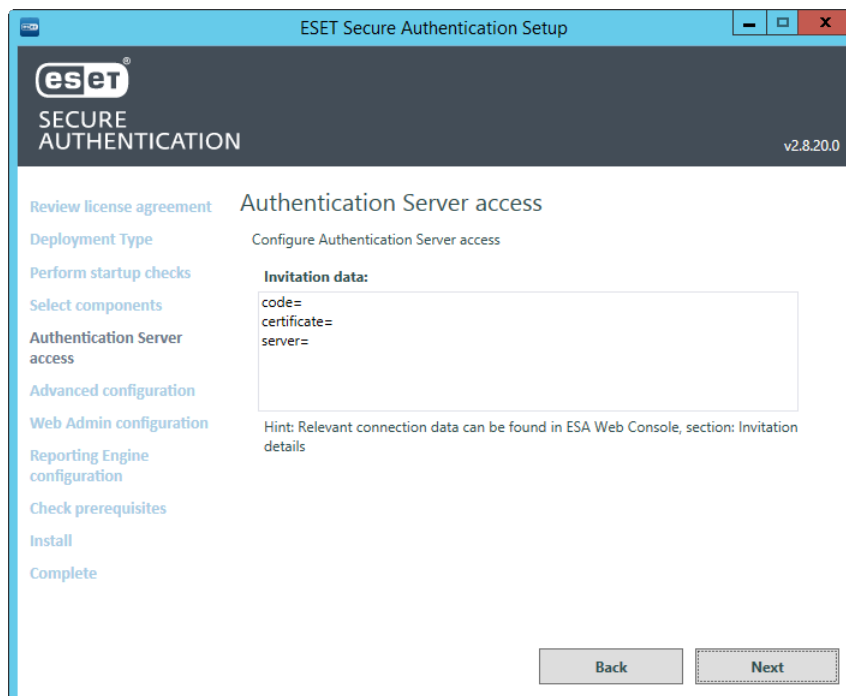
If you access Elasticsearch via [Kibana](#), you can generate various charts from the collected data.

3.3 Installation of the Remote Desktop plugin

1. To start installation, on the appropriate Remote Desktop Access machine, run the supplied .exe file. The installer will run a number of prerequisite checks as was done during the [Installation of Authentication Server](#).
2. When prompted, select the check box next to Remote Desktop and click **Next**.



3. Enter the the [connection information of Authentication Server](#) when prompted. Click **Next**.



If the connection to Authentication Server is successful, and the server certificate has been verified, select checkbox **Add certificate with this thumbprint to machine store** if available. Click **Next**.

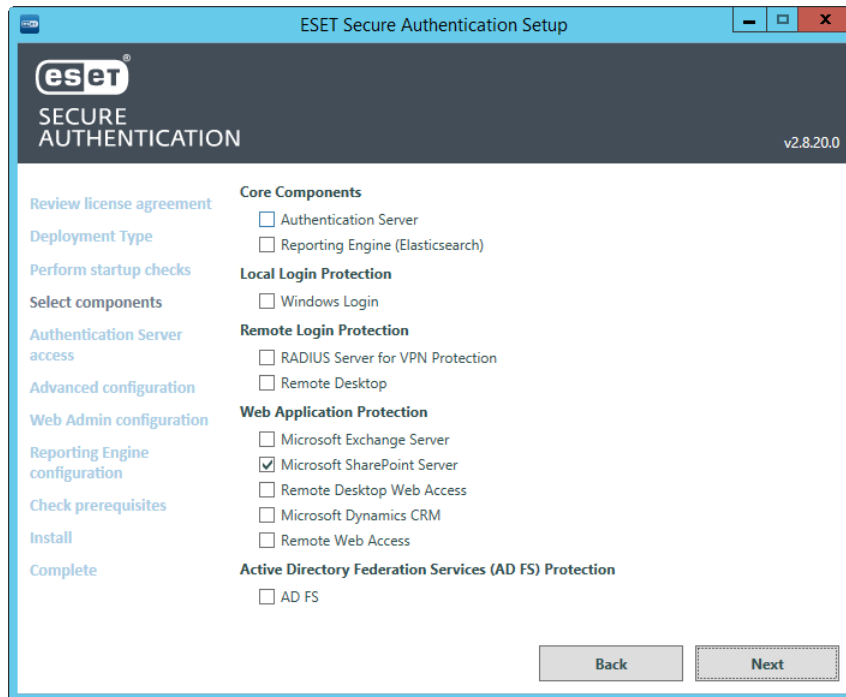


Prerequisite checks will run to verify the ESA Remote Desktop plug-in can be installed. Any failures must be corrected before installation can proceed.

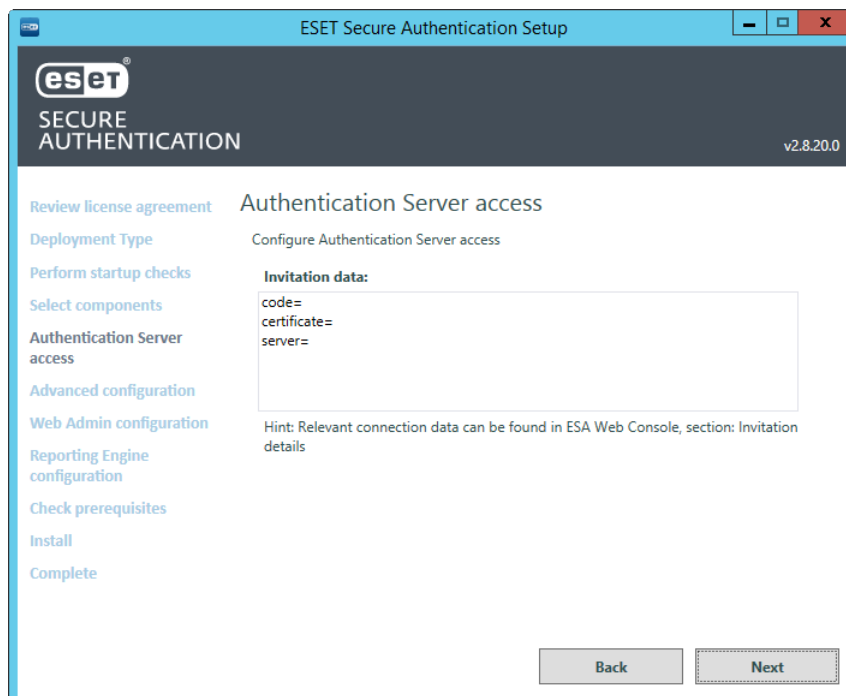
5. Go through the remainder of the steps as prompted by the installer and close the installer when complete.

3.4 Installation of the Web App plugin

1. To start installation, on the appropriate machine running the Web App, run the supplied .exe file. The installer will run a number of prerequisite checks as was done during the [Installation of Authentication Server](#).
2. When prompted, select the check box next to the applicable Web App and click **Next**.



3. Enter the the [connection information of Authentication Server](#) when prompted. Click **Next**.



If the connection to Authentication Server is successful, and the server certificate has been verified, select checkbox **Add certificate with this thumbprint to machine store** if available. Click **Next**.



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.

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



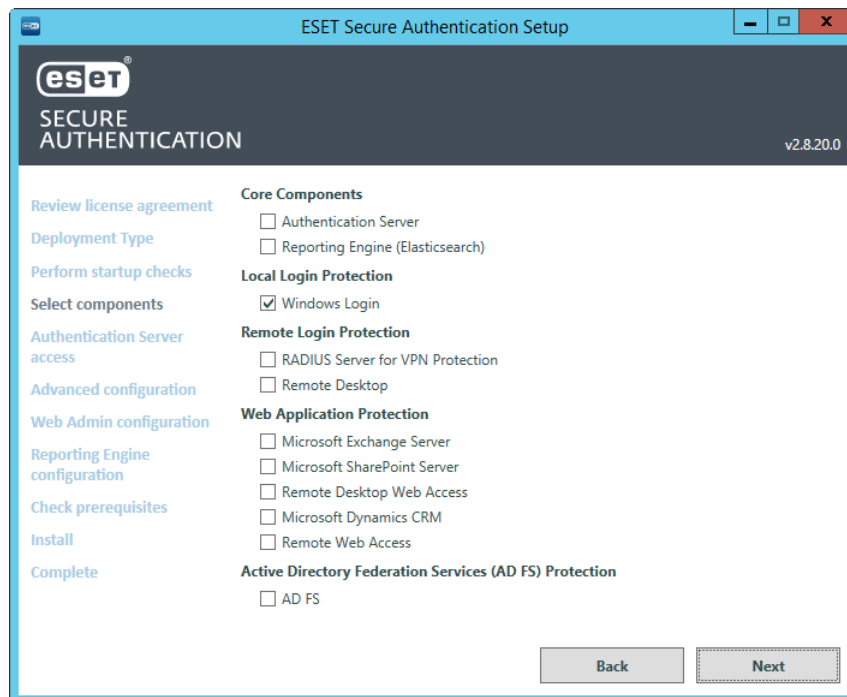
MSI installer

When using the [.msi installer](#) to install 2FA protection for Microsoft SharePoint Server, Remote Desktop Web Access, or Microsoft Dynamics CRM, run the installer with elevated privileges.

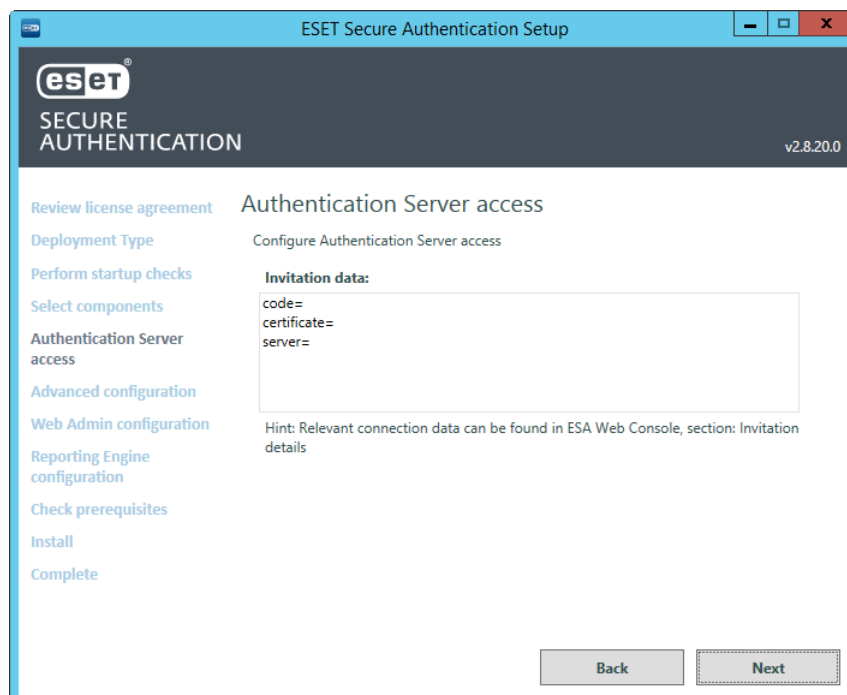
3.5 Installation of Windows Login plugin

Windows Login protection is available for local user accounts and Active Directory user accounts only.

1. To install the ESA Windows Login plug-in, on the applicable machine, run the supplied .exe file. The .NET Framework version 4.5 is installed automatically if it is not detected.
2. When prompted, click **Select components**, select the check box next to **Windows Login** and then click **Next**.



3. Enter the the [connection information of Authentication Server](#) when prompted. Click **Next**.

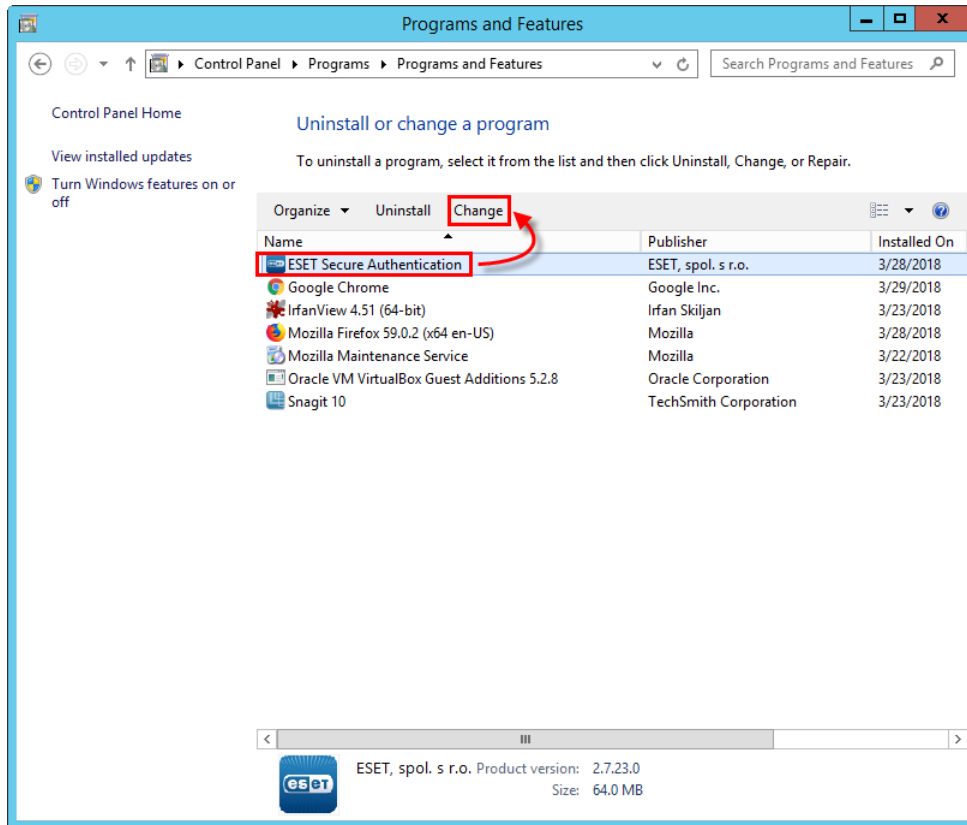


If the connection to Authentication Server is successful, and the server certificate has been verified, select checkbox **Add certificate with this thumbprint to machine store** if available. Click **Next**.

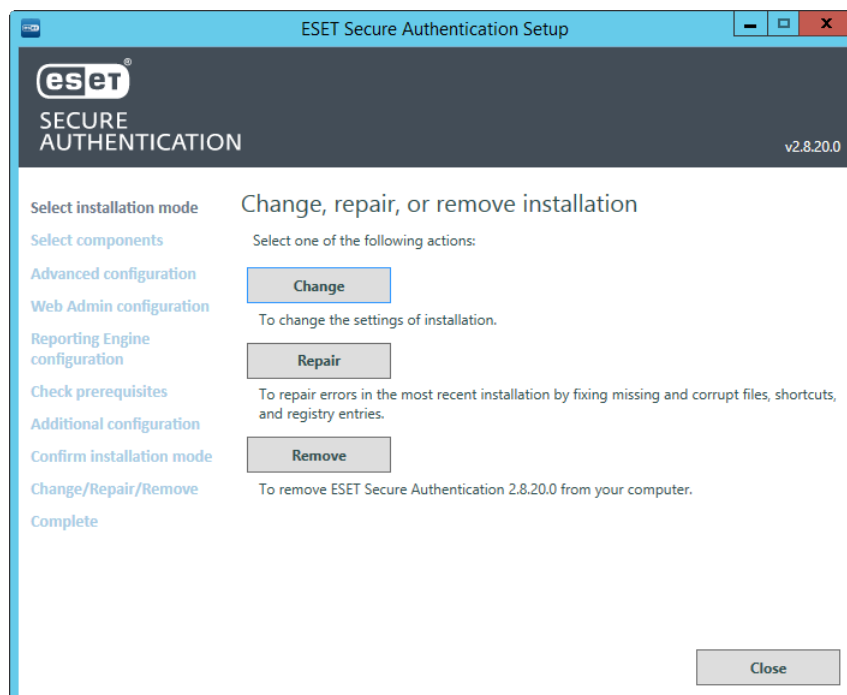
5. Go through the remainder of the steps as prompted by the installer and close the installer when complete.

3.6 Change, repair, remove installation

1. Run the supplied .exe file again or in the Windows Control Panel, click **Programs > Programs and Features**, select ESET Secure Authentication and then click **Change**.



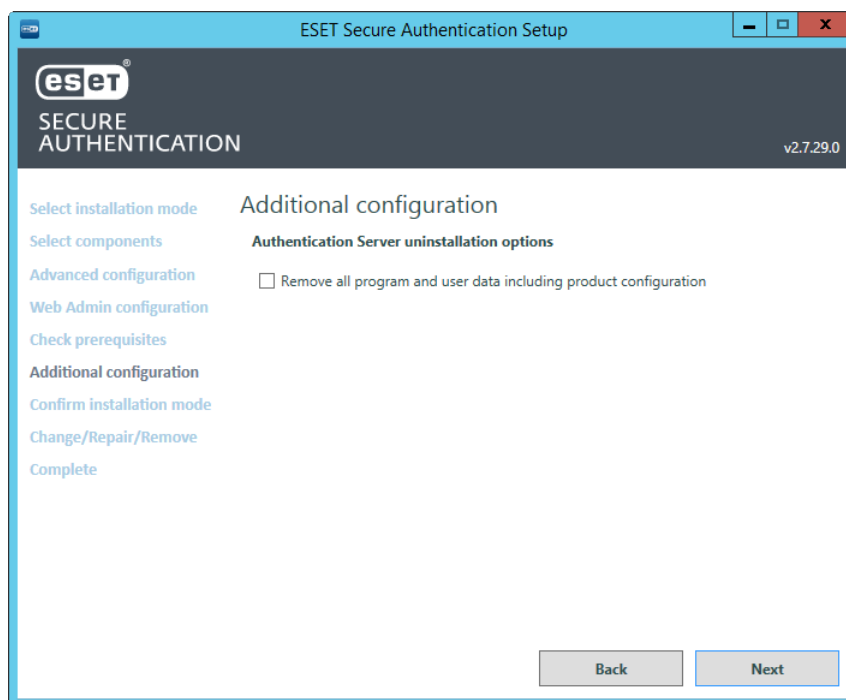
To install new components or remove existing components, click **Change** or **Remove**.



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

Removal of Authentication Server

To uninstall [ESA core](#), in the **Additional configuration** screen, select the check box next to **Remove all program and user data including product configuration**. This option is not available if ESA core is not the last component in the Active Directory domain you are preparing to uninstall or you do not have Domain Admin uninstall privileges.



If you do not want to install ESET Secure Authentication again on this machine, or you want to use this machine for a different ESET Secure Authentication Active Directory domain, select the check box next to **Remove all program and user data including product configuration**. This option is available as a **AUTHENTICATION_SERVER_CLEAN_DATA** parameter when executing a silent uninstall via [.msi package](#):

```
msiexec /x ESA.msi /qn AUTHENTICATION_SERVER_CLEAN_DATA=1
```



If [ESA core](#) was installed on a sub-domain using Domain Admin privileges, you will not be able to perform a complete uninstall using sub-domain admin privileges.

3.7 Installation of Windows Login and RDP protection via GPO

Applies to **Active Directory Integration** deployment type only.

Prerequisites

- Server (or main computer) where the [Authentication Server of ESET Secure Authentication \(ESA\)](#) is installed:
 - must belong to the same Active Directory (AD) domain as the the client computer(s), where Windows login protection and RDP protection will be installed
 - Microsoft Group Policy Management Console (GPMC) must be installed on your server. [Click here for instructions to install GPMC](#).
 - The computer you will install Windows login protection on, [must be added to EsaServices through Active Directory Users and Computers](#).
- Client computer(s):
 - [.NET Framework](#) 4.5 or higher version must be installed on the client computer.

- Active Directory membership - the computer must belong to the same AD domain as your server (main computer) where the [Authentication Server of ESA](#) is installed.
- Domain Admin privileges - the installer must be run by a member of the "Domain Administrators" security group.
- Windows 7 / Windows Server 2008 R2 or later - the computer must be running Windows 7 (or later) or Windows Server 2008 R2 (or later).

☐ Additionally, for RDP protection:

- Remote Desktop connection must be enabled on the particular computer (*Start > Control Panel > System Properties > Remote* tab).

Adding a computer to EsaServices

1. Open **Active Directory Users and Computers** management tool.
2. Click **View > Advanced Features**.
3. Navigate to **<your_active_directory_domain> > ESET Secure Authentication**, right-click **EsaServices**, select **Properties**.
4. Click **Members** tab > **Add...** > **Object Types** > select **Computers** > **OK**.
5. Type the name of computer you wish to install Windows login protection on to the **Enter the object names to select** field > click **Check Names** to make sure the computer name is correct.
6. If the computer name is correct click **OK**, click **OK** again.

Obtaining the .msi installation file

If ESA [Authentication Server](#) is installed using the .exe installer, then .msi installers are automatically created in "C:\Program Files\ESET Secure Authentication\msi\".

Alternatively, obtain the installer following the steps below:

1. Download the .exe installer for ESA from <https://www.eset.com/us/products/secure-authentication/>
2. Extract the .msi installation file (named ESET Secure Authentication x64.msi or ESET Secure Authentication x86.msi) from the downloaded .exe file
3. Upload the obtained .msi installation file to a shared folder of your server (main computer) that is accessible from members of your [AD](#) domain.

Proceed with one of the deployment options below:

- [Startup script](#)
- [Software Installation task](#)

The MSI installer is also available in the [ESET Remote Administrator](#) repository.

3.7.1 Startup script

Prepare a startup script (.bat file) with the essential parameters

1. Press the **windows key + R** key, type **notepad.exe** into the **Run** dialog box and then press **Enter**.
2. When notepad opens, enter the following code:

```
msiexec /i "<path_to_msi_file>" NO_DOMAIN_ADMIN_MODE=1  
ADDLOCAL="Credential_Provider,Win_Credential_Provider" /qn /L*v "c:  
\esa_install_log.txt"
```

where the `<path_to_msi_file>` must be replaced with a valid Universal Naming Convention (UNC) path (network path) to the shared installer package (for example, `\\fileserver\share\filename.msi`). The code must be entered in a single line.

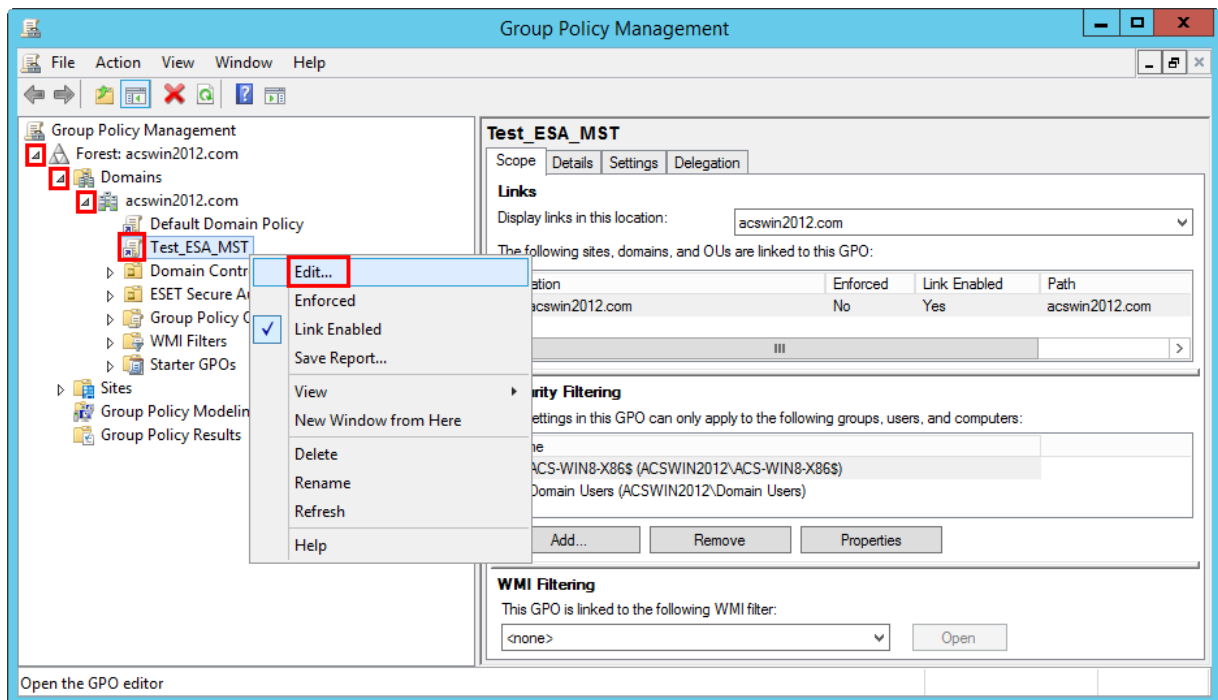


`Credential_Provider` stands for RDP login protection, `Win_Credential_Provider` stands for Windows Login protection. See [MSI arguments](#) for more information.

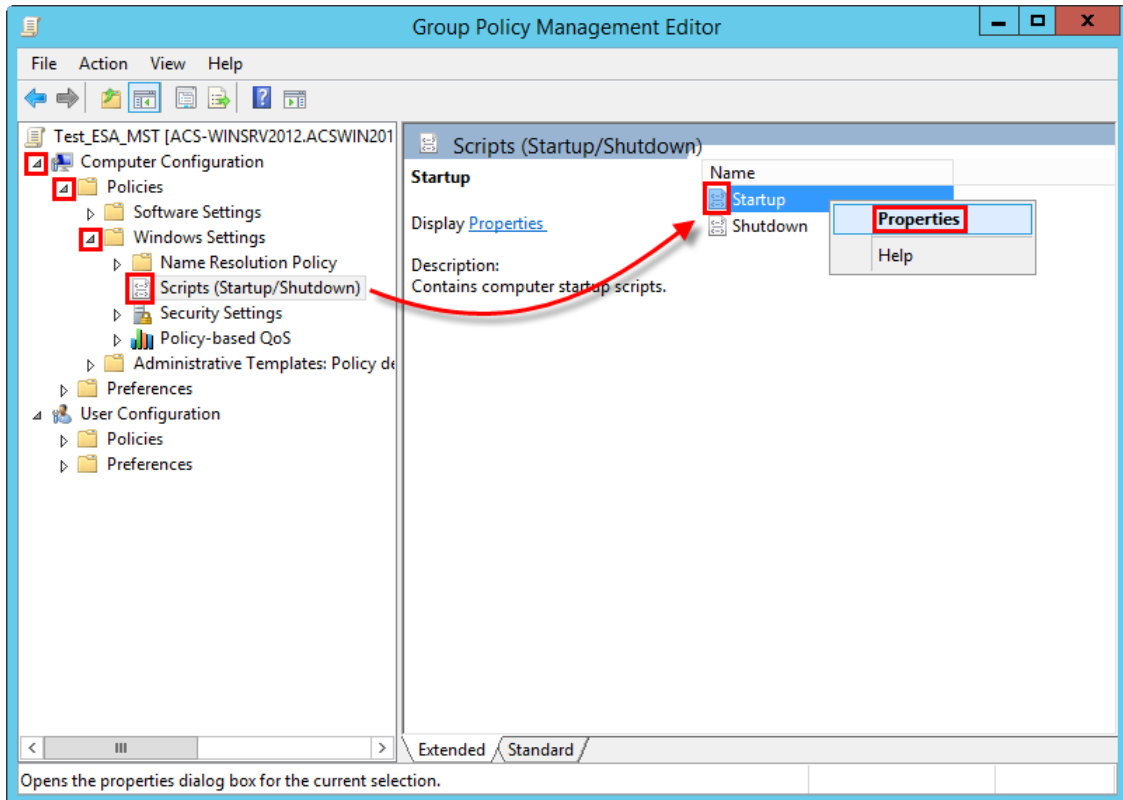
3. In Notepad, click **File > Save As**, select **All Files** from the **Save as type** drop-down menu and enter: **esainstall.bat** as the file name.

Deployment of startup script

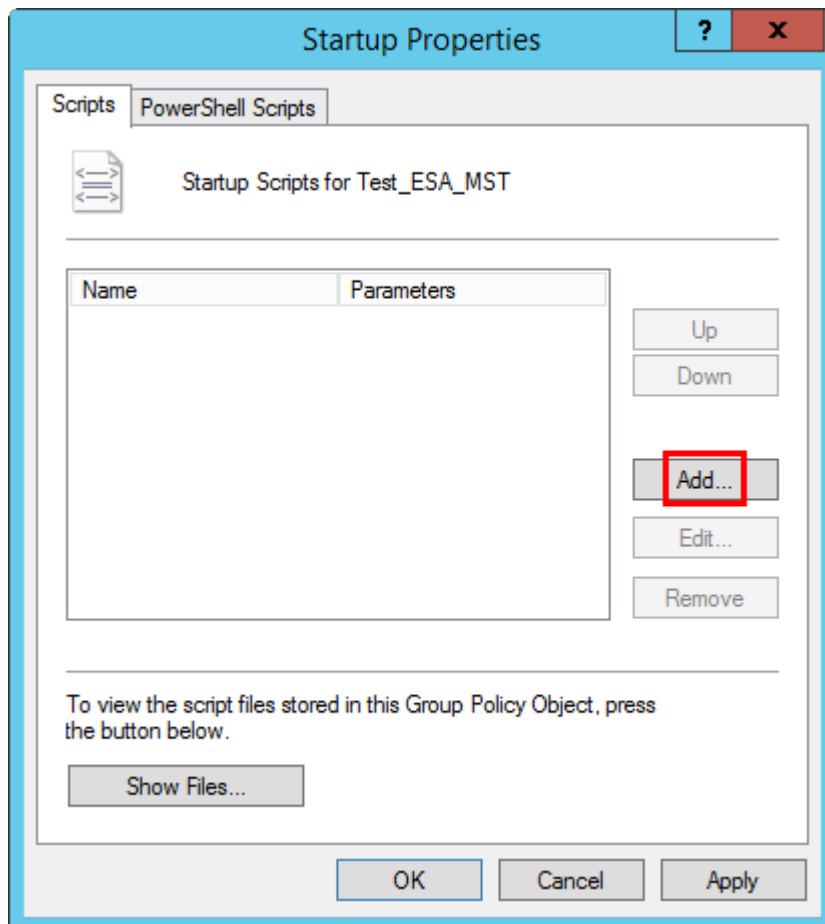
1. Open **Group Policy Management**, locate your domain, right-click the desired group policy and then select **Edit**.



In **Group Policy Management Editor**, under your domain policy expand **Computer Configuration > Policies > Windows Settings**, right-click **Startup** and select **Properties**.



Click **Add...** > **Browse...** and browse for the **esainstall.bat** file uploaded to the shared folder of your AD domain, click **Open** and then click **OK**.



2. Click **OK** to apply the changes and close the **Startup Properties** window.

3.7.2 Software Installation task

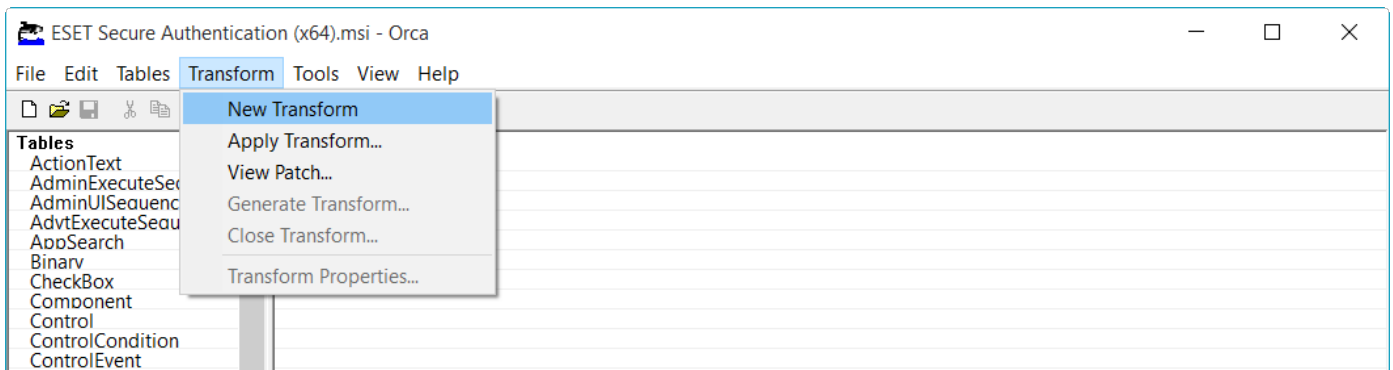
Prior to creating a **Software Installation** task via **GPO**, it is essential to create an **.mst** transform file.

Prerequisite

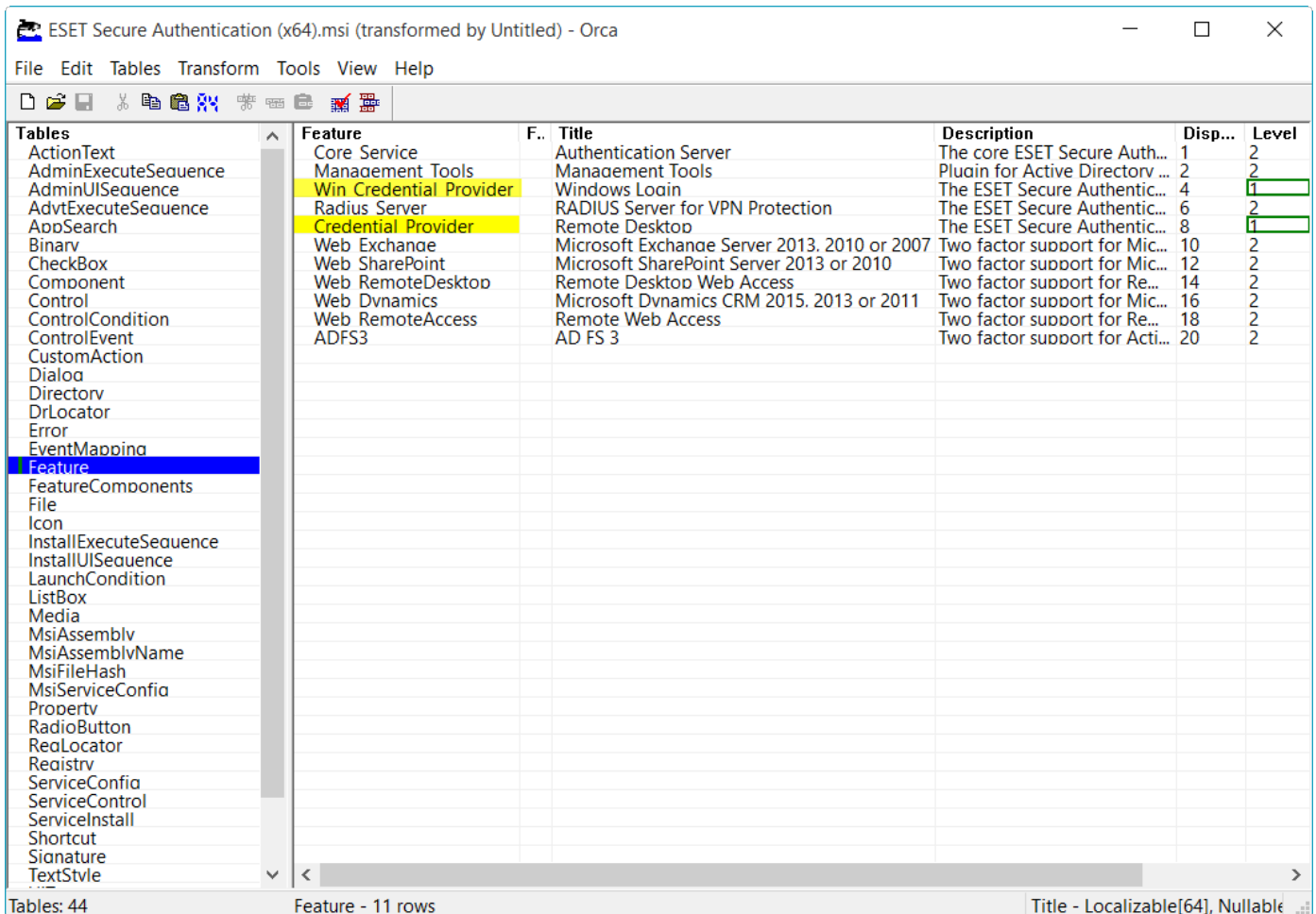
- The Orca database editor tool must be installed on your computer. Orca is available as part of the Windows SDK. For instructions to download and install Orca, visit the following Microsoft Knowledge Base article: [How to use the Orca database editor to edit Windows Installer files.](#)

Creating an .mst transform file

1. Click **Start > All Programs > Orca** to launch Orca database editor.
2. Click **File > Open**, navigate to the **.msi** installer file that you want to apply the transformation file to, select it and then click **Open**.
3. Click **Transform > New Transform**.



Select **Features** in the **Tables** column, select **Windows Login** and change the **Level** to **1**. Then select **Remote Desktop** and change the **Level** to **1**.





All changes are marked in green.

5. Select **Property** in the **Tables** column, right-click an empty row and select **Add row**.

Tables	Property	Value
ActionText	UpgradeCode	{2A8BE5D-30F6-4290-AC2B-A1FBEA28EF09}
AdminExecuteSequence	WixUIRMOption	UseRM
AdminUISequence	ALLUSERS	1
AdvExecuteSequence	WixAppFolder	WixPerMachineFolder
AppSearch	CORE SERVICE DOMAIN	Nothing
Binary	CORE SERVICE USERNAME	EIPsrv COMPUTERTNAME
CheckBox	CORE SERVICE PASSWORD	Nothing
Component	DOMAIN DN	Nothing
Control	SCHEMA MASTER	Nothing
ControlCondition	MsiLoaaina	v!
ControlEvent	Manufacturer	ESET. spol. s r.o.
CustomAction	ProductCode	{C7879B68-4D86-47D2-BE56-15E5460678C3}
Dialog	ProductLanguage	1033
Directory	ProductName	ESET Secure Authentication 2.5.22.0 (x64)
DrLocator	ProductVersion	2.5.22.0
Error	DefaultUIFont	WixUI Font Normal
EventMapping	WixUI Mode	FeatureTree
Feature	ErrorDialog	ErrorDia
FeatureComponents	ARPPRODUCTICON	Product.ico
File	SecureCustomProperties	CORE SERVICE DOMAIN:CORE SERVICE PASSWORD:CORE SERVICE USERNAME:DOMAIN...
Icon	MsiHiddenProperties	CORE SERVICE PASSWORD
InstallExecuteSequence		
InstallUISequence		
LaunchCondition		
ListBox		
Media		
MsiAssembly		
MsiAssemblyName		
MsiFileHash		
MsiServiceConfig		
Property		
RadioButton		
RealLocator		
Registry		
ServiceConfig		
ServiceControl		
ServiceInstall		
Shortcut		
Signature		
TextStyle		

Tables: 44 Property - 21 View in Decimal No column is selected.

In the **Add Row** dialog window type **NO_DOMAIN_ADMIN_MODE** into the **Property** field, set the **Value** field to **1** and click **OK**.

Add Row [X]

Name	Value
Property	NO_DOMAIN_ADMIN_MODE
Value	1

Column
Value - Localizable String[0], Required

OK Cancel

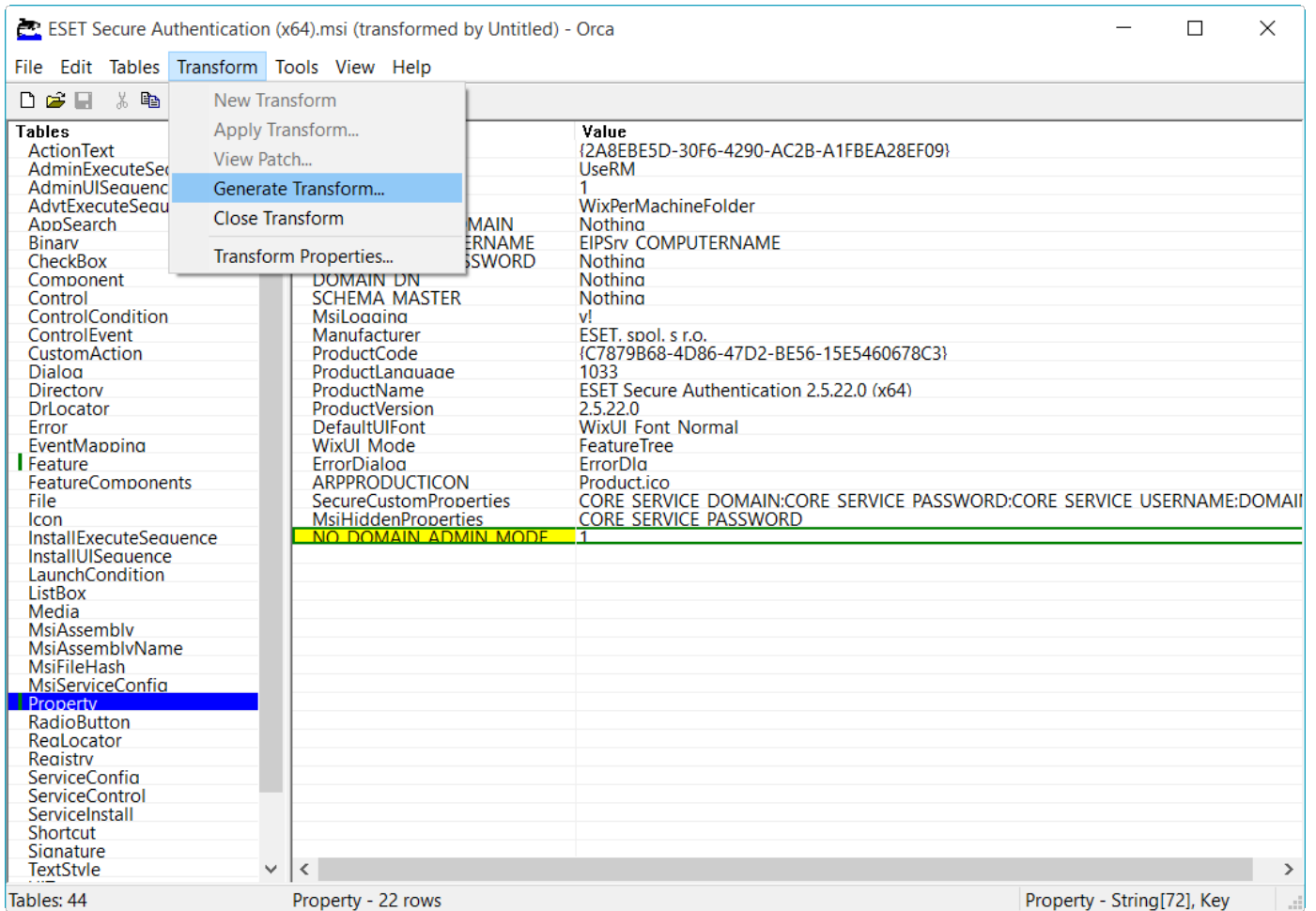
ESET Secure Authentication (x64).msi (transformed by Untitled) - Orca

File Edit Tables Transform Tools View Help

Tables	Property	Value
ActionText	UpgradeCode	{2A8EBE5D-30F6-4290-AC2B-A1FBEA28EF09}
AdminExecuteSequence	WixUIRMOption	UseRM
AdminUISequence	ALLUSERS	1
AdvtExecuteSequence	WixAppFolder	WixPerMachineFolder
AppSearch	CORE SERVICE DOMAIN	Nothing
Binary	CORE SERVICE USERNAME	EIPsvy COMPUTERNAME
CheckBox	CORE SERVICE PASSWORD	Nothing
Component	DOMAIN DN	Nothing
Control	SCHEMA MASTER	Nothing
ControlCondition	MsiLocaina	v!
ControlEvent	Manufacturer	ESET, spol. s r.o.
CustomAction	ProductCode	{C7879B68-4D86-47D2-BE56-15E5460678C3}
Dialog	ProductLanguage	1033
Directory	ProductName	ESET Secure Authentication 2.5.22.0 (x64)
DrLocator	ProductVersion	2.5.22.0
Error	DefaultUIFont	WixUI_Font_Normal
EventMapping	WixUI_Mode	FeatureTree
Feature	ErrorDialog	ErrorDia
FeatureComponents	ARPPRODUCTICON	Product.ico
File	SecureCustomProperties	CORE SERVICE DOMAIN:CORE SERVICE PASSWORD:CORE SERVICE USERNAME:DOMAIN
Icon	MsiHiddenProperties	CORE SERVICE PASSWORD
InstallExecuteSequence	NO_DOMAIN_ADMIN_MODE	1
InstallUISequence		
LaunchCondition		
ListBox		
Media		
MsiAssemblies		
MsiAssemblyName		
MsiFileHash		
MsiServiceConfig		
Property		
RadioButton		
ReaLocator		
Registry		
ServiceConfig		
ServiceControl		
ServiceInstall		
Shortcut		
Signature		
TextStyle		

Tables: 44 Property - 22 rows Property - String[72], Key

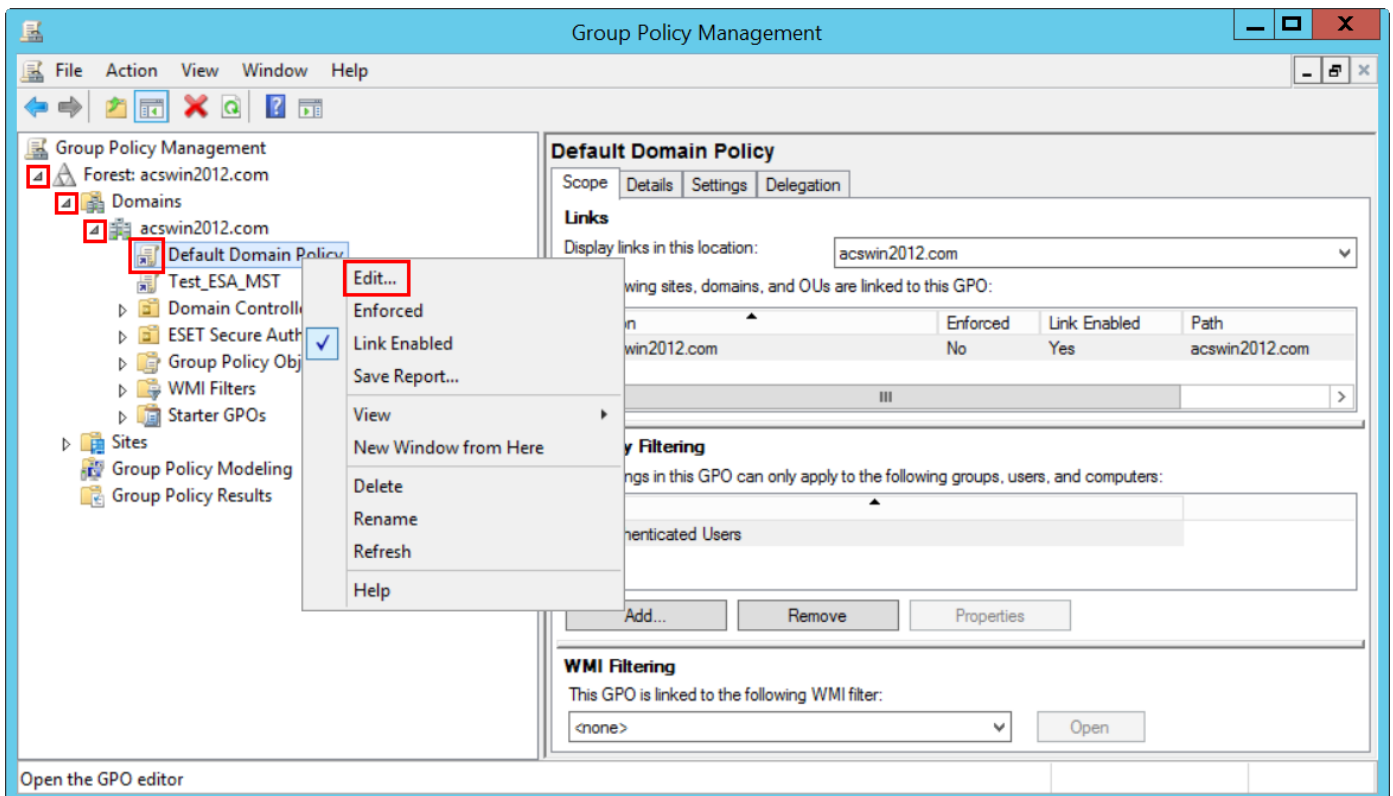
Click **Transform > Generate Transform...**



Create a Software Installation task via GPO

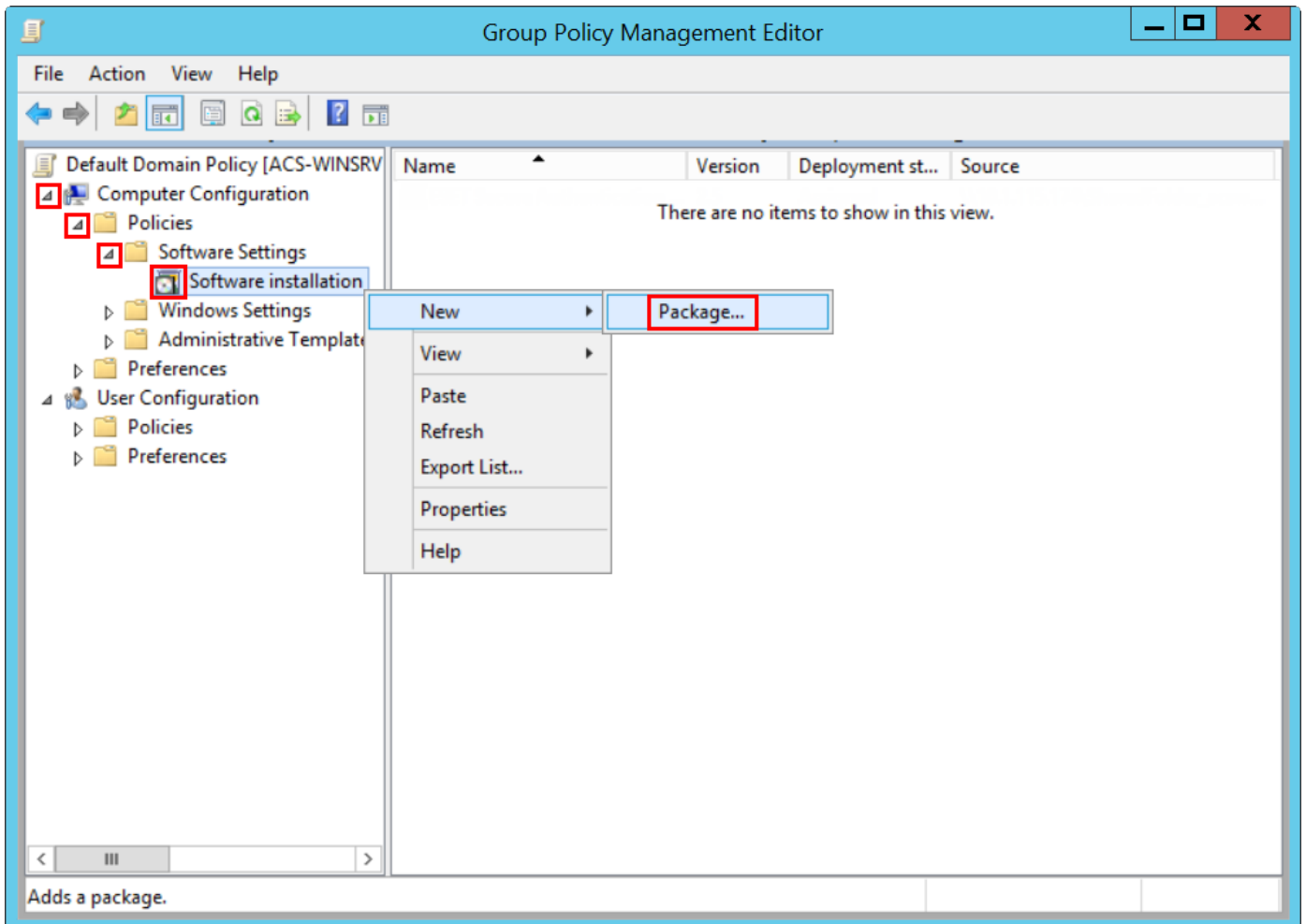
The steps below are demonstrated in Microsoft Server 2012 R2.

1. Open **Group Policy Management** > locate your domain > right-click **Default Domain Policy** or a custom policy you created and then select **Edit**.

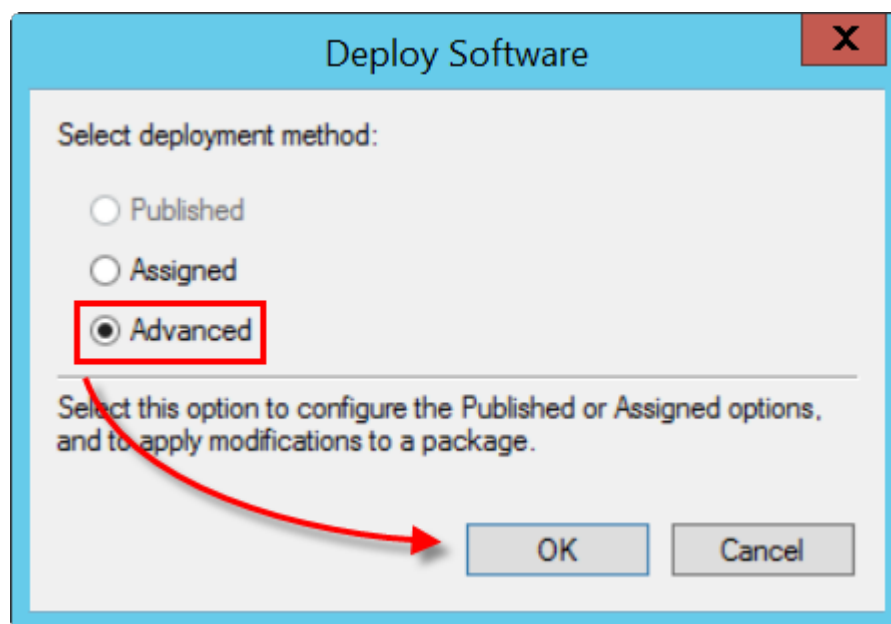


In **Group Policy Management Editor**, under your domain policy expand **Computer Configuration > Policies > Software Settings**.

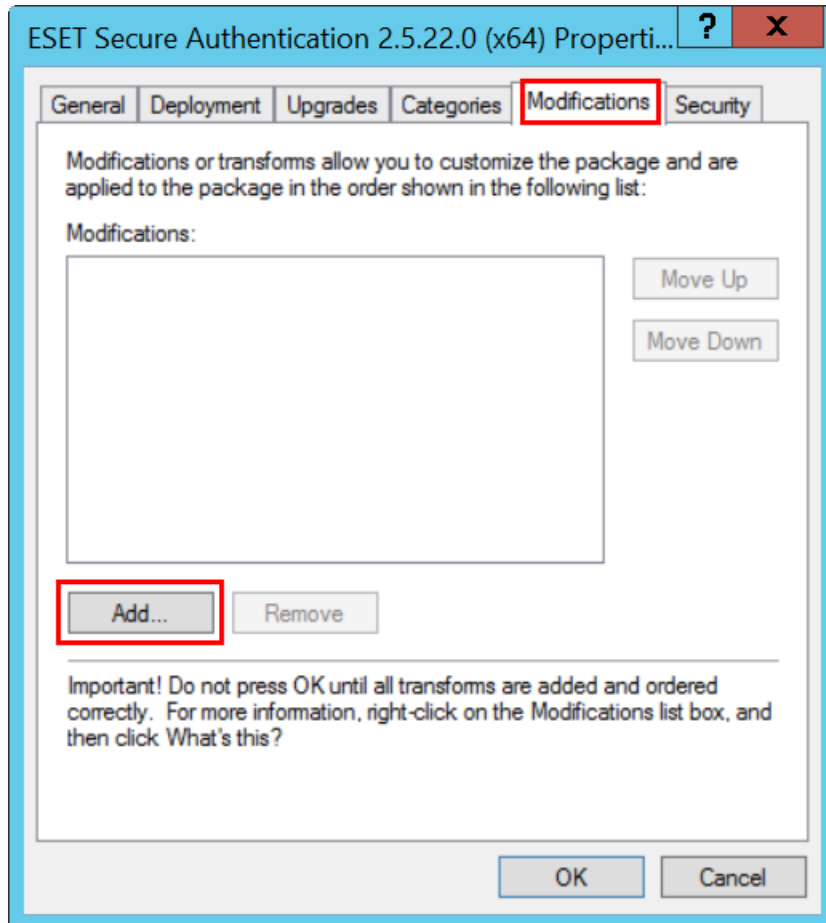
3. Right-click **Software installation**, select **New > Package** and navigate to the location where the ESA installer *.msi* is saved. Type the full Universal Naming Convention (UNC) path of the shared installer package (for example, \\fileserver\share\filename.msi), and click **Open**.



Select **Advanced** and click **OK**.

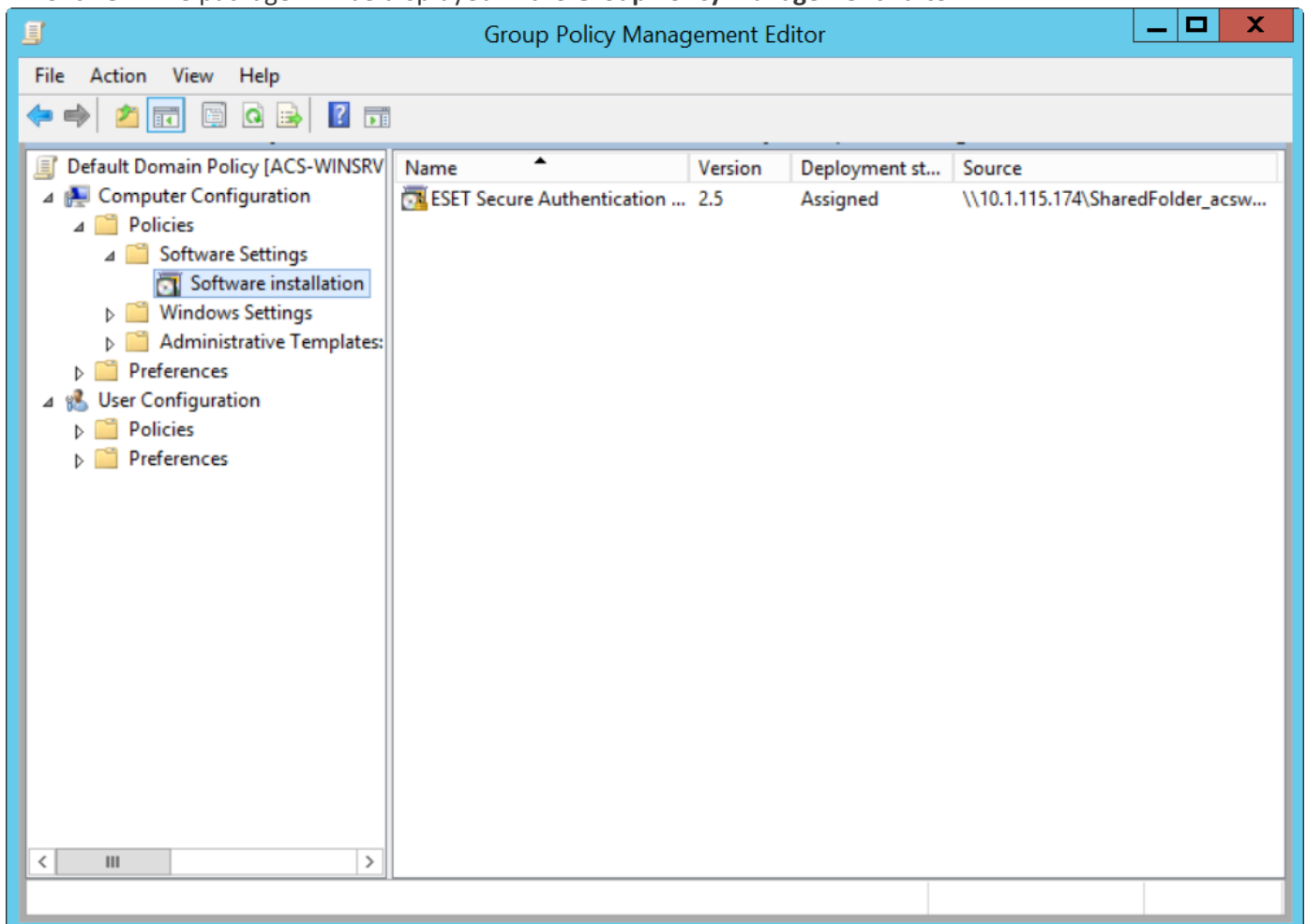


5. Select the **Modifications** tab and click **Add...**



Navigate to the ESA installer transform file (in the same location you referenced in step 3), enter the UNC path of the *.mst* file (for example, \\fileserver\share\filename.mst) and click **Open**.

7. Click **OK**. The package will be displayed in the **Group Policy Management Editor**.



The package will be installed to all client computers the edited group policy applies to.

[See Microsoft Knowledgebase how to use Group Policy to install software remotely in Windows Server 2003 and 2008.](#)

3.7.3 MSI arguments

When using the *.msi installer* either as a [Logon script](#) or [Installation task](#), several arguments can be used.

- To specify components to be installed, the ADDLOCAL argument is used. Possible values include the following:
Credential_Provider = Remote Desktop protection component
Win_Credential_Provider = Windows Login protection component
Radius_Server
Web_Exchange, Web_SharePoint, Web_RemoteDesktop, Web_Dynamics, Web_RemoteAccess
Management_Tools = Management console
ADFS3
Core_Service = Authentication server
Reports_Elasticsearch = Reporting engine (Elasticsearch)
- To set initial username and password for ESA Web Console:
ESA_CONFIG_WEB_CONSOLE_USER, ESA_CONFIG_WEB_CONSOLE_PASSWORD
- To set a custom RADIUS port or set the details of proxy server to be used, the following arguments are available. Set the corresponding values.
ESA_CONFIG_RADIUS_PORT
ESA_CONFIG_PROXY_SERVER, ESA_CONFIG_PROXY_PORT, ESA_CONFIG_PROXY_USER,
ESA_CONFIG_PROXY_PASSWORD
- To set a custom domain port (Active Directory Integration deployment type only) or a custom API port, the following arguments are available. Set the corresponding values:
ESA_CONFIG_CORE_PORT_DOMAIN
ESA_CONFIG_CORE_PORT_API
- To specify deployment type, the ESA_COMPUTER_CONFIG_INTEGRATION_MODE argument is used. Possible values include the following:
1 = Active Directory Integration (default value)
2 = Standalone

If value number **2** is used, the following arguments must be configured also, unless installing [ESA components](#) on the same machine where the Authentication Server is installed:

ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ADDRESS - IP address of Authentication Server to be used in [invitations](#).

ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ACCESS - [invitation](#) code.

TRUSTED_CERT_HASH - hash of trusted Certificate to be added to certificate store.

- Useful MSIEXEC arguments:
/L*v "c:\esa_install_log.txt" - to create an installation log file named *esa_install_log.txt* in the C directory
/qn - silent installation mode, meaning, the installation is accomplished in the background without the interaction of being logged in user.
- To install or remove ESA components without a Domain Admin user, use NO_DOMAIN_ADMIN_MODE=1.
- For complete removal of [ESA Authentication Server](#), including configuration data stored in Active Directory, use AUTHENTICATION_SERVER_CLEAN_DATA=1.

3.8 Upgrade installation

In ESET Secure Authentication version 2.5.X and later, you can upgrade ESA by launching the installer. There is no need to manually uninstall the previous version.

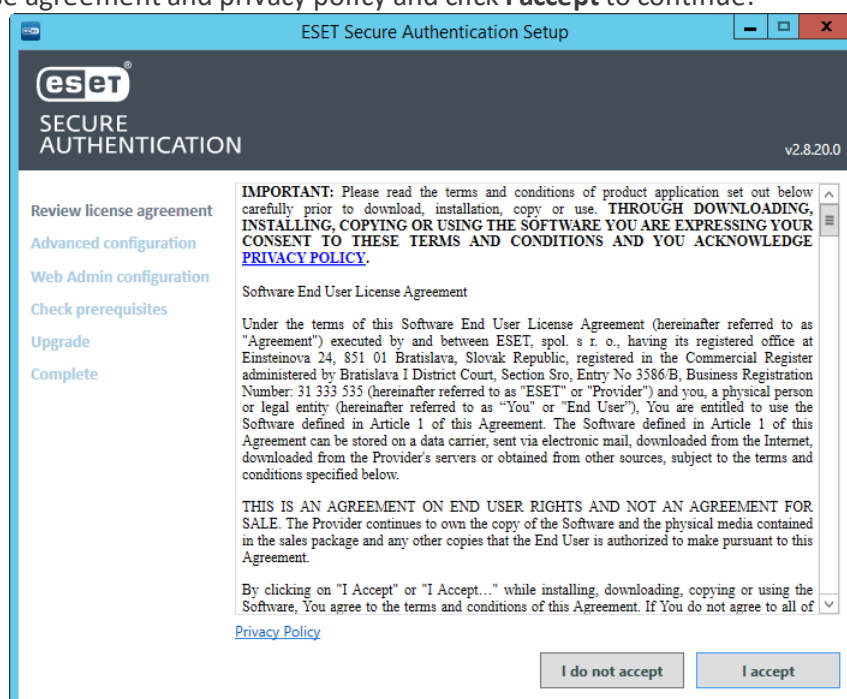


Upgrade Order

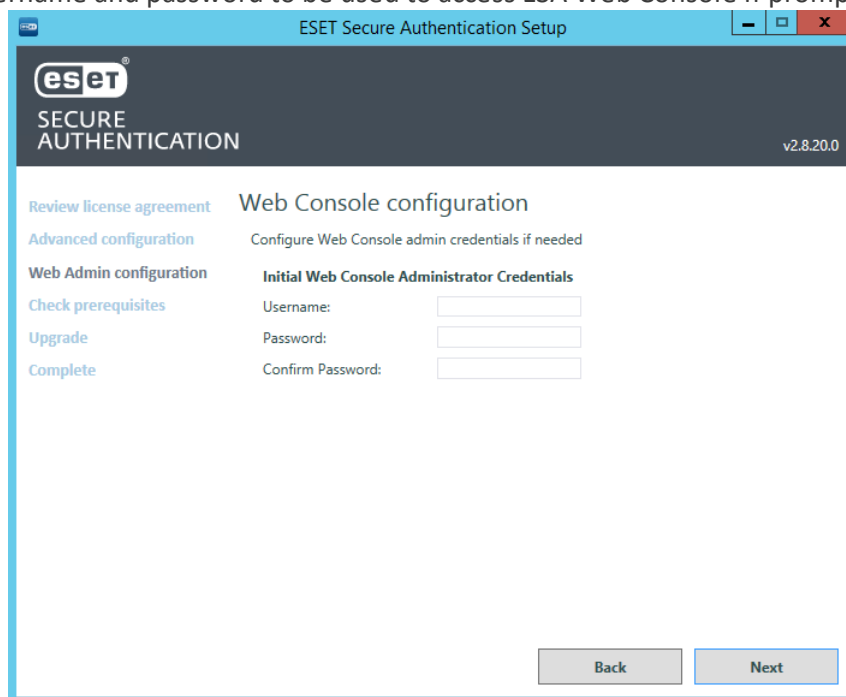
You must upgrade the Authentication Server first and then upgrade other components on computers secured by ESA to maintain [compatibility](#).

If you have multiple Authentication Servers (possible only in Active Directory environment), upgrade all of them. When upgrading one of them, the other ones must be stopped in order to maintain data compatibility.

1. Review the license agreement and privacy policy and click **I accept** to continue.



Enter the desired username and password to be used to access ESA Web Console if prompted.



When all prerequisites are satisfied, click **Next**.

4. Follow the instructions in the installer to complete the upgrade. Close the installer when you are finished.

When the upgrade is complete, a shortcut labeled as ESA Web Console will be automatically created on the desktop of your Windows OS. Double-click the shortcut to open the Web Console.



ESA Web Console certificate

ESA Web Console uses a self-signed certificate. If you access the Web Console from a different machine than the machine hosting the Authentication Server, you will receive a certificate issue message.

Accessing the Web Console via Mozilla Firefox from the machine hosting the Authentication Server will also result in a certificate issue message.

Enter the login credentials you configured during the upgrade in the Web Console. If you upgraded from version 2.7 where ESA Web Console was already in use, the login credentials will be the same as they were.

In the **Dashboard**, the **Components** tile shows the number of outdated components. Outdated components include components on computers using an earlier version than the installed version of Authentication Server. Click the number in the **Out of date** column to see the affected computers. Use the installer of the same version as your Authentication Server to upgrade the ESA Components ([Windows Login](#), [Remote Desktop Protection](#), [IIS](#), [ADFS](#), [RADIUS](#)) on the affected computers.

3.8.1 Compatibility

Version compatibility between ESA Core (Authentication Server) and the other components ([Windows Login](#), [Remote Desktop Protection](#), [IIS](#), [ADFS](#), [RADIUS](#), [ADUC](#)) of ESET Secure Authentication has been improved. The tables below show which versions of ESA core, ESA Component and Management Console (MMC) are cross-compatible.

Compatibility table - component connecting to Authentication Server 2.8

Component	Component v2.4	Component v2.5	Component v2.6	Component v2.7	Component v2.8
Windows Login	OK*	OK*	OK	OK	OK
RDP	OK*	OK*	OK	OK	OK

Component	Component v2.4	Component v2.5	Component v2.6	Component v2.7	Component v2.8
AD FS	OK*	OK*	OK	OK	OK
IIS	FAIL	FAIL	OK	OK	OK
Management Tools (ADUC , MMC)	FAIL	FAIL	FAIL	FAIL	OK

* Works if the component was registered (used) with the corresponding version of Authentication Server (2.4 or 2.5) prior to upgrading Authentication Server to version 2.8.



You cannot register older component versions with a newer server version. The connection will fail due to compatibility issues and you will receive a notification of the error.

[IIS](#) component v2.6 or higher is essential to communicate with the latest ESA core.

4. Using reverse proxy

When using ESET Secure Authentication behind a reverse proxy server, consider the information below:

- In [invitation](#) details:
 - Use the IP address of the proxy server instead of the name of Authentication Server
 - Use the certificate hash of the proxy server certificate
- If Authentication Server is installed in Active Directory Integration mode:
 - ESA components (for example, [Windows Login](#), [Remote Desktop Protection](#), [RADIUS](#)) have to be installed in Standalone mode
 - In invitation use the IP address of the proxy server instead of the name of Authentication Server
 - Cannot log in to the ESA Web Console using domain authentication

If you want to use a proxy server for port forwarding only, you still have to regenerate a server certificate with the new *IP_address:port* as the alternative name.

4.1 Configure proxy for ESA

The example below refers to using Nginx as a reverse proxy server for ESET Secure Authentication.

Configure Nginx reverse proxy following the [Nginx guide](#), while applying the following settings:

- a. Set the listening port to 443.
- b. Define the SLL certificate you generated. Example of generating an OpenSSL certificate.

Make sure OpenSSL for Windows is installed. Generate an OpenSSL certificate using Windows command line.

```
openssl req -config sampleSSL.conf -new -x509 -sha256 -newkey rsa:2048 -1
```

To avoid "Invalid certificate" warning, the *sampleSSL.conf* file has to include the list of alternative DNS names by which the authentication server will be available. The command above will generate *newKey.rsa* and *newCertificate.crt* files.

Sample content of sampleSSL.conf file:

```
[ req ]
default_bits          = 4096
distinguished_name    = req_distinguished_name
req_extensions        = req_ext

[ req_distinguished_name ]
countryName           = Country Name (2 letter code)
countryName_default   = SK
stateOrProvinceName  = State or Province Name (full name)
stateOrProvinceName_default = Slovakia
localityName          = Locality Name (eg, city)
localityName_default  = Bratislava
organizationName      = Organization Name (eg, company)
organizationName_default = My company running ESA
```

```

commonName          = Common Name (e.g. server FQDN)
commonName_default  = localhost

[ req_ext ]
subjectAltName = @alternative_names

[alternative_names]
DNS.1    = my.esa.installation.com
DNS.2    = my.authentication.server
DNS.3    = twofactor.auth

```

- c. Set `proxy_pass` to use the IP address of the Authentication Server, for instance: <https://10.0.0.2:8001>.



Authentication Server and Nginx on a different Windows server machine

If Nginx is on a different Windows Server machine than the Authentication Server, import the certificate of ESET Secure Authentication to the certificate store of Nginx machine, specifically to **Certificates (Local Computer) > Trusted People**.

If you receive a certificate issue message when trying to access ESA Web Console from a computer, add an exception.

Add Certificate exception

- Mozilla Firefox
 1. Click **Advanced** and click **Add Exception...**
 2. In the **Add Security Exception** window make sure the **Permanently store this exception** is selected.
 3. click **Confirm Security Exception**.
- Google Chrome
 1. Click **Advanced**.
 2. Click **Proceed to <web address of ESA Web Console> (unsafe)**.
 3. At this point, Google Chrome remembers the exception.
- Internet Explorer 11
 1. Click **Continue to this website (not recommended)**.
 2. In the right section of address bar click **Certificate error**, click **View certificates**, and then click **Install Certificate...**
 3. In Certificate Import Wizard window select **Local Machine** for Store Location, click **Next**.
 4. In the next screen select "*Place all certificates in the following store*", and click **Browse**.
 5. Select **Show physical stores** checkbox, select Trusted Root Certification Authorities, and then click **OK**.
 6. Click **Next** and click **Finish**.
 7. Restart the computer.
- Microsoft Edge
 1. Try to access the Web Console in Internet Explorer 11 first, and then carry out the steps on adding certificate exception as described for Internet Explorer 11.

5. Getting started with ESET Secure Authentication Web Console

Once all required ESA components have been installed, some basic configuration is necessary via the ESA Web Console.

On your desktop, double-click the ESA Web Console shortcut.

ESA Web Console certificate

ESA Web Console uses a self-signed certificate. If you access the Web Console from a different machine than the machine hosting the Authentication Server, you will receive a certificate issue message.

Accessing the Web Console via Mozilla Firefox from the machine hosting the Authentication Server will also result in a certificate issue message.

To avoid a certificate issue message, add an exception.

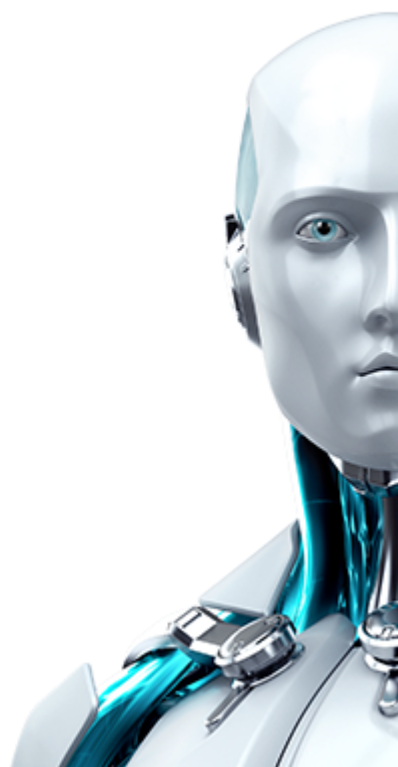
Add Certificate exception

- Mozilla Firefox
 1. Click **Advanced** and click **Add Exception...**
 2. In the **Add Security Exception** window make sure the **Permanently store this exception** is selected.
 3. click **Confirm Security Exception**.
- Google Chrome
 1. Click **Advanced**.
 2. Click **Proceed to <web address of ESA Web Console> (unsafe)**.
 3. At this point, Google Chrome remembers the exception.
- Internet Explorer 11
 1. Click **Continue to this website (not recommended)**.
 2. In the right section of address bar click **Certificate error**, click **View certificates**, and then click **Install Certificate...**
 3. In Certificate Import Wizard window select **Local Machine** for Store Location, click **Next**.
 4. In the next screen select "*Place all certificates in the following store*", and click **Browse**.
 5. Select **Show physical stores** checkbox, select Trusted Root Certification Authorities, and then click **OK**.
 6. Click **Next** and click **Finish**.
 7. Restart the computer.
- Microsoft Edge
 1. Try to access the Web Console in Internet Explorer 11 first, and then carry out the steps on adding certificate exception as described for Internet Explorer 11.

Log in to ESA Web Console

Log in using the access credentials you created for ESA Web Console during the Authentication Server install. In an Active Directory (AD) environment, if Active Directory Integration type of deployment has been used, log in clicking **Use domain authentication** in [supported browsers](#).

Log in



[Activate your installation of ESET Secure Authentication.](#)

To configure 2FA for a [supported Web Application](#), refer to the [Web Application Protection](#) section. For configuring 2FA on your VPN, refer to the [VPN Protection](#) section. To configure 2FA for Remote Desktop, refer to the [Remote Desktop Protection](#) section.

Provide feedback on ESET Secure Authentication via the **Submit feedback** section in ESA Web Console. That section appears only if your installation of ESET Secure Authentication has been activated.



You can provide feedback on ESET Secure Authentication via the **Submit feedback** section in ESA Web Console. That section appears only if your installation of ESET Secure Authentication has been activated.

Enable or disable 2FA for the ESA Web Console

To enable or disable 2FA for the ESA Web Console, navigate to **Components > ESA Web Console**, and switch the **Enable 2FA for Web Console** toggle. If a Domain Admin user has 2FA enabled (by default it is), access to the Active Directory Users and Computers > ESET Secure Authentication screen and ESA Management Console is removed. To enable the access to those screens, disable 2FA for the ESA Web Console.

5.1 Activate ESET Secure Authentication

Activate your ESA system using an ESA license, [ESET Business Account](#) (EBA) or [ESET MSP Administrator](#) (EMA) login credentials.

You can obtain a license from your ESET distributor or you can use the demo license (in *License.txt*) that was shipped with the installer.

To activate your ESA Server:

1. Launch the ESA Web Console.
2. Click **Settings > License** and select the appropriate activation method:
 - **ESET Business Account:** For registered [ESET Business Account \(EBA\)](#) users who have an ESET Secure Authentication [license imported to EBA](#). Your EBA username and password are required.
 - **Enter a License Key:** For users who purchased an ESET Secure Authentication License Key.
 - **Offline License:** Use this option if the ESA Authentication Server cannot connect to the internet.
3. Once your license is active, configure your token name (the name that will be displayed in the Mobile Application on user's phones) under **Settings > Mobile application > Account name**.

Using EBA or EMA login credentials to activate ESA

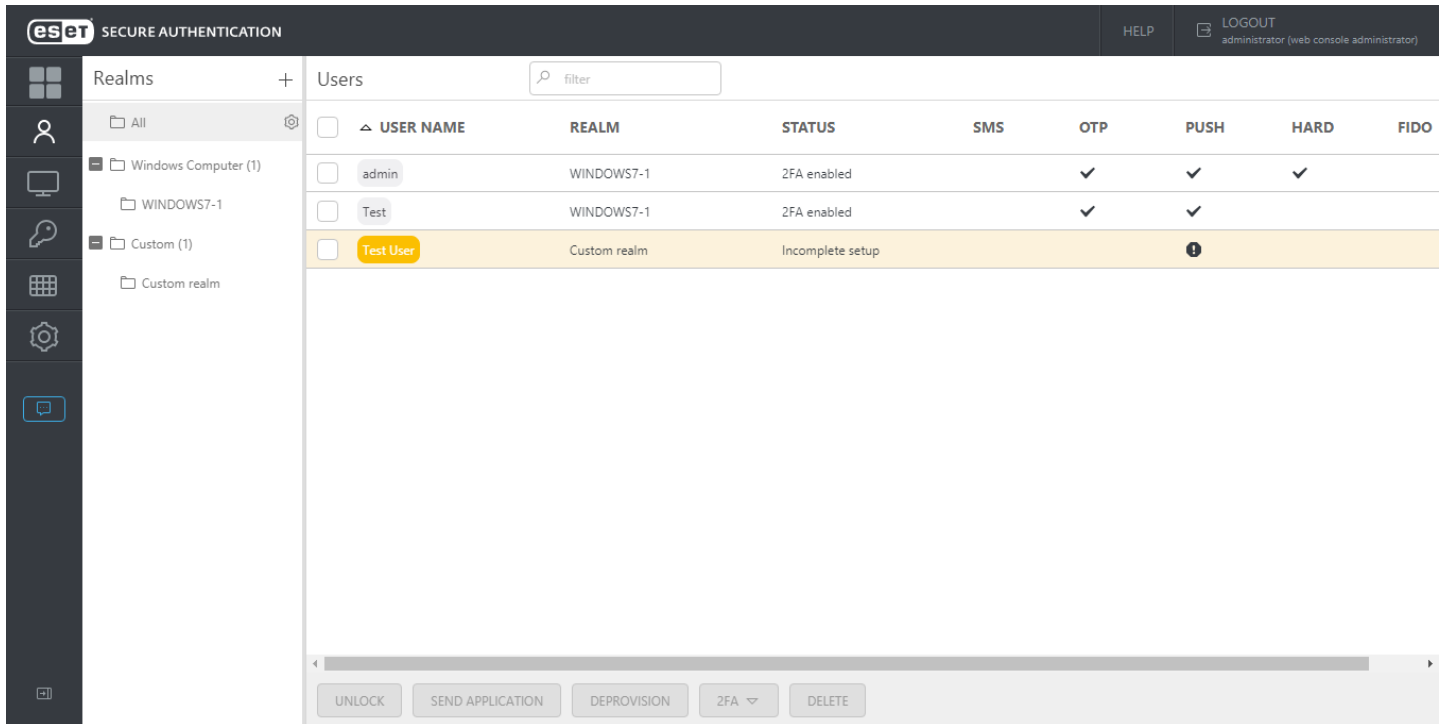
1. In the ESA Web Console, click **Settings > License**.
2. Select **ESET Business Account**.
3. Enter your EBA or EMA login credentials.
4. If there is only a single ESA license in your EBA or EMA account and no [sites](#) are created, the activation will complete instantly. Otherwise, you have to select a particular license or a site (license pool) to active ESA.
5. Click **Activate**.

5.2 User Management - Provisioning

All user management takes place in the **Users** section of the Web Console. All ESA users must have valid mobile phone numbers, unless the user will authenticate using a [Hard Token](#) or [FIDO](#) authenticator. The phone number for each user is either entered manually when creating/editing the user in the Web Console, or imported along with the user information if [synchronizing with LDAP](#), or entered by the user if [self-enrollment](#) is enabled.

Each user belongs to a realm (domain, computer name, etc.). Realms and users are created automatically when a user logs on a machine with an [ESA component](#) installed, logs in to a service protected by ESA, or if ESA is synchronized with LDAP. You can also create custom realms manually.

The image below shows a custom realm and an automatic realm. The custom realm was created manually (Custom Realm) and Test User user was added to it. The automatic realm, and its 2 users were created automatically (admin,Test). The realm name was taken from the computer where the Windows Login plug-in of ESA is installed and the 2 users are logged on. The [status](#) column indicates if the user has 2FA enabled (and used 2FA at least once) or not.



Create a custom realm manually

1. Click the **+** icon next to **Realms** and click **Create custom Realm**.
2. Enter desired string for both **Realm ID** and **Realm Name**, select **Category** and click **Save**.

Add user to a realm manually

1. Select the realm where you want to add the user.
2. Click **Add user...**
3. Enter the name and phone number of the user.
4. Click **Create user**.



Phone number format

Mobile numbers must be in international format "+421987654321", where +421 is the country code. For example, a Slovak phone number 0987654321 would be entered as +421987654321 replacing the leading zero "0" with the country code "+421". A US phone number "201-321-4567" would be entered as "+12013214567", where "+1" is the country code.

You can also [import users to a custom realm from a file](#).

Send mobile application to users

1. Select the check box next to users who will receive the mobile application.
2. Click **Send application**.
3. Close the confirmation window.

Enabling 2FA per user

Click a user and select the desired authentication options. OTP and Push authentication are the most convenient ones. If Hard Token OTPs have been enabled and imported, then Hard Tokens will be available in the drop-down menu under the **Hard Token** slider bar. Click **Save** to save the changes.

If an authentication method requires any information, a notification is displayed. You can still save the user's profile, and if [self-enrollment](#) is enabled, the user can fill in the missing information once they sign up for 2FA.

If Mobile Application OTP or Mobile Application Push has been turned on, a notification will display to remind you to send the enrollment/provisioning message to the user to activate the mobile application.

If you click **Do not send** or **Cancel**, you can use the **Actions** button to send the enrollment/provisioning message later. If you click **Send**, an information window will show you the unique application URL that has been sent to the user.

Enabling 2FA for multiple users at one time

1. Select the check box next to the users you are enabling 2FA for.
2. Click **2FA**, select **Enable** and select the desired authentication option.
3. Close the confirmation window.

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

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

[See a list of IP addresses and ports used for communication with ESET Secure Authentication Provisioning Server.](#)

If users change their phone number, the provisioning must be carried out again, however, the previous token(s) must be deleted from the mobile application. To delete a token, tap the tile to generate an OTP, when the OTP is visible, hold the tile and swipe left. Confirm the removal.

5.2.1 User Status

A user may be in various statuses during regular operation. Before enabling a user for 2FA, or uninitialized status, the **Status** column in the **Users** screen is empty.

- **Incomplete setup:** 2FA is enabled but either the mobile application has not yet been sent to the user, or it has not been used yet.
- **2FA enabled :** User has authenticated with 2FA to access a computer or service protected by ESA. This state also applies if only SMS-based OTPs and/or Hard Tokens are enabled for the user, though the user has not yet authenticated.

Additional information regarding **Incomplete setup** is available in user's profile next to each enabled 2FA method.

A user may then be enabled for either SMS-based OTPs, Mobile Application OTPs, Mobile Application Push or all. If they are enabled for all, they are in what is known as the transitioning state. This type of status is visible only in the users's profile.

The screenshot shows the user profile for 'admin (WINDOWS7-2)'. At the top, there is a navigation bar with 'eset SECURE AUTHENTICATION', 'HELP', and 'LOGOUT administrator (web console administrator)'. Below the navigation bar, there is a sidebar with icons for user management. The main content area is divided into two panels. The left panel has a warning icon and the text 'User setup is not complete.' Below this, there is a section for 'Authentication Events' with a table showing 'Last Successful Login', 'Last Failed Login', and 'Consecutive Failed Logins' with a value of '0'. The right panel is titled 'Mobile Number' and shows a mobile number field with 'Slovakia' as the country. Below this, there are several 2FA methods with their respective status and actions: 'SMS-based OTPs' (enabled, 'Transitioning to mobile app'), 'Mobile Application OTP' (enabled, 'Waiting to use app'), 'Mobile Application Push' (enabled, 'Waiting to use app'), 'Hard Token' (disabled), and 'FIDO' (disabled). At the bottom of the profile, there are 'ACTIONS' and 'DELETE USER' buttons.

In this state, a user will receive SMS-based OTPs when authentication attempts are initiated, but as soon as a valid mobile OTP is used for authentication or a Push notification (authentication request) is approved, SMS-based OTPs will be disabled, and the user will only be able to authenticate using mobile OTPs or Push notifications. When a user has successfully authenticated using a mobile app OTP, a green flag is displayed in user details.

When authenticating OTPs, a user can enter an incorrect OTP 10 times. On the 11th failed OTP, the user's 2FA will be locked. This is to prevent brute force guessing of OTPs. When a user's 2FA is locked, the name is highlighted in red in the **Users** screen, the status changes to 2FA locked, and a red triangle with an exclamation mark along with additional information is displayed in the profile:

The screenshot shows the user profile for 'Test (WINDOWS7-1)'. At the top, there is a navigation bar with 'eset SECURE AUTHENTICATION', 'HELP', and 'LOGOUT administrator (web console administrator)'. Below the navigation bar, there is a sidebar with icons for user management. The main content area is divided into two panels. The left panel has a warning icon and the text '2FA is locked out due to too many incorrect login attempts.' Below this, there is a section for 'Authentication Events' with a table showing 'Last Successful Login' (3/11/2019, 2:32:23 AM) and 'Last Failed Login' (3/11/2019, 2:33:18 AM) with a value of '11' consecutive failed logins. The right panel is titled 'Mobile Number' and shows a mobile number field with 'Slovakia' as the country. Below this, there are several 2FA methods with their respective status and actions: 'SMS-based OTPs' (disabled), 'Mobile Application OTP' (enabled, 'Time-based (TOTP)'), 'Mobile Application Push' (enabled), 'Hard Token' (disabled), and 'FIDO' (disabled). At the bottom of the profile, there are 'ACTIONS' and 'DELETE USER' buttons.

If it has been confirmed that the user's identity is not under attack, click **Actions**, then **Unlock** to unlock the user's 2FA.

If [Hard Token](#) OTPs have been enabled and imported, there are then more states in which the user may potentially find him or herself.

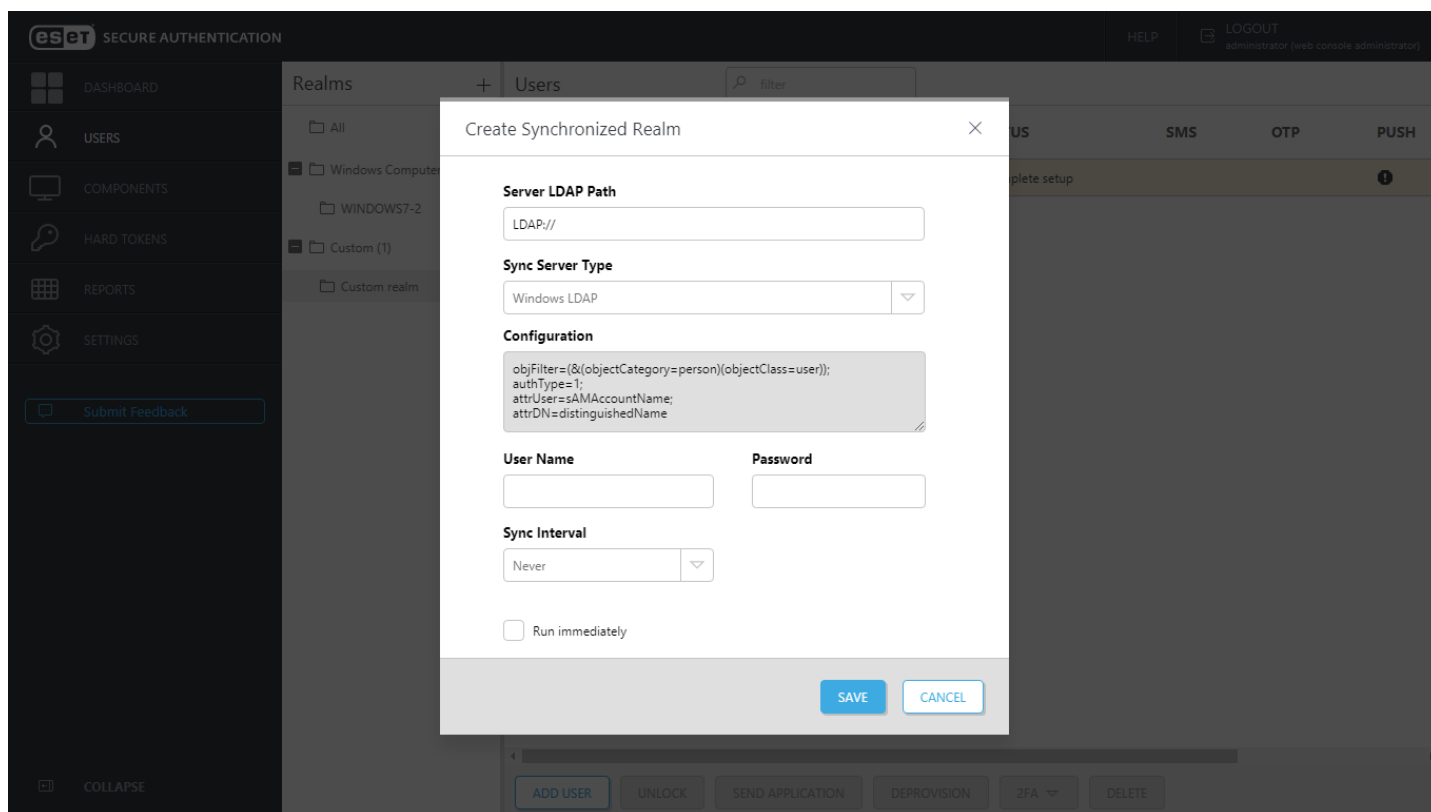
The user may be in a Hard Token OTP only state, or may be enabled for any combination of the three OTP types, or the user may be in a transitioning state where all three OTP types are enabled. In this state, a user will receive SMS OTPs when authentication attempts are initiated, but as soon as a valid 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.

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


5.2.2 Synchronizing with LDAP

ESET Secure Authentication supports synchronization with LDAP.

1. Access ESA Web Console and click **Users**.
2. Next to **Realms**, click **+**, select **Create Synchronized Realm**.
3. Enter the address of your LDAP server, select the applicable LDAP server type from the **Sync Server type** drop-down menu, and enter your LDAP username and password.
4. If this a one time import, leave the **Sync interval** intact. Otherwise, select the applicable synchronization interval.
5. Select the check box next to **Run immediately** and click **Save**.



Once your ESA instance is synchronized with LDAP, to synchronize it again manually:

1. In the **Realms** section, select the saved and synchronized LDAP server.
2. Click the gear icon  and then click **Synchronize Now**.

Supported configuration parameters


- `objFilter` - Required; used as a filter for selecting the user object in LDAP.
- `AttrName` - Optional; name of LDAP user property storing the user name. If **Windows LDAP** is selected for **Sync Server Type**, the username is read from "`sAMAccountName`" property. Otherwise, the username is read from "`cn`" property.
- `AttrPhone` - Optional; name of LDAP user property holding the phone number. If the `AttrPhone` parameter is not used, the mobile number is taken from the user field that is set as default in ESA Web Console > **Settings** > **Mobile Number Field**.
- `AuthType` - Optional; defines the type of authentication used when connecting to LDAP server. Default value for the Windows platform is 1 (Secure), for the other platform 0 (None). Available values:
 - 0 (None)
 - 1 (Secure)
 - 2 (Encryption/SecureSocketsLayer)
 - 4 (ReadOnlyServer)
 - 16 (Anonymous)
 - 32 (FastBind)
 - 64 (Signing)
 - 128 (Sealing)
 - 256 (Delegation)
 - 512 (ServerBind)

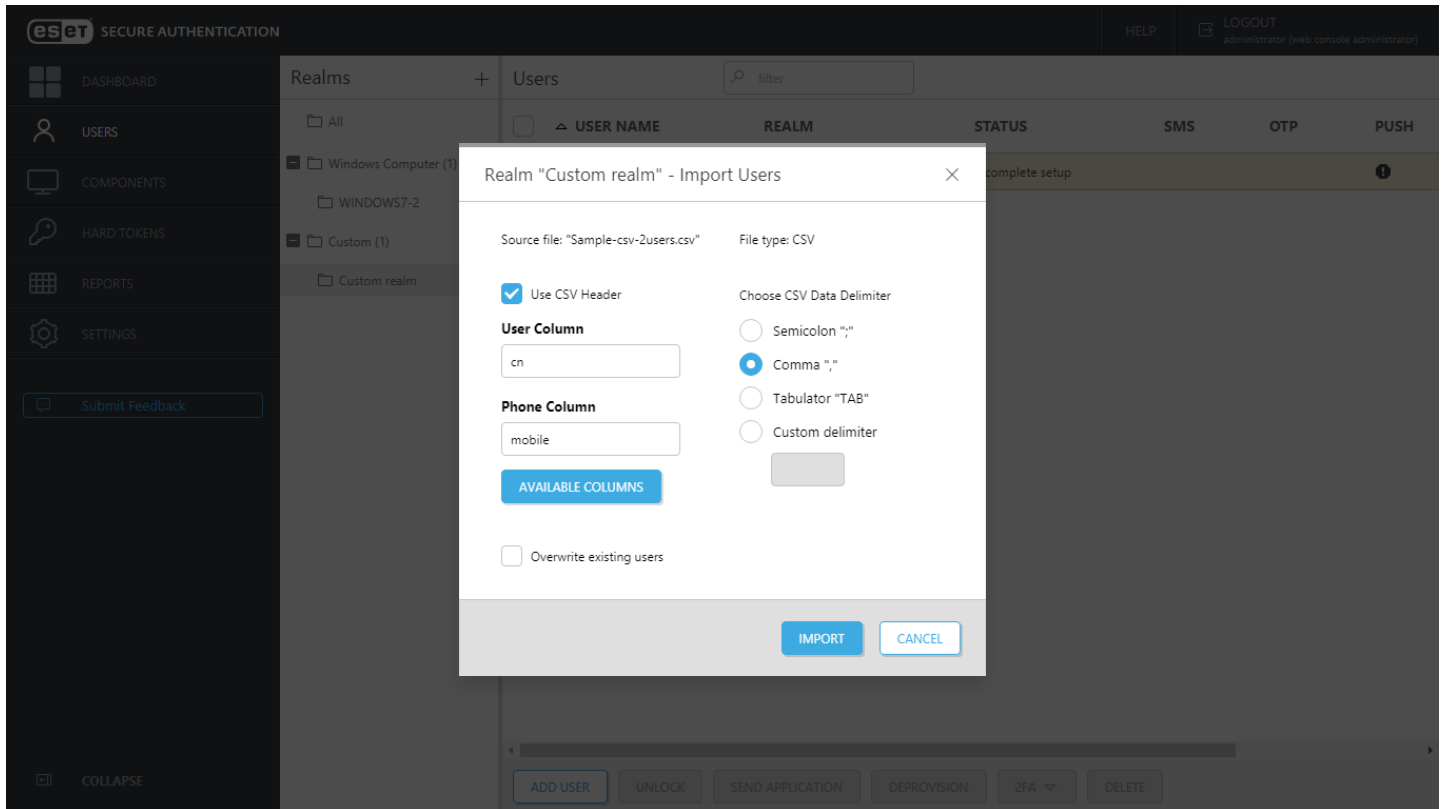
For more information on each authentication type see the official [Microsoft documentation](#).

5.2.3 Import users from file

ESET Secure Authentication 2.7 and later allows to import users to custom realms from a CSV or LDF file. The file has to contain the name of the user at least.

To import users to a custom realm, follow the steps below:

1. Select a custom realm.
2. Click the gear icon , select **Import Users** and then select file type.
3. Browse for the file, click **Open**.
4. In the import dialog, adjust settings if necessary based on the format of your CSV file.
5. Click **Import**.



To import users from an Active Directory environment to a [Standalone](#) installation of ESET Secure Authentication, export the appropriate CSV or LDF file using the command line on your Domain Controller (main computer).



Export Active Directory users to a file

- Export to CSV file:

```
csvde -f output.csv -r "(objectclass=user)" -l "dn,c,l,st,postalCode,r
```

- Export to LDF file:

```
ldifde -f export.ldf -s mydomain.com -r "(objectclass=user)" -l "cn, r
```

5.2.4 Self-enrollment

If self-enrollment is not enabled, but the user has a [2FA](#) method enabled and not yet functional due to missing information, they will be unable to log in to a machine protected by ESET Secure Authentication (for example [Windows Login protection](#)). The user will need to contact the administrator to generate a [Master Recovery Key](#) (MRK) to authenticate.

If self-enrollment is enabled, the user can authenticate using MRK, or enroll by clicking **Set up** and filling in the missing information.

Enable self-enrollment

1. In the [ESA Web Console](#), navigate to **Settings > Enrollment**.
2. Click the slider bar to automatically enable authentication options for new users.
3. Click the slider bar in the **Self enrollment** section.
4. Click **Save**.

Default authentication types

To assign new users (either [imported](#) or created automatically upon first login to an environment protected by ESA) an authentication method by default, enable the desired authentication method in the [ESA Web Console](#) in **Settings > Enrollment > Default authentication types**.

Add another authentication option

If a user is enabled for Hard Token with Mobile Application Push as the second authentication factor, but has been using Hard Token OTP to authenticate so far (they do not have [ESA Mobile App installed](#) or [provisioned](#)), and now they want to use another 2FA option, self-enrollment allows them to choose (activate) a new option.

1. Log in to a machine protected by ESET Secure Authentication (for example [Windows Login protection](#)).
2. When prompted to enter an OTP related to the Hard Token, click **Add another authentication method**.
3. Enter an OTP related to the Hard Token.
4. Click **Setup**.
5. Scan the QR code using the ESA Mobile Application by tapping the + icon inside the app and complete the installation and/or provisioning of ESA Mobile Application.
6. The self-enrollment process will require the user to verify the successful registration of the new authentication method by approving the push notifications.

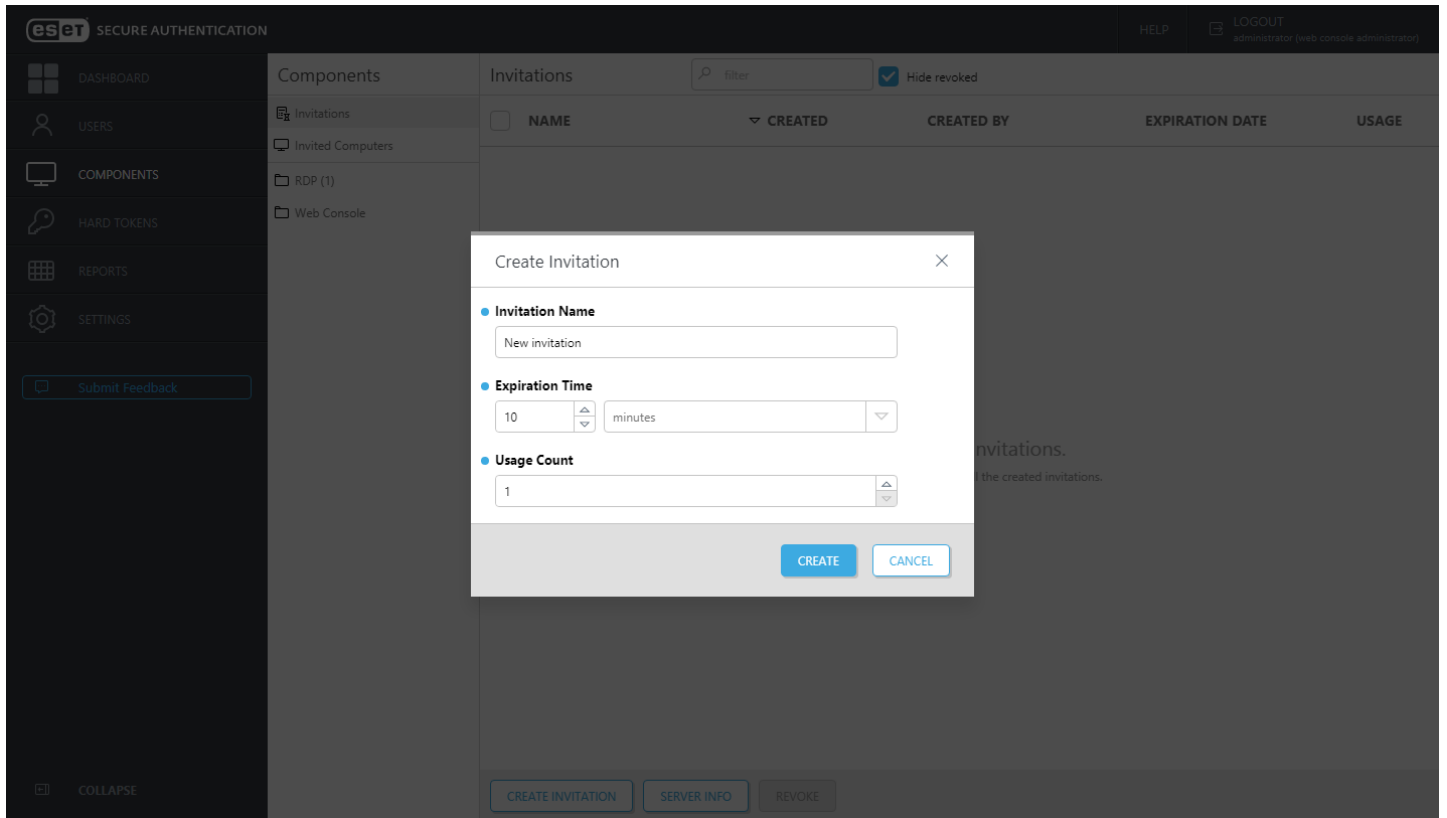
5.3 Invitations

Invitations were introduced in ESET Secure Authentication 2.7 to be able to deploy 2FA protection of ESA in a domain/network environment not established by Active Directory Domain Services. An invitation contains connection information of Authentication Server, certificate thumbprint and expiration, and a unique code based on which invitation is identified. Each invitation is limited by time and usage count.

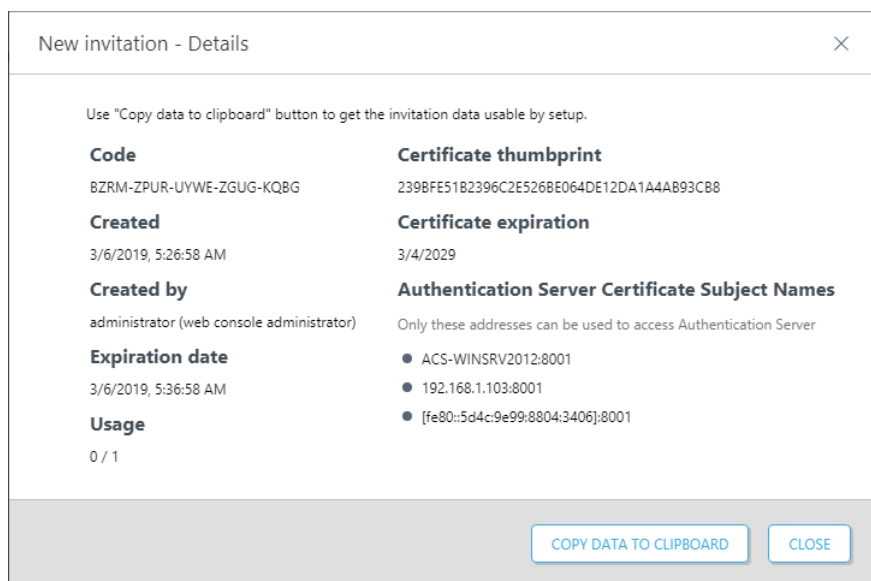
If you use ESET Secure Authentication in a domain established by Active Directory Domain Services, and you want to deploy 2FA on computers outside that domain, invitations make it possible.

Generate an invitation

1. In the ESA Web Console, click **Components > Invitations**.
2. Click **Create invitation...**
3. Enter an invitation name, expiration time and usage count. Click **Create**.



The invitation details displays. To save the details to a text file or to copy elsewhere, click **Copy data to clipboard**.



Click **Close**, and the list of invitations will display.

The screenshot shows the ESET Secure Authentication web console. The top navigation bar includes the ESET logo, 'SECURE AUTHENTICATION', and links for 'HELP' and 'LOGOUT' (Administrator (web console administrator)). The left sidebar contains navigation options: DASHBOARD, USERS, COMPONENTS, HARD TOKENS, and SETTINGS. The main content area is divided into two sections: 'Components' and 'Invitations'. The 'Invitations' section is active and shows a table with the following data:

	NAME	CREATED	CREATED BY	EXPIRATION DATE	USAGE
<input type="checkbox"/>	New invitation	4/17/2018, 4:13:26 AM	Administrator (web console administr...	4/19/2018, 4:13:26 AM	0 / 25

Below the table, there are three buttons: 'CREATE INVITATION...', 'SERVER INFO', and 'REVOKE'. The 'Invitations' section also includes a search filter and a message: 'No component types are available. Component types are shown here automatically when components are installed.'

Click the name of an invitation to open the invitation details again. Click **Server info** to view the connection information of Authentication Server, certificate thumbprint and expiration.

5.4 Use domain authentication

In an Active Directory (AD) environment, if Active Directory Integration type of deployment is used, you can log in to ESA Web Console clicking **Use domain authentication** in [supported browsers](#). This kind of authentication works if you log on to the machine hosting the Authentication Server with a user who belongs to the same Active Directory domain, and also belongs to the group of domain administrators.

If domain authentication does not work out of the box, attempt to troubleshoot with the steps below:

- Internet Explorer 11
 1. Click Tools, select **Internet options**.
 2. Select the **Security** tab.
 3. Click **Trusted Sites**.
 4. Click **Custom level...**
 5. Scroll down to **User Authentication**, select "**Automatic logon with current user name and password**".
 6. Click **OK** on both open configuration windows.
- Microsoft Edge, Google Chrome
 1. Complete the steps listed for Internet Explorer, and the domain authentication regarding ESA Web Console will work in both Microsoft Edge and Google Chrome.
- Mozilla Firefox
 1. Type **about:config** in the address bar.
 2. Click the **I accept the risk!** button.
 3. Type `network.negotiate-auth.trusted-uris` into **Search** bar.
 4. Double click the found result.
 5. Enter the domain name of **ESA Web Console** without protocol (<https://>), without port number and trailing slash.
 6. Press **Enter** key.

6. Authentication options

ESET Secure Authentication provides several options for authenticating users to access computers or services protected by two-factor authentication.

- OTP (one time password) received via sms - requires [SMS Credits](#) or [custom delivery](#) utilizing a custom SMS gateway
- OTP generated via [ESA mobile application](#)
 - Event-based OTP (HOTP)—expires when used or when generating a new OTP
 - Time-based OTP (TOTP)—expires within a few seconds (expiry animation displayed in the mobile application) even if not used
- [Push Authentication](#)
- [Hard tokens](#), Time-Based Hard tokens
- OTP received via [custom delivery option](#)
- [FIDO](#)— only one FIDO authenticator can be registered per user



Reliability of SMS delivery

Due to the technical nature of SMS messages, which are typically handled by local operators of telecommunication services, the reliability of SMS delivery to end-user mobile phone cannot be guaranteed by ESET.

6.1 Mobile Application

The mobile application of ESET Secure Authentication makes it easy to generate OTPs or approve [push authentication](#) requests to access computers, services protected by 2FA. The mobile application version 2.40+ supports authentication of multiple users, meaning, if you use several user accounts in a domain/network protected with 2FA, the authentication tokens of all your user accounts may be stored in your one mobile application.

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

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

[See a list of IP addresses and ports used for communication with ESET Secure Authentication Provisioning Server.](#)

Note that in case of PIN-protected Mobile Application the message of **Approve on phone** is displayed on Android watch when a push notification is generated.



PIN-protected Mobile Application

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.



OTPs and Whitespace

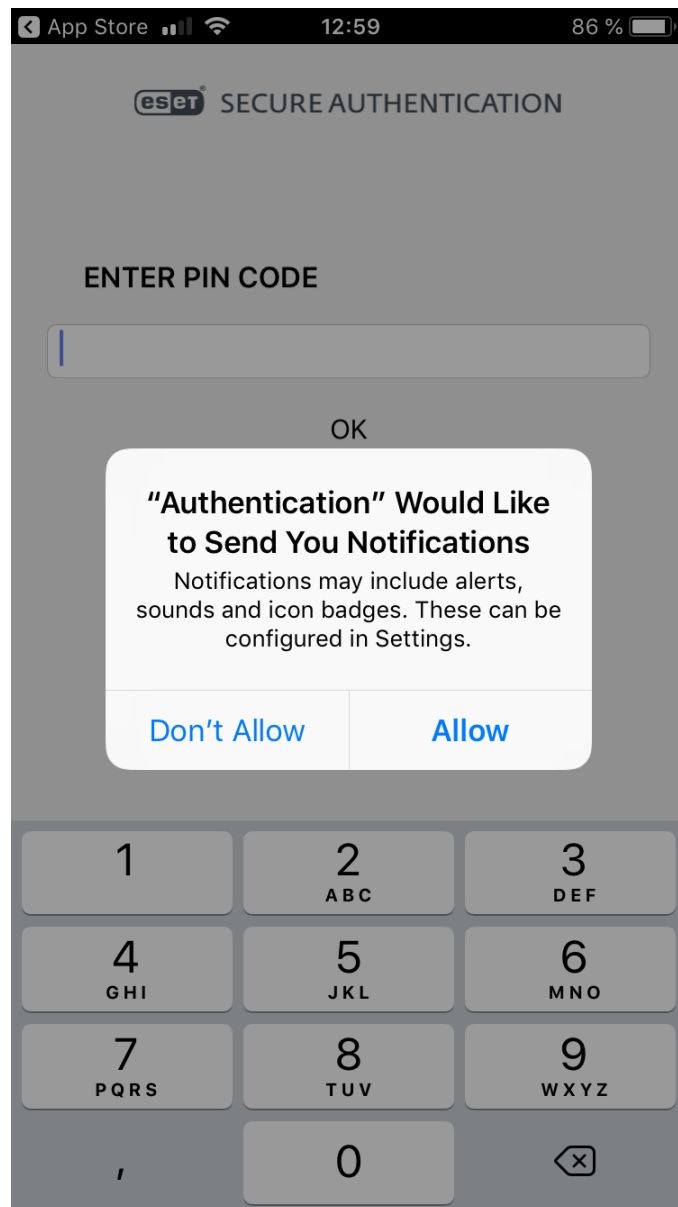
OTPs are displayed in the mobile application with a space between the 3rd and 4th digits in order to improve readability. All authentication methods except MS-CHAPv2 strip whitespace from the provided credentials, so a user may include or exclude whitespace without affecting authentication.

6.2 Push Authentication

The Push authentication method, which uses push notifications on mobile devices, was introduced in ESET Secure Authentication (ESA) version 2.5.X, and was available only for Android devices. ESA 2.6.X extended Push authentication to iOS devices also, and ESA 2.7 extends it to Windows phone as well.

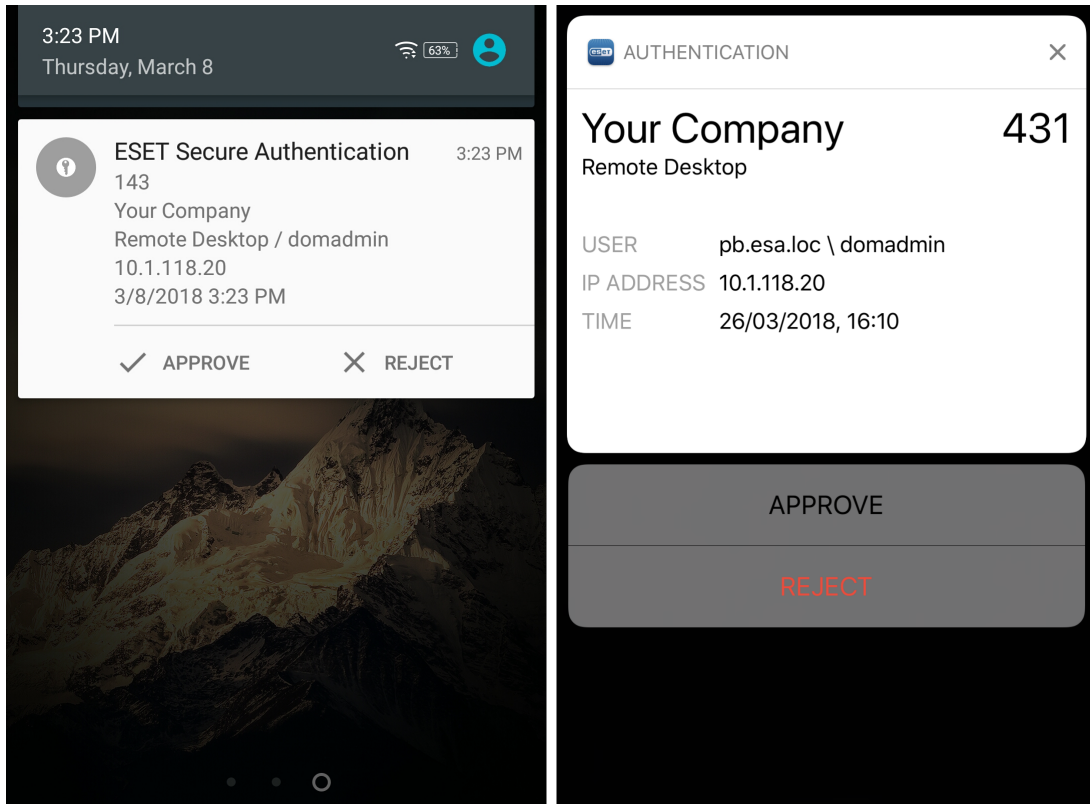
Both **OTP** and **Push** [authentication can be enabled per user or for multiple users](#) in one go in **Users** section of ESA Web Console.

To enable push notifications on iOS devices, when prompted, tap **Allow**. On Android devices, notifications are enabled automatically.



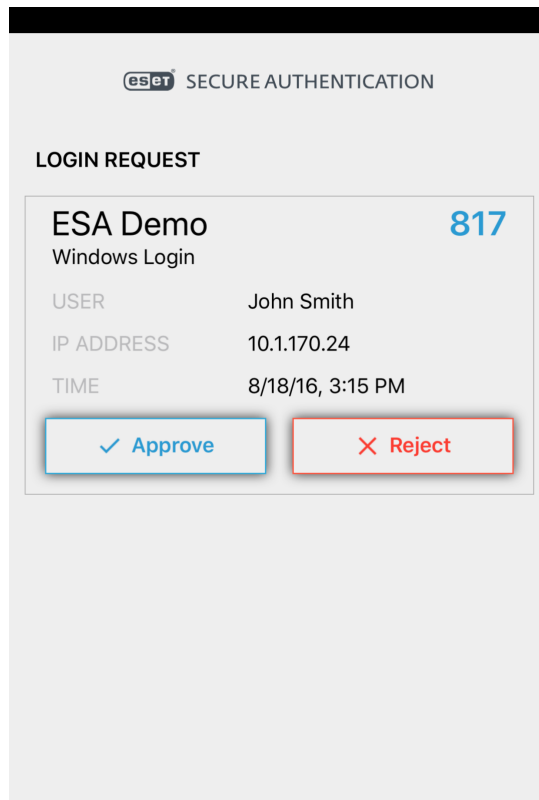
It may take some time for the push notifications to start working after the user's phone has been provisioned, or push notifications have been turned on in ESA Web Console.

Users can approve or reject the authentication request directly from the notification area of their mobile device.



Android; iOS

Tap the notification somewhere off the **Approve** and **Reject** buttons to open the Mobile application where you can approve or reject the authentication request.

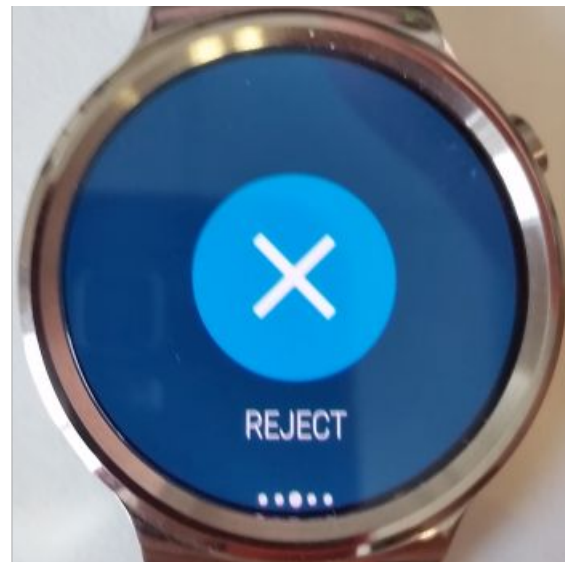
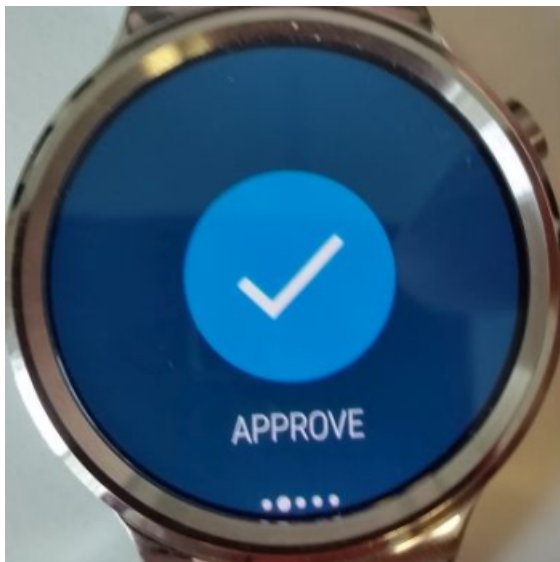


ESA Mobile App

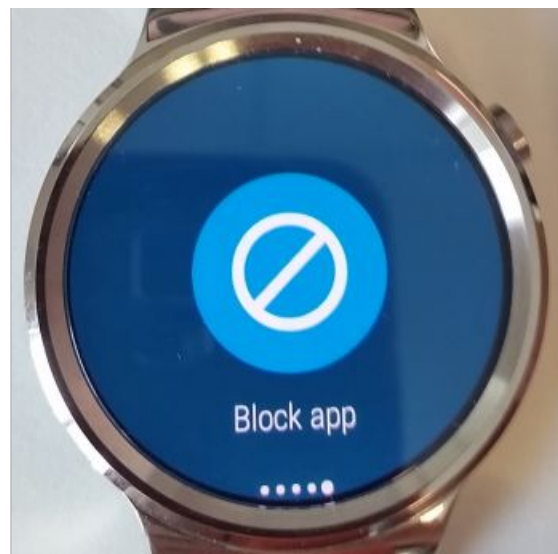
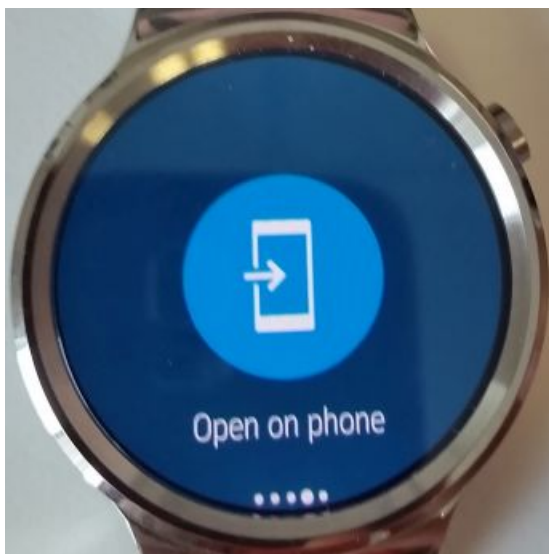
You can also manage Push authentication requests on smart watches running Android OS or iOS. Each push notification contains an ID which matches the ID of the authentication request screen.

Android smart watch

When an ESET notification displays on an Android smart watch, slide the screen right or left to see available options:



Approve the authentication request; Reject the authentication request



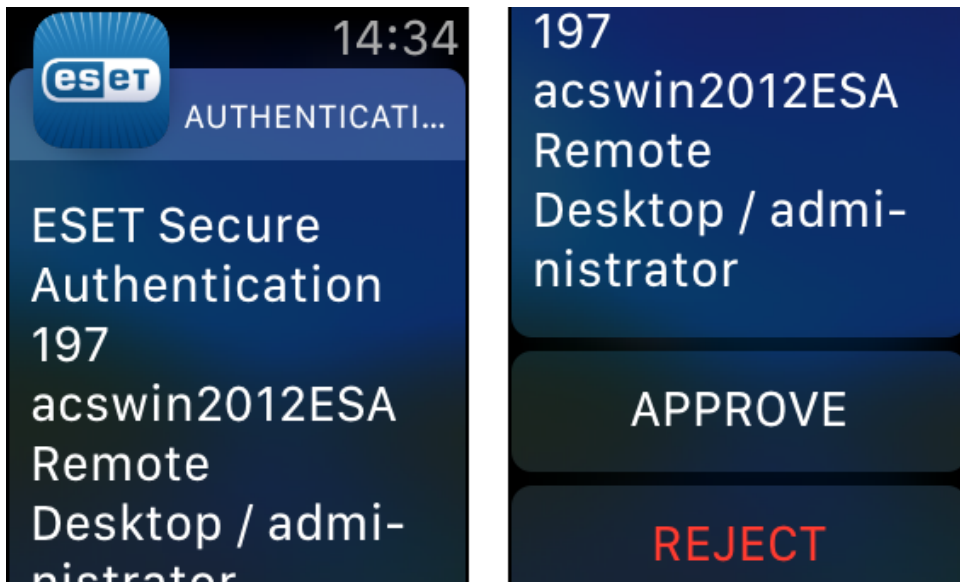
Open authentication request in mobile app; Disable notification on smartwach

If a PIN-protected Mobile Application is in use, 'Approve on phone' is displayed.



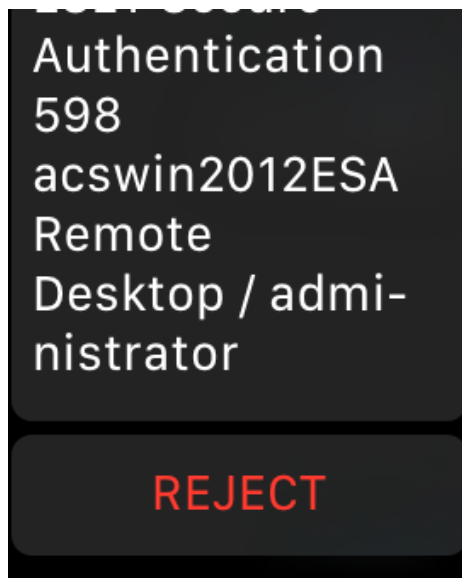
Apple watch

When an ESET notification displays on an Apple watch, scroll down to **Approve** or **Reject**.



Notification arrived; Scroll down to action buttons

If a PIN-protected Mobile Application is in use, only the **Reject** option is available.

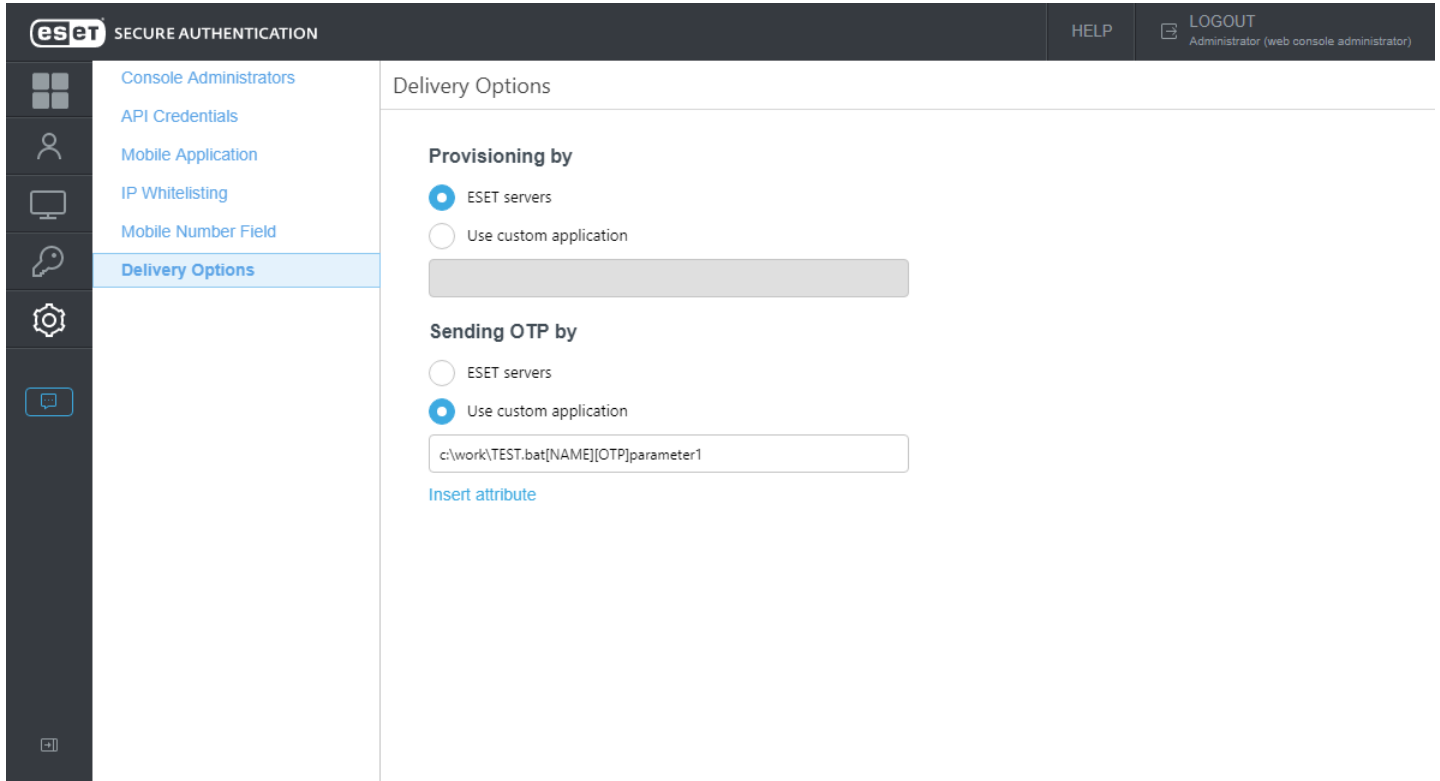


6.3 Custom delivery options

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

Standalone deployment type

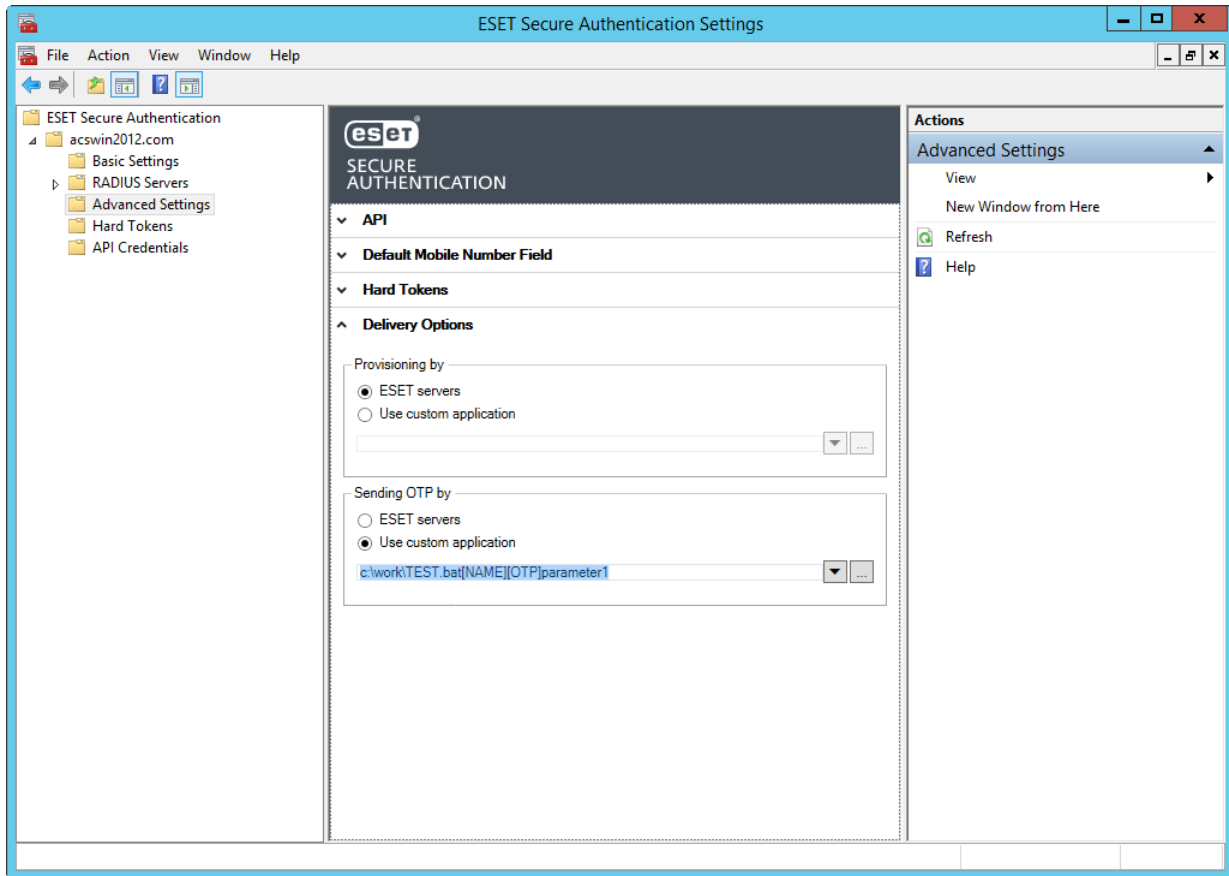
In ESA Web Console navigate to **Settings** , and click **Delivery Options**.





Here you can specify the path to your custom script by which you wish to handle provisioning or delivery of OTP. Click **Insert attribute** 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).

Active Directory Integration deployment type

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 available in Active Directory Integration deployment type - 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.



It is not necessary to make any change in the **Default Mobile Number Field** section to make the email delivery option work.

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



Example

```
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[1])
server.quit()
```



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

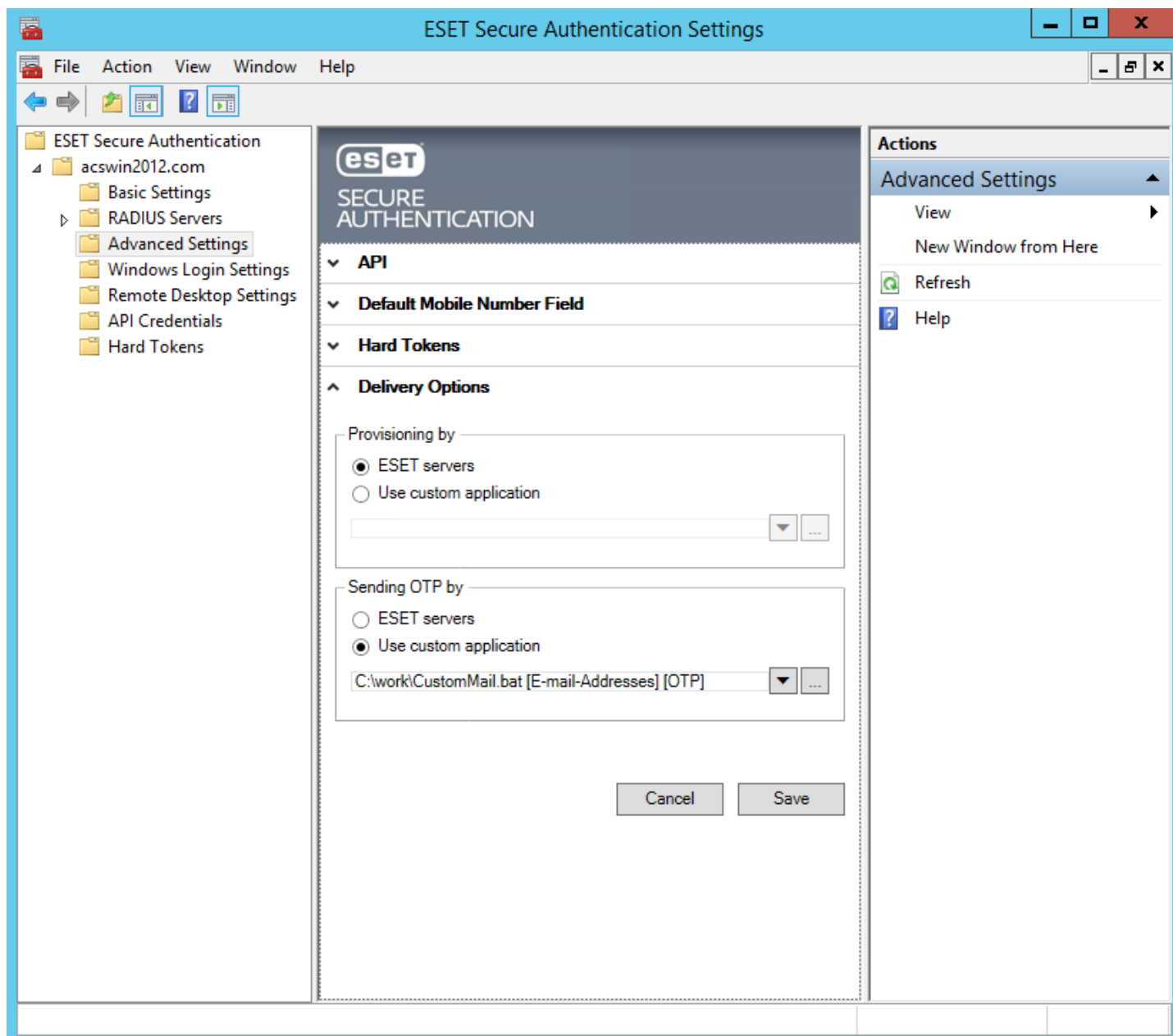
Sample .bat script for calling the `sendmail.py` script while passing the essential parameters to it - we name the file as **CustomMail.bat**:

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



This sample scenario assumes the python library is installed in your main computer where the ESA Authentication Server 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].



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).

6.3.1 Sample PowerShell scripts

Below are two sample PowerShell scripts to be used for delivering OTP via e-mail.

PowerShell script using Send-MailMessage - we name the file as sendmail.ps1



Example

```
param
(
    [string] $toAddress,
    [string] $otp
)

$smtpServer = "<server>"
$smtpPort = "<port>"
$smtpUsername = "<username>"
$smtpPassword = "<password>"

$fromAddress = "esa@localhost"
$subject = "ESA OTP"
$body = "Your OTP: $otp"

$smtpPassword_sec = ConvertTo-SecureString $smtpPassword -AsPlainText
$credential = New-Object System.Management.Automation.PSCredential ($smtpUsername, $smtpPassword_sec)

Send-MailMessage -SmtpServer $smtpServer -Port $smtpPort -Credential $credential -From $fromAddress -Subject $subject -Body $body -To $toAddress
```

PowerShell script using System.Net.Mail - we name the file as sendmail.ps1



Example

```
param
(
    [string] $toAddress,
    [string] $otp
)

$smtpServer = "<server>"
$smtpPort = "<port>"
$smtpUsername = "<username>"
$smtpPassword = "<password>"
```



```

$fromAddress = "esa@localhost"
$subject = "ESA OTP"
$body = "Your OTP: $otp"

$mailMessage = New-Object System.Net.Mail.MailMessage($fromAddress, $toAddress, $subject, $body)
$smtpClient = New-Object System.Net.Mail.SmtpClient($smtpServer, $smtpPort)
$smtpClient.EnableSsl = $true
$smtpClient.Credentials = New-Object System.Net.NetworkCredential($smtpUsername, $smtpPassword)
$smtpClient.Send($mailMessage)

```



In the sample scripts above, replace the <server>, <port>, <username> and <password> placeholders with the corresponding SMTP details.

Test and use

1. Save the script in a desired location, for example `c:\work\sendmail.ps1`
2. Test the script outside of ESET Secure Authentication (ESA) using Windows command line:

- a. Press Windows key + R key combination.
- b. Type in `cmd.exe`, press Enter.
- c. In the command line window, execute:

```
powershell c:\scripts\sendmail.ps1 test@address.com 123456
```

while `test@address.com` is supposed to be replaced with a valid email address, you can read its inbox.

- d. If the test is successful, proceed with the next step.

3. In the **Delivery Options** section of ESA, refer to the script this way:

```
powershell c:\scripts\sendmail.ps1 [E-mail-Addresses] [OTP]
```

6.4 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.

To use and manage hard tokens, see instructions below.

Enable and Import Hard Tokens

1. In the ESA Web Console, click **Hard Tokens**.
2. Select the **Enabled** checkbox if it has not been selected by default.
3. Click the **Import Hard Tokens** button.
4. Select the file to import. This should be an XML file in the PSKC format. If such a file was not received from the hard token vendor, contact the vendor. If the XML file is password protected or protected by an encryption key,

type the password or encryption key (HEX or base64 format) to the **Password** field in **Import Hard Tokens** window.

5. Click the **Import tokens** button.
6. A result notification will pop up indicating how many hard tokens were imported and the imported hard tokens will be displayed.

<input type="checkbox"/>	SERIAL NUMBER	START DATE	EXPIRY DATE	ASSIGNED	ISSUER	MANUFACTURER
<input type="checkbox"/>	1540	11/11/2014	11/11/2024	(none)	ESA	NagralD
<input type="checkbox"/>	1541	11/11/2014	11/11/2024	(none)	ESA	NagralD
<input type="checkbox"/>	1542	11/11/2014	11/11/2024	(none)	ESA	NagralD

Assign Hard Token to a user

1. In the ESA Web Console, click **Users**.
2. Click the name of the appropriate user.
3. Click the toggle next to **Hard Token** and select a hard token from the list.
4. Click **Save**.

2FA is activated with SMS-based OTPs

Authentication Events

4/10/2018, 2:09:06 AM	4/9/2018, 11:03:03 PM	0
Last Successful Login	Last Failed Login	Consecutive Failed Logins

Mobile number: +[REDACTED]

SMS-based OTPs

Mobile Application OTP

Mobile Application Push

Hard Token

Not assigned
1540
1541
1542

Revoke Hard Tokens


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

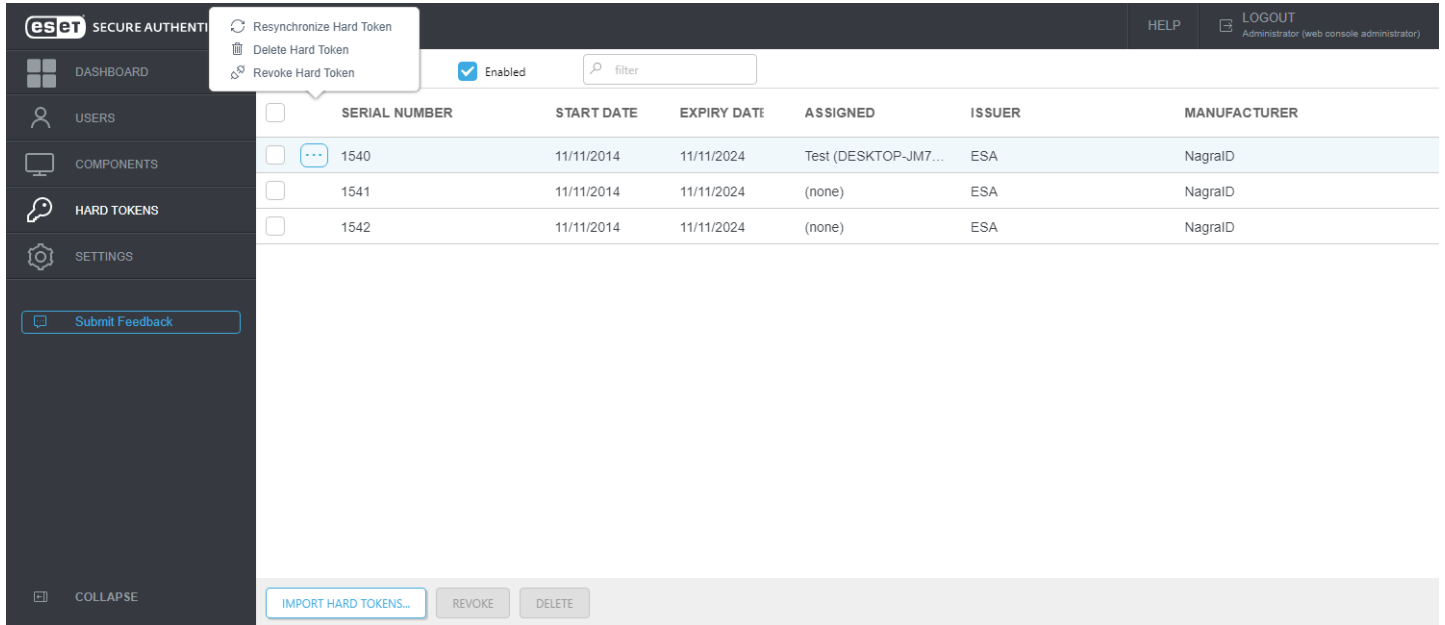
1. In the ESA Web Console, click **Hard Tokens**.
2. Select the appropriate tokens and click **Revoke**.

Resynchronize a Hard Token

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 span of time. In this scenario, a resynchronization will be required.

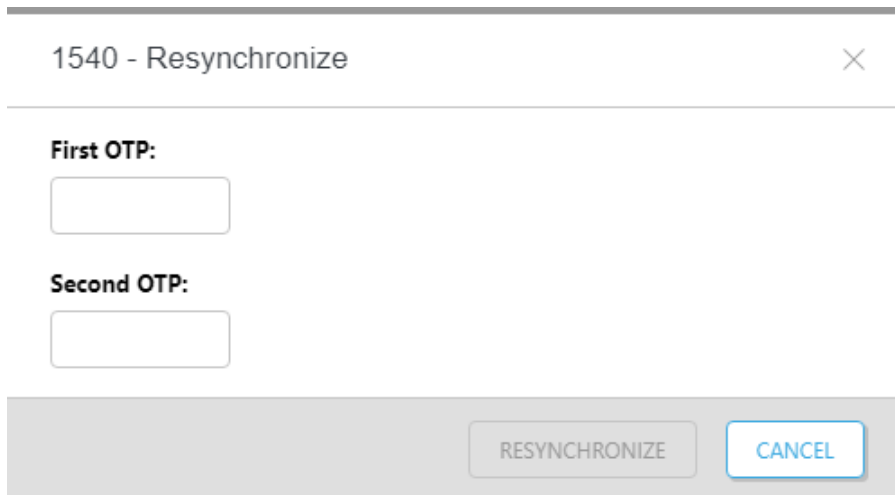
A token can be resynchronized as follows:

1. In the ESA Web Console, click **Hard Tokens**.
2. In the appropriate row, click , and select **Resynchronize Hard Token**.



<input type="checkbox"/>	SERIAL NUMBER	START DATE	EXPIRY DATE	ASSIGNED	ISSUER	MANUFACTURER
<input type="checkbox"/>	1540	11/11/2014	11/11/2024	Test (DESKTOP-JM7...	ESA	NagraID
<input type="checkbox"/>	1541	11/11/2014	11/11/2024	(none)	ESA	NagraID
<input type="checkbox"/>	1542	11/11/2014	11/11/2024	(none)	ESA	NagraID

Generate and enter two consecutive OTPs using the selected hard token.



1540 - Resynchronize

First OTP:

Second OTP:

RESYNCHRONIZE CANCEL

3. Click the **Resynchronize** button.
4. A successful message will display.

Delete Hard Tokens

1. In the ESA Web Console, click **Hard Tokens**.
2. Select the appropriate tokens and click **Delete**.

6.5 FIDO

From version 2.8 ESET Secure Authentication (ESA) supports two-factor authentication (2FA) on devices that support [FIDO2](#) (and FIDO U2F) authentication standards. [See more information about FIDO here.](#)

Requirements

- Web browser that supports Web Authentication API
 - Mozilla Firefox
 - Google Chrome
 - Microsoft Edge

For up-to-date information about supported browsers, visit <https://platform-status.mozilla.org/> and search for "Web Authentication API".

- Secure connection (HTTPS) (self-signed certificates can also be used)
- .NET Framework 4.7.2 installed on the machine where [ESA Authentication Server](#) is installed

Supported environment

- Web-based login environment protected by ESA:
 - [ESA Web Console](#)
 - [IIS](#)
 - [AD FS](#)



NOTE

FIDO implementation in ESET Secure Authentication has not yet been certified by the FIDO alliance.

Configuration in ESA Web Console

The configuration in **Settings > FIDO** is for advanced FIDO administrators; there is no need to make any changes there.

- User Verification
 - Required—The FIDO-compatible authenticator must support user verification (e.g. via biometrics or PIN code). If there is no user verification, the FIDO-compatible authenticator cannot be used as second authentication factor.
 - Preferred—It is preferred for the FIDO-compatible authenticator to support user verification, however it is not essential.
 - Discouraged—It does not matter if the FIDO-compatible authenticator supports user verification or not.
- Authenticator Type
 - Platform (On bound)—The FIDO authenticator is a built-in solution (software, hardware) of the device where it is used as a second authentication factor.
 - Cross-platform (Roaming)—The FIDO authenticator is detachable and can be used with several devices.
 - Not specified—Does not matter if the FIDO authenticator is detachable or not.

Register FIDO origin

If you are using FIDO as a second authentication factor to access the ESA Web Console available at <https://my-web-console.com:8001>, then <https://my-web-console.com:8001> must be registered as the origin.

1. In ESA Web Console, navigate to **Components > Web Console**.
2. Turn on **FIDO**.
3. Enter the ESA Web Console URL in the **FIDO Origin** window. In our example, <https://my-web-console.com:8001>.
4. Click **Apply > Save**.

Activate FIDO for a user

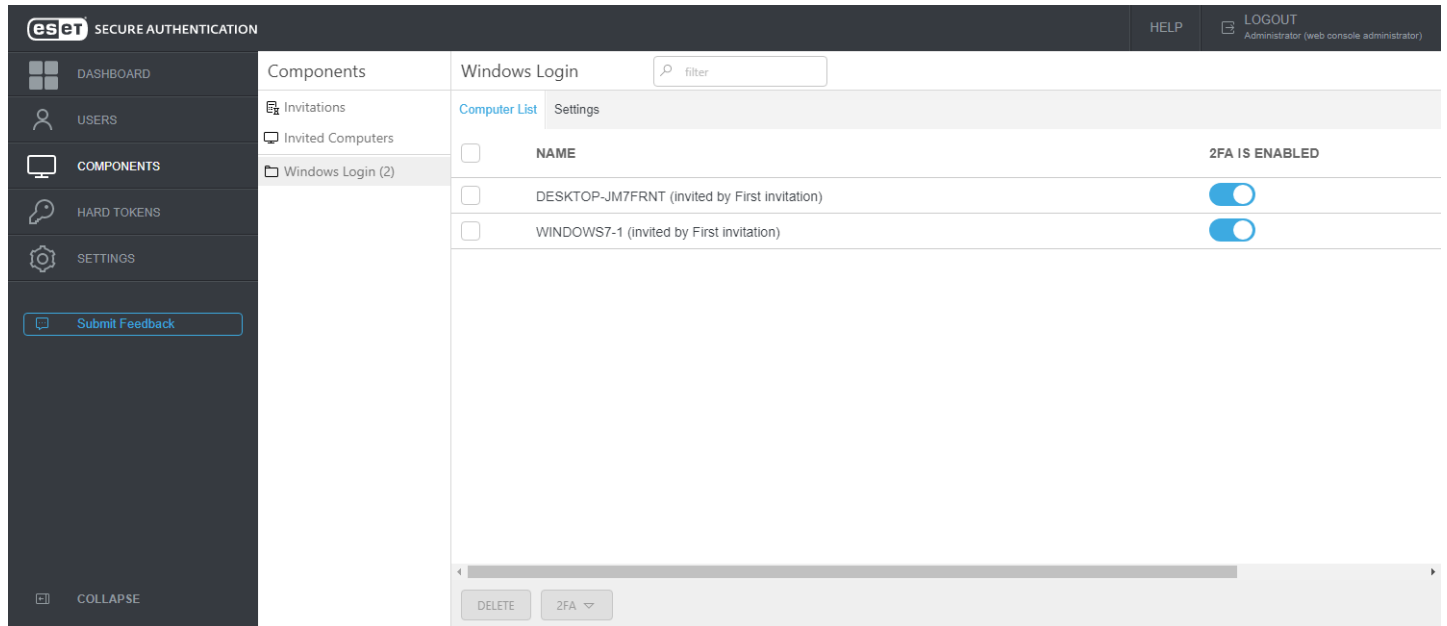
In our example, we activated FIDO as a second factor for an administrator of ESA Web Console who wants to use a FIDO USB key as a hardware authenticator.

1. Navigate to **Settings > Web Console Administrators**, click the name of the administrator.
 - a. If you are activating FIDO for a general user, look up the user in the **Users** screen.
2. In the user's profile turn on **FIDO**.
3. Plug in the FIDO USB key into the computer where you accessed ESA Web Console.
4. Click **Actions > Register FIDO credentials** and then click **Apply**.
5. When the USB key blinks, touch the touch sensor on the FIDO USB key.
6. ESA Web Console will confirm the successful registration of FIDO credentials.

From now on, when attempting to access the ESA Web Console, the administrator will be required to approve authentication by tapping the FIDO USB key after the correct login credentials were entered.


7. Windows Login Protection

ESA features local login protection for Windows in a domain or LAN environment. To utilize this feature, the **Windows Login** component must be included during [installation](#) of ESA. Once installation is finished, access ESA Web Console, navigate to **Components**, click **Windows Login**. The list of computers where the **Windows Login** component of ESA is installed will display. From this screen you can enable/disable 2FA protection per computer.

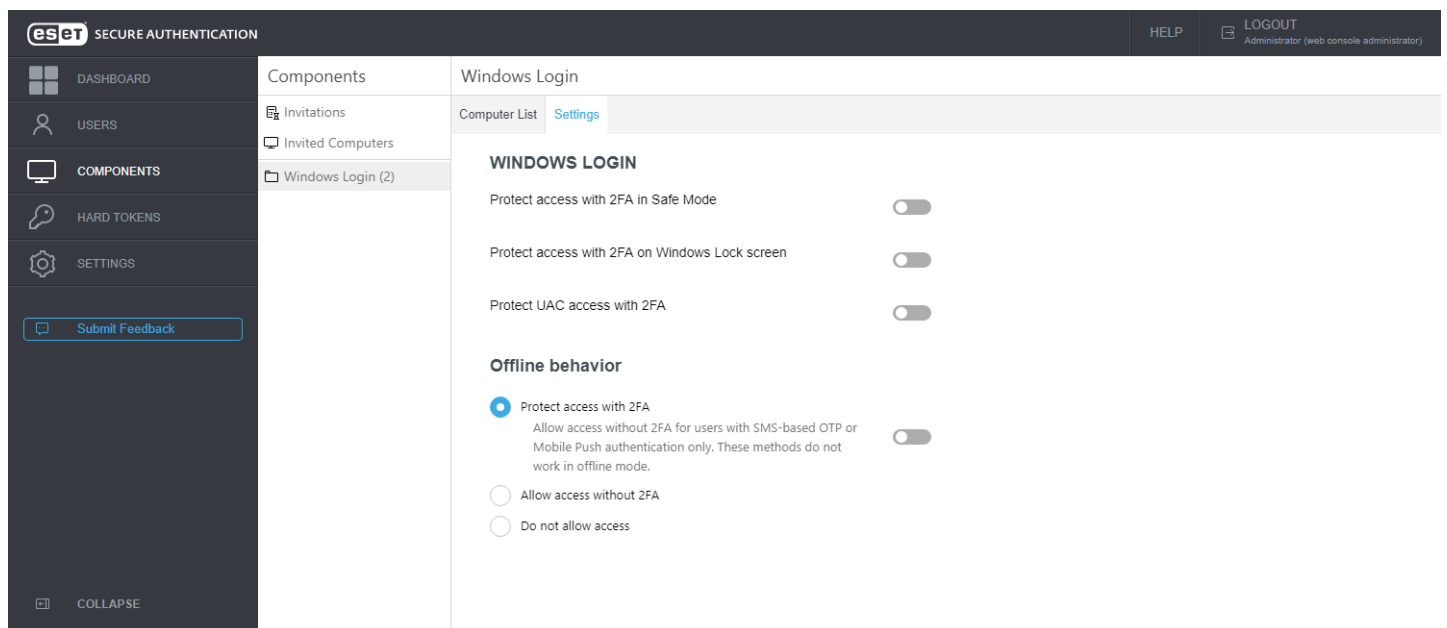


NAME	2FA IS ENABLED
DESKTOP-JM7FRNT (invited by First invitation)	<input checked="" type="checkbox"/>
WINDOWS7-1 (invited by First invitation)	<input checked="" type="checkbox"/>

If you have a long list of computers, use the **Filter** field to search for a specific computer by typing its name.

If the **Windows Login** component of ESA version 2.6 or later is uninstalled from a particular computer, the computer will be removed from the Computer List of ESA Web Console automatically. A computer entry can be deleted manually also from the Web Console. Select a computer entry and click **Delete**, or hover a computer, click  and select **Delete**. Click **Delete** in the confirmation window also. If a computer entry is removed from the Computer List but the **Windows Login** component is not removed from the particular computer, the computer will show up again in the Web Console with default settings.

Click **Settings** tab to see available settings.



WINDOWS LOGIN

- Protect access with 2FA in Safe Mode
- Protect access with 2FA on Windows Lock screen
- Protect UAC access with 2FA

Offline behavior

- Protect access with 2FA
Allow access without 2FA for users with SMS-based OTP or Mobile Push authentication only. These methods do not work in offline mode.
- Allow access without 2FA
- Do not allow access

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).

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 users with SMS-based OTP or Mobile Push authentication only**.

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 username and password again to receive a new OTP.

2FA protection cannot be bypassed by any attacker even if the attacker knew the 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.

We recommend to combine 2FA protection with whole disk encryption to mitigate the breach risk if an attacker has physical access to the disk.



2FA enabled for offline mode

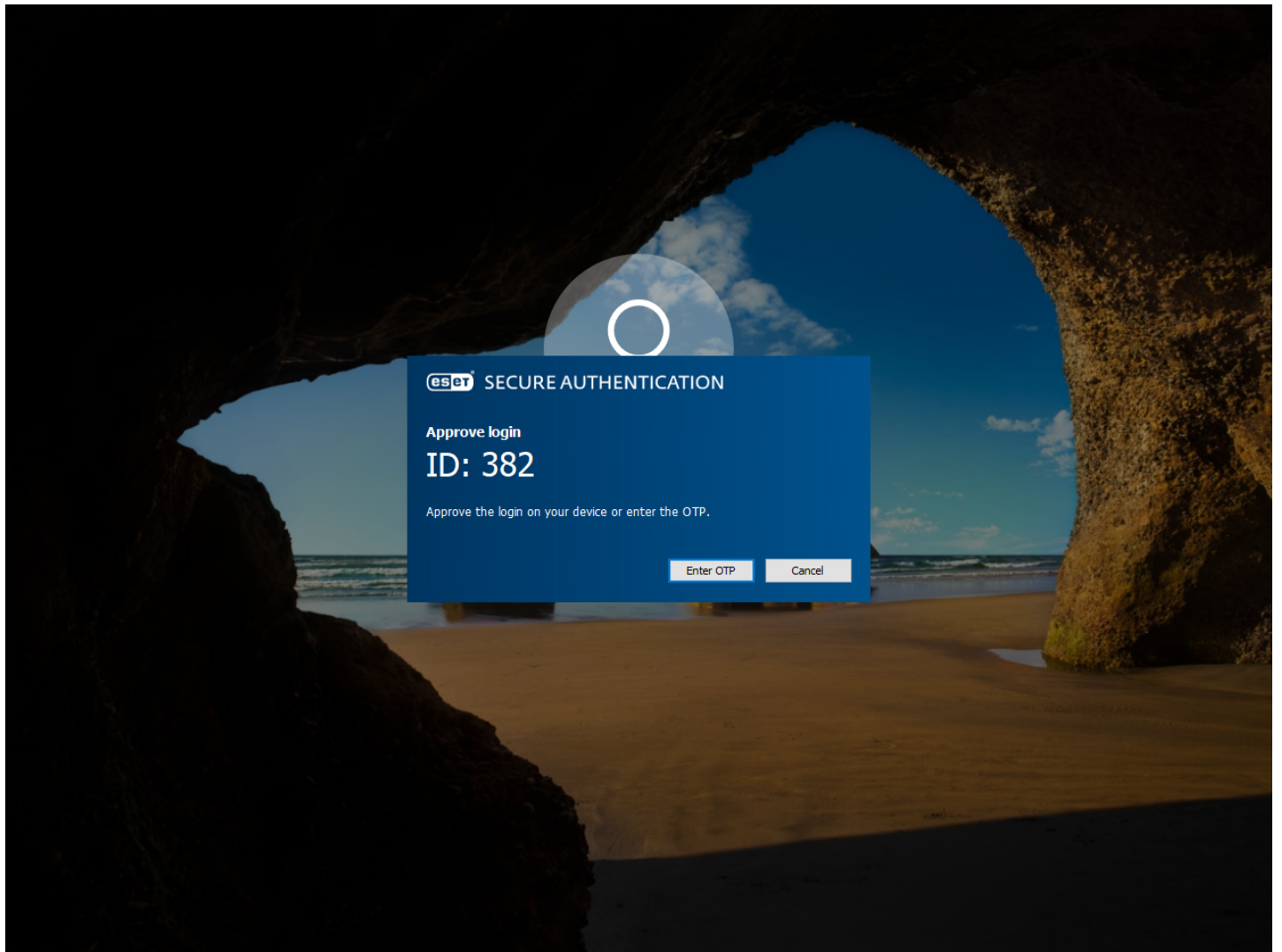
If 2FA protection is enabled for offline mode, all users whose accounts are secured by 2FA and who want to use a 2FA-protected PC must log in to that PC for the very first time while the PC is online. By 'online' we mean that the main computer where [Authentication Server](#) of ESA is installed and 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 Authentication Server is installed and 2FA protection for Safe Mode is enabled on that computer while offline mode is disabled (**Do not allow access** is selected in **Offline behavior** section), then the user will be allowed to log in to Safe Mode (without networking) without OTP.

The offline mode allows to log in 20 times using valid OTP each time. If the limit is exceeded, the machine needs to be online when trying to log in. Whenever the machine is online while trying to log in, the limit counter is reset.

To allow specific users to log on to certain computer(s) only in an Active Directory environment, configure a "[Deny log on locally](#)" policy.

Windows 10 login secured by ESA in - after entering a valid username and password, users will be prompted to approve login on their Android/iOS mobile device or Android/Apple watch, or to enter an OTP :



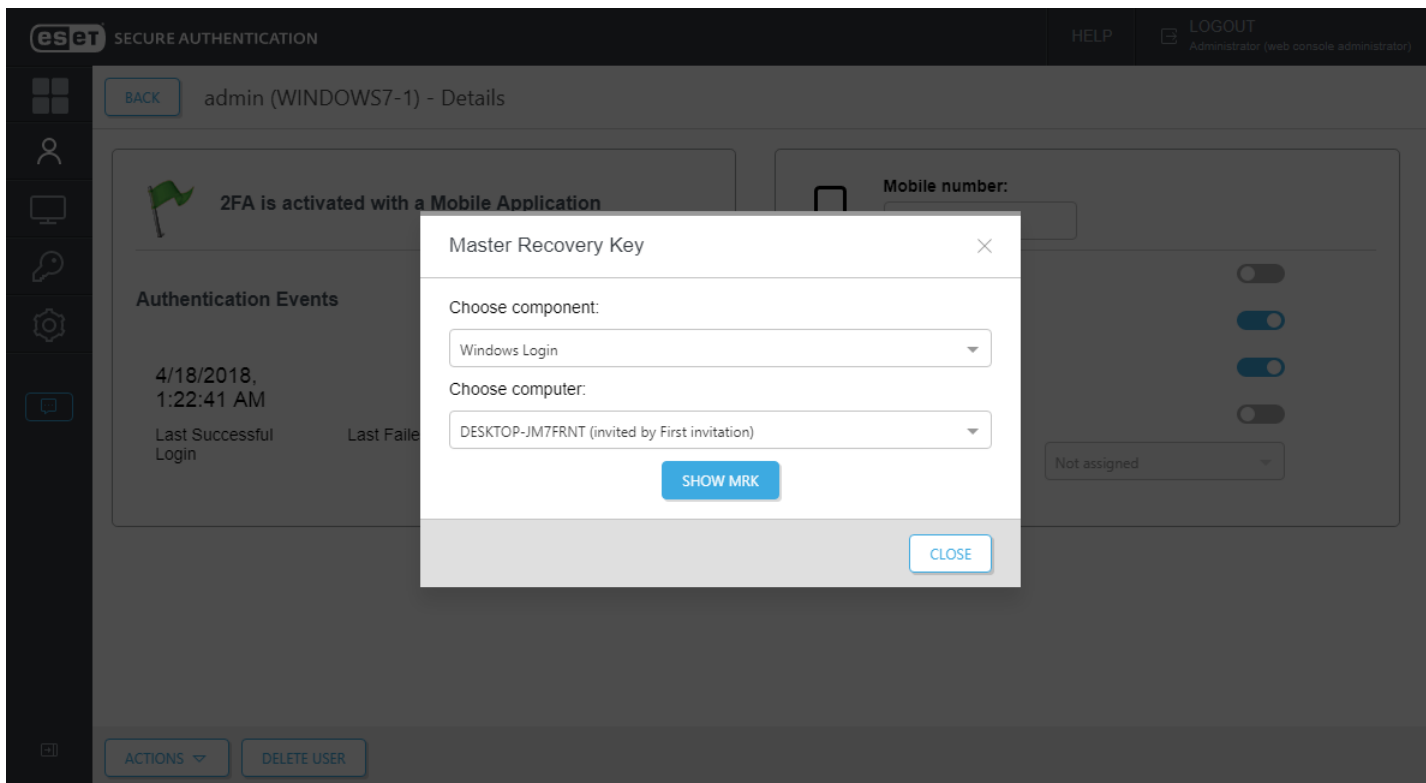
7.1 Master recovery key

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, or cannot authenticate by approving a push notification. 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 Web 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.

You can use MRK version 2.6 and later for other protection modules of ESA.

To use MRK for authentication:

1. Users cannot obtain an OTP, so they need to call the administrator.
2. The administrator opens ESA Web Console, navigates to **Users** > clicks the name of the particular user > clicks **Actions** > selects **Show MRK** > selects the particular protection module from the **Choose component** list-box, then selects the particular computer from the **Choose computer** list-box and clicks **Show MRK**. At this point a **MRK** is generated.



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 to log in to the particular Windows machine multiple times.

After first successful connection to ESA Authentication Server the previously generated MRK is invalidated and can not be used anymore, even if it was not used at all.

MRK generated for other protection modules of ESA are valid at most for 1 hour or until regenerated.

MRK for ESA Web Console administrator

In a case where the administrator of the ESA Web Console is unable to authenticate (for example, reinstalled [ESA Mobile Application](#), lost PIN code, lost phone where the ESA Mobile Application was installed), reset ESA Web Console credentials:

1. Run the installer of ESET Secure Authentication again.
2. Click **Change**.
3. To replace the old account with a new one, enter the *original* administrator username and a *new* password when prompted. To create a different account, enter a new username and password.
4. Close the installer when complete.

8. 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.

Though it is used in most configurations, ESA RADIUS does not necessarily need to be used to allow for VPN protection alone. For more information see [RADIUS PAM modules on Linux/Mac](#).

8.1 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. In the ESA Web Console, navigate to **Components > RADIUS**, select a RADIUS server and click **Create new RADIUS client**.
2. Give the RADIUS client a memorable name for easy reference.
3. 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. If your appliance communicates via IPv6, use that IP address along with the related [scope ID](#) (interface ID). The shared secret is the RADIUS shared secret for the external authenticator that you will configure on your appliance.
4. 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.
5. Optionally, you can allow any non-2FA users to use the VPN.



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 log in using the VPN. Using this configuration is not recommended.

6. Optionally, restrict VPN access to an existing [AD](#) security group.
7. Select "Current AD domain" or "Current AD domain and domains in trust" from the **Realm** selection box to have the realm (domain) of the user be automatically registered when the user authenticates for the first time using VPN and 2FA. Alternatively, select a specific realm from the selection box to have all users be registered to the same realm..
8. Once you are finished making changes, click **Save**.
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.



If the Mobile Application Push authentication method is enabled, set the authentication expiration time of your VPN server to more than 2.5 minutes.

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

Additional attributes to be sent by ESA RADIUS

If your VPN client requires additional RADIUS attributes to be sent by ESA RADIUS, configure it in *C:\Program Files\ESET Secure Authentication\EIP.Radius.WindowsService.exe.config* by adding a code snippet similar to following:

```
<appSettings>
  <add key="Radius_Attribute_ID" value="any_value_expected_by_your_VPN_server" />
</appSettings>
```

If the `<appSettings>` tag is already present, do not duplicate it, just add the `<add key... >` code below it.

Supported additional attributes: Filter-Id, Framed-IP-Address, Framed-IPv6-Prefix and Framed-Interface-Id.

Filter-Id bears a static value you configure in *EIP.Radius.WindowsService.exe.config* file. The value of other supported attributes can be configured in Active Directory Users and Computers (ADUC).

Supported attributes configurable in ADUC

EIP.Radius.WindowsService.exe.config key field value	RADIUS attribute	Value retrieved from AD user attribute	Where to configure in ADUC?
RadiusSendAttribute_Framed-IP-Address	Framed-IP-Address	msRADIUSFramedIPAddress	Dial-In tab > Assign Static IP Addresses > Assign a static IPv4 address
RadiusSendAttribute_Framed-IPv6-Prefix	Framed-IPv6-Address	msRADIUS-FramedIpv6Prefix	Dial-In tab > Assign Static IP Addresses -> Assign a static IPv6 address - Prefix
RadiusSendAttribute_Framed-Interface-Id	Framed-Interface-Id	msRADIUS-FramedInterfaceId	Dial-In tab > Assign Static IP Addresses > Assign a static IPv6 address - Interface ID

8.2 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.

8.3 VPN Authentication Options

This section reviews available configuration options for a RADIUS client using either the [ESA Web Console](#), or ESA Management Console in an [AD](#) environment.

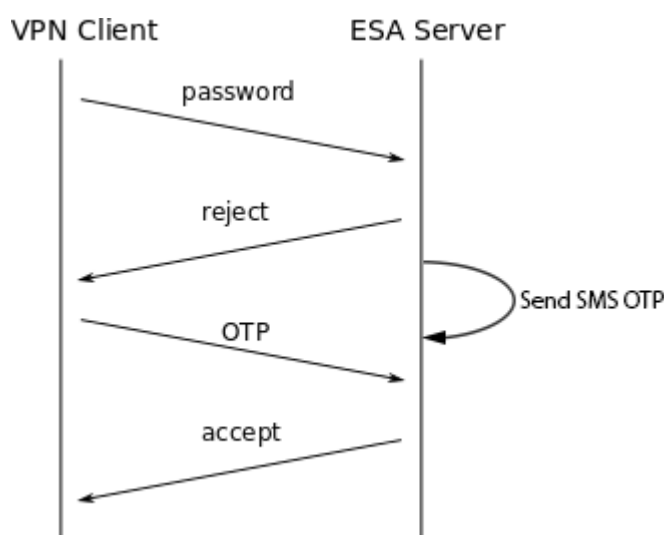
8.3.1 SMS-based OTPs

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: RADIUS SMS OTP Authentication.

Supported authentication protocols: PAP, MSCHAPv2.



RADIUS SMS OTP Authentication

8.3.2 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" in the **ESA OTP** field to receive a One Time Password via SMS.



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.

8.3.3 Mobile Application

This scenario occurs if the user is configured to use only the OTP and/or Push and the RADIUS client is configured to use Mobile Application OTPs and/or Mobile Application Push authentication.

The user logs in with an OTP generated by the Mobile Application or by approval of push notification generated on their Android/iOS mobile device or Android/Apple watch. Note that PIN enforcement is strongly recommended in this configuration to provide a second authentication factor.



PIN-protected Mobile Application

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.

Supported PPTP Protocols: PAP, MSCHAPv2.

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 OTPs.

In this scenario, a user logs into the VPN by entering their Active Directory (AD) password, in addition to 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.



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.

8.3.4 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 a 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, in addition to an OTP generated by their Hard Token. For example, given an AD password of 'password' and an OTP of '123456', the user enters 'password123456' in the password field of their VPN client.

Supported authentication protocols: PAP.

8.3.5 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.

8.3.6 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.



About upgrading

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.

8.3.7 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.

8.4 ESA Authentication Methods and PPP Compatibility

The VPN server must be configured to allow all protocols a clients might want to use. End-user VPN clients only need to 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
SMS-Based OTPs	Supported	Supported
On-demand SMS-Based OTPs	Supported	Supported
Mobile-Application (OTP or Push)	Supported	Supported
Mobile Application (Compound Authentication)	Supported	Not supported
Hard Token OTPs	Supported	Supported
Hard Token (Compound Authentication)	Supported	Not supported
Active Directory passwords without OTPs	Supported	Supported

9. 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.

In general, any service using RADIUS can be configured to use 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, configure your [Linux](#) or [Mac](#) computer based on the instructions in the following sub-chapters.

9.1 Mac OS - configuration

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



Non-2FA users

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.

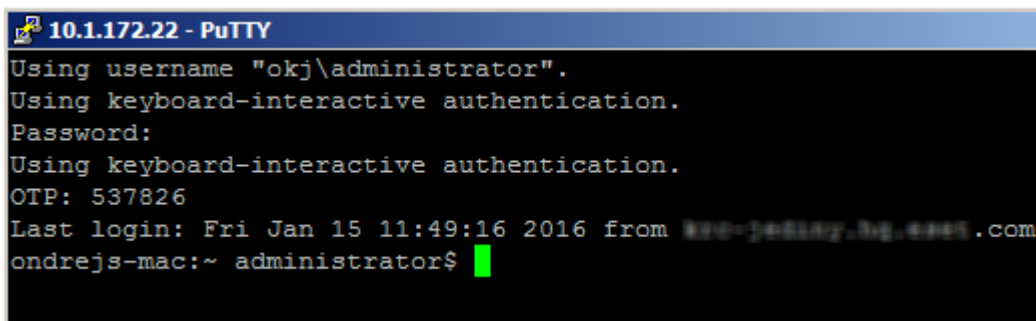
Incorporating the PAM module into SSH

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
```

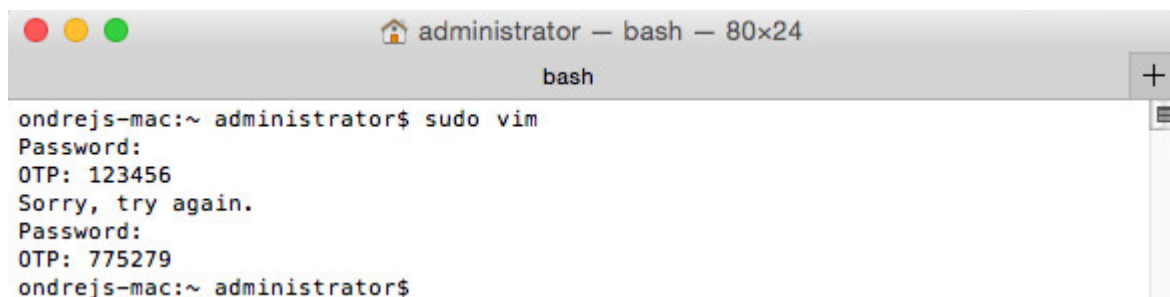
Next, enable SSH in OS X. Under *System Preferences... > Sharing*, enable **Remote Login**.

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 193-104-107.103.cores.com
ondrejs-mac:~ administrator$
```

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



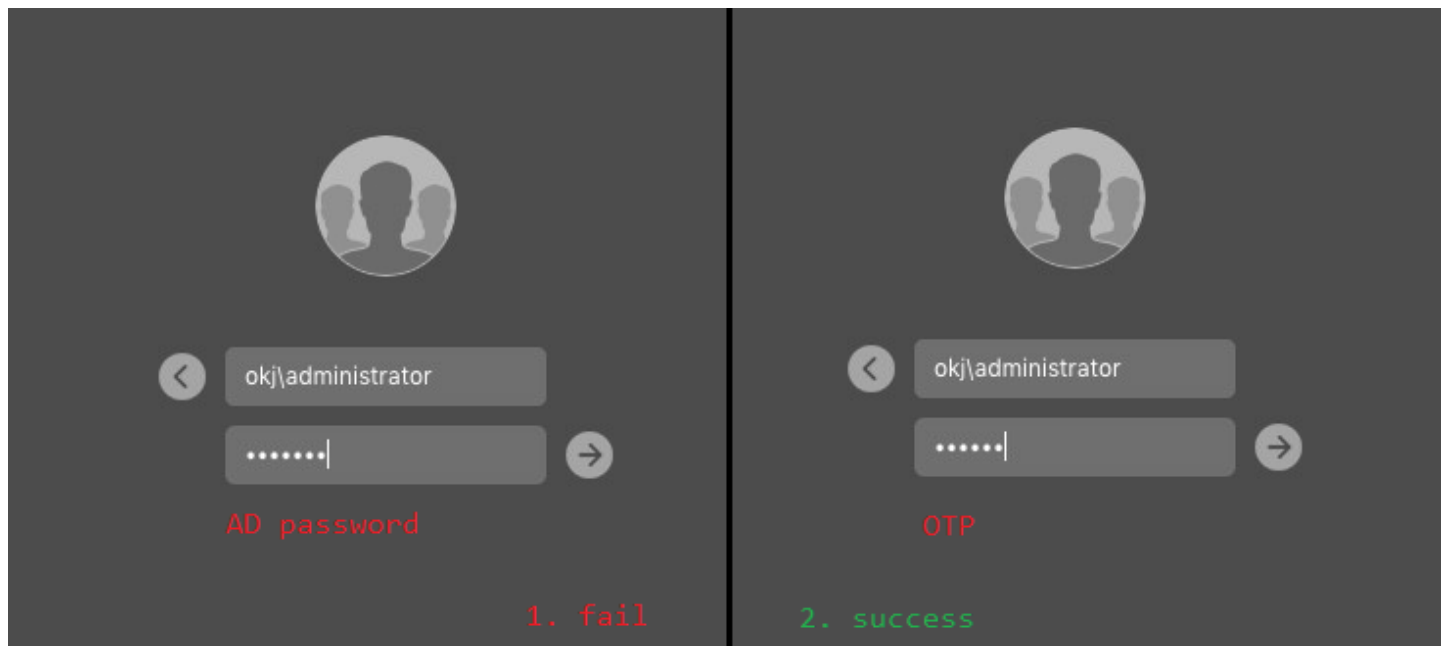
```
administrator — bash — 80x24
bash
ondrejs-mac:~ administrator$ sudo vim
Password:
OTP: 123456
Sorry, try again.
Password:
OTP: 775279
ondrejs-mac:~ administrator$
```

Incorporating the PAM module into Desktop Logins

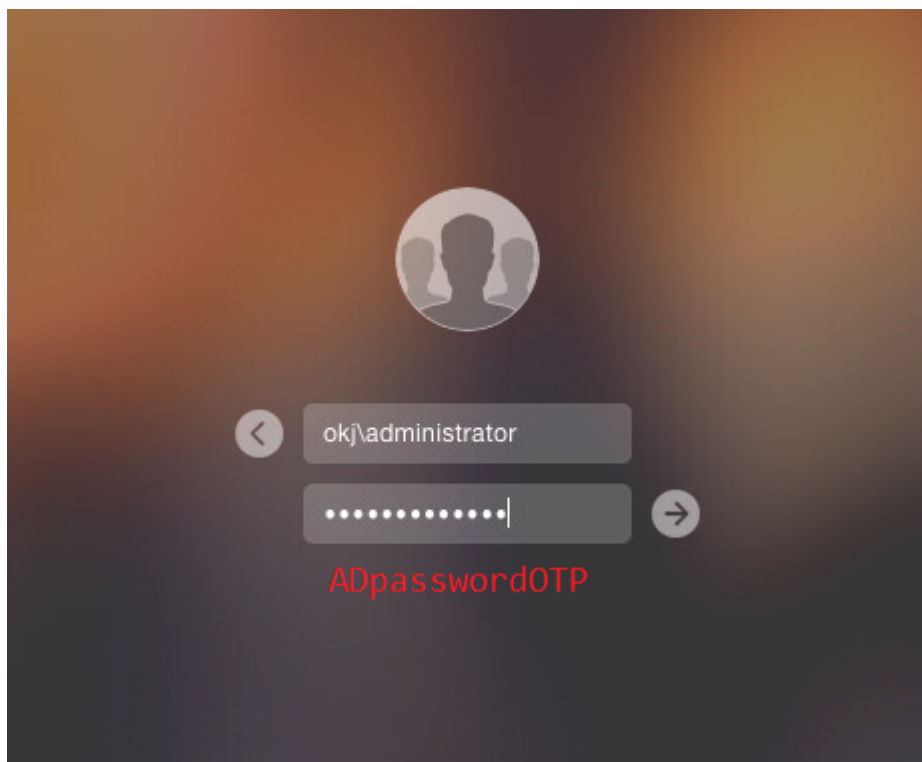
For Desktop login, we cannot use RADIUS Accept-Challenge like the VPN Type when configuring the RADIUS client in the ESA Management Tool. The RADIUS client configuration should be as shown in the **VPN Type - VPN does not validate AD username and password** section of the [Other RADIUS configurations](#) 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.



9.2 Linux - configuration

The steps described here were accomplished on OpenSUSE Leap 42.1.



Non-2FA users

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.



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 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:

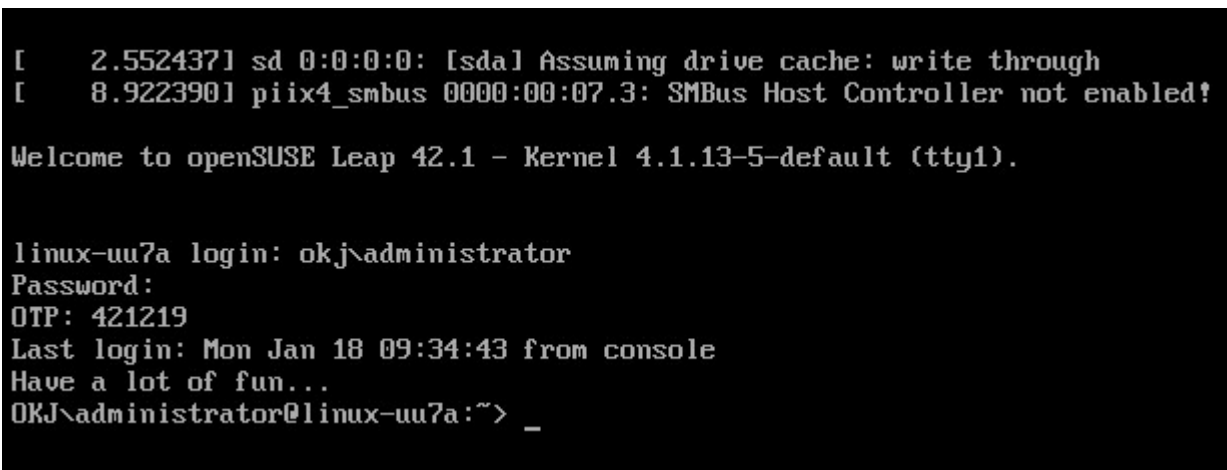
```
auth required /lib/security/pam_radius_auth.so
```

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).

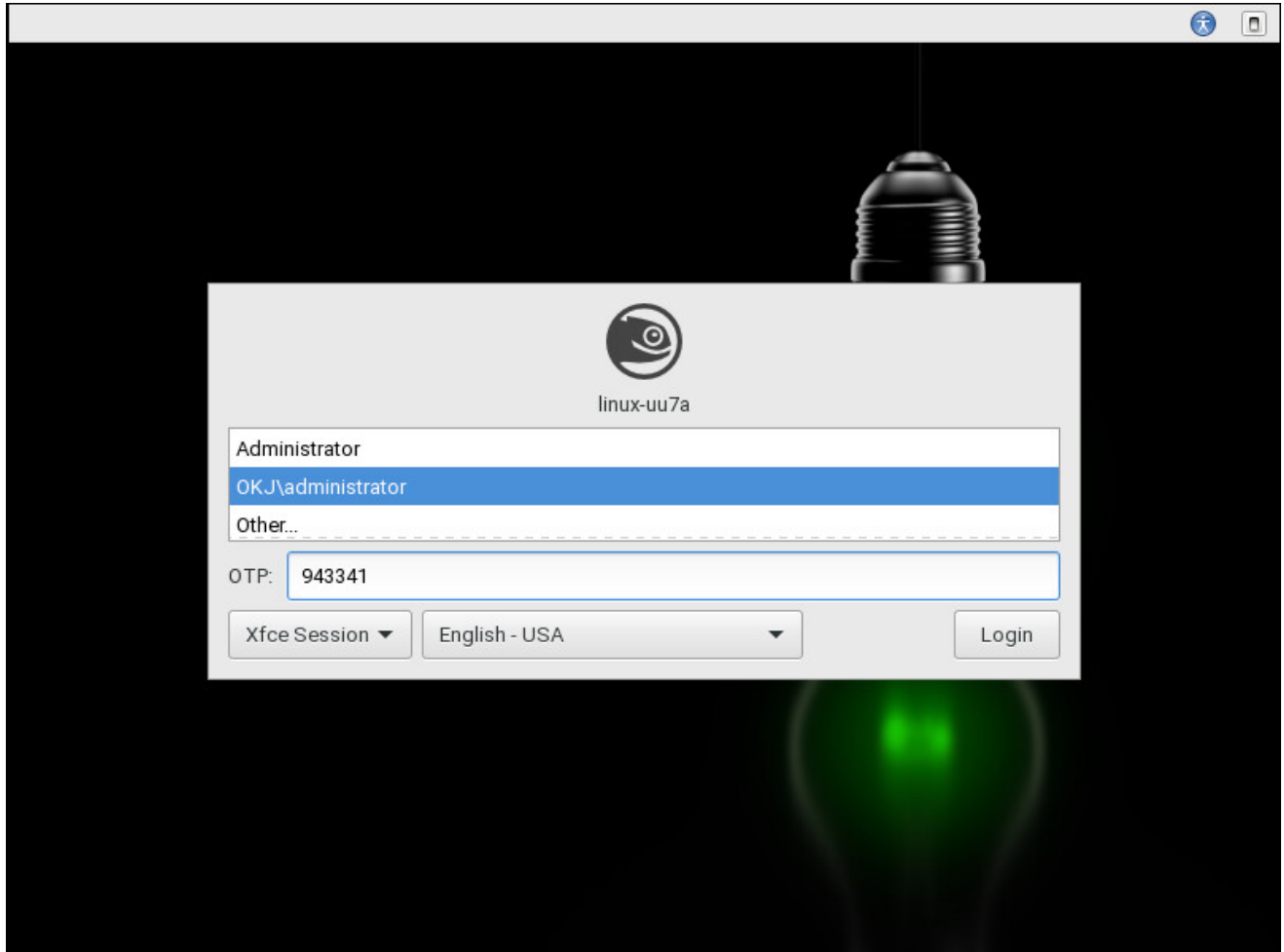
linux-uu7a login: okj\administrator
Password:
OTP: 421219
Last login: Mon Jan 18 09:34:43 from console
Have a lot of fun...
OKJ\administrator@linux-uu7a:~> _
```

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:



9.3 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:

UnixPAM (ACS-WINSRV2012) - Details

Identification:

Name:

IP Address:

Shared Secret: Show secret

VPN Type:

Authentication Methods:

- SMS-based OTPs
 - On-demand SMS OTPs
- Mobile Application OTPs
 - Compound Authentication (passwordOTP)
- Hard Token OTPs
 - Compound Authentication (passwordOTP)
- Mobile Application Push
- Active Directory passwords without 2FA

Access Control:

Restrict access to:

Realm:

SAVE DELETE CLOSE

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

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

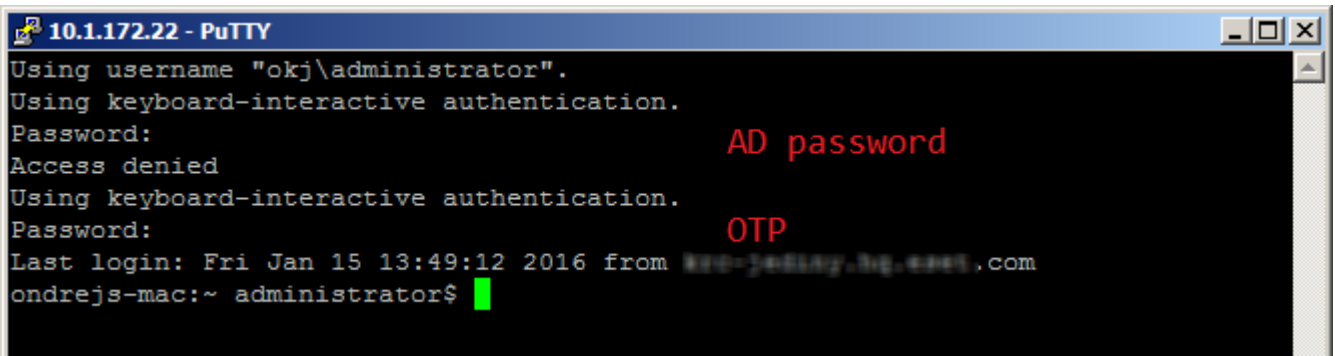
and comment (place a # tag at the beginning) all the other auth lines.



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

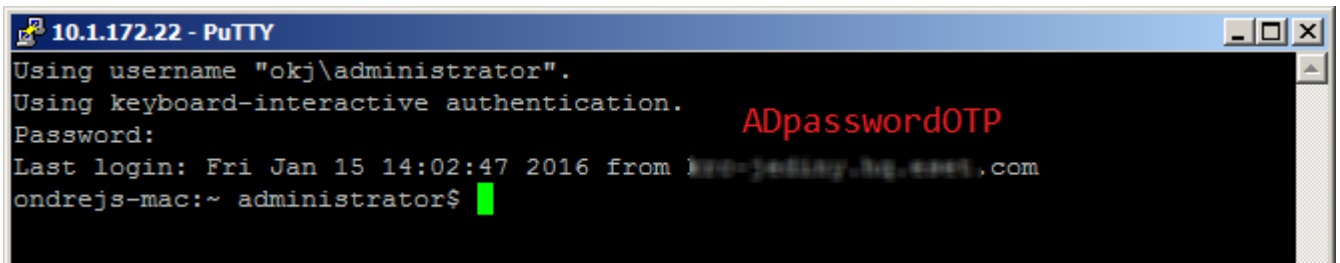
In this case a SSH login process would look like this:

- 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:

UnixPAM (ACS-WINSRV2012) - Details
✕

Identification:

Name:

IP Address:

Shared Secret: Show secret

VPN Type:

Authentication Methods:

SMS-based OTPs

On-demand SMS OTPs

Mobile Application OTPs

Compound Authentication (passwordOTP)

Hard Token OTPs

Compound Authentication (passwordOTP)

Mobile Application Push

Active Directory passwords without 2FA

Access Control:

Restrict access to:

Realm:

Warning (SMS): A user may be able to log in without entering a password if this setting is used incorrectly. Consult the relevant integration guide. Warning (Mobile): Mobile Application PINs are not currently enforced. A user could log in without entering a password or PIN. Warning (Hard Token): A user may be able to log in without entering a password if the RADIUS client does not check the credentials by itself. Consult the relevant integration guide.

When configuring RADIUS in this manner, add the following line in `/etc/pam.d/sshd` (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 kzo-jediny.bg.eset.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 kzo-jediny.bg.eset.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/sshd` (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

10. 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 or prompted to approve the push notification. The user will only be allowed access to the Web Application if a valid OTP is entered or the push notification is approved.

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

10.1 Configuration

The Web Application integration can be configured from the **Components** page of ESA Web Console. There you will see the list of [supported Web applications](#) for which ESA has been installed.

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.

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 Allow non 2FA 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.

10.2 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 plugins will not display the "Cancel" button.

ESET[™] SECURE AUTHENTICATION

Your One-Time Password (OTP):

Cancel

Log On

© 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.



- 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.
- c. If the user has installed the ESA mobile application on their phone and is allowed to use both OTP and Push authentication, the screen will indicate approval of a push notification or prompt the user for an OTP. Alternatively, the user can proceed to OTP authentication by taping **Enter OTP**.

The screenshot shows the ESET[™] SECURE AUTHENTICATION interface. At the top, the title "ESET[™] SECURE AUTHENTICATION" is displayed. Below the title, there is a horizontal line. On the right side of the screen, the text "Approve login" is shown in bold, followed by "ID: 141" in a larger, bold font. Below this, the instruction "Approve the login on your device or enter the OTP." is displayed. At the bottom of the screen, there are two buttons: "Enter OTP" and "Cancel".

5. If a push notification is approved or a valid OTP is entered, 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 the push notification is not approved in 2 minutes, the user will be redirected to a page requesting an OTP. 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):

Cancel

Log On

© 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.

If you want a custom logo to be displayed in the screen waiting to enter OTP ,or approve a notification instead of the default ESET Secure Authentication logo, follow the steps below. All the steps are performed on the computer where compatible ESA component ([Web App plugin](#), [ADFS protection](#)) is installed.

1. Save the desired logo as a .png image file. Recommended maximum dimension is 350px x 100px (width x height).
2. Place the logo to *C:\ProgramData\ESET Secure Authentication\Customization* and name it "*logo.png*".

11. 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 [Remote Desktop plugin of ESA 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.



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.

11.1 Configuration in an Active Directory environment

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.

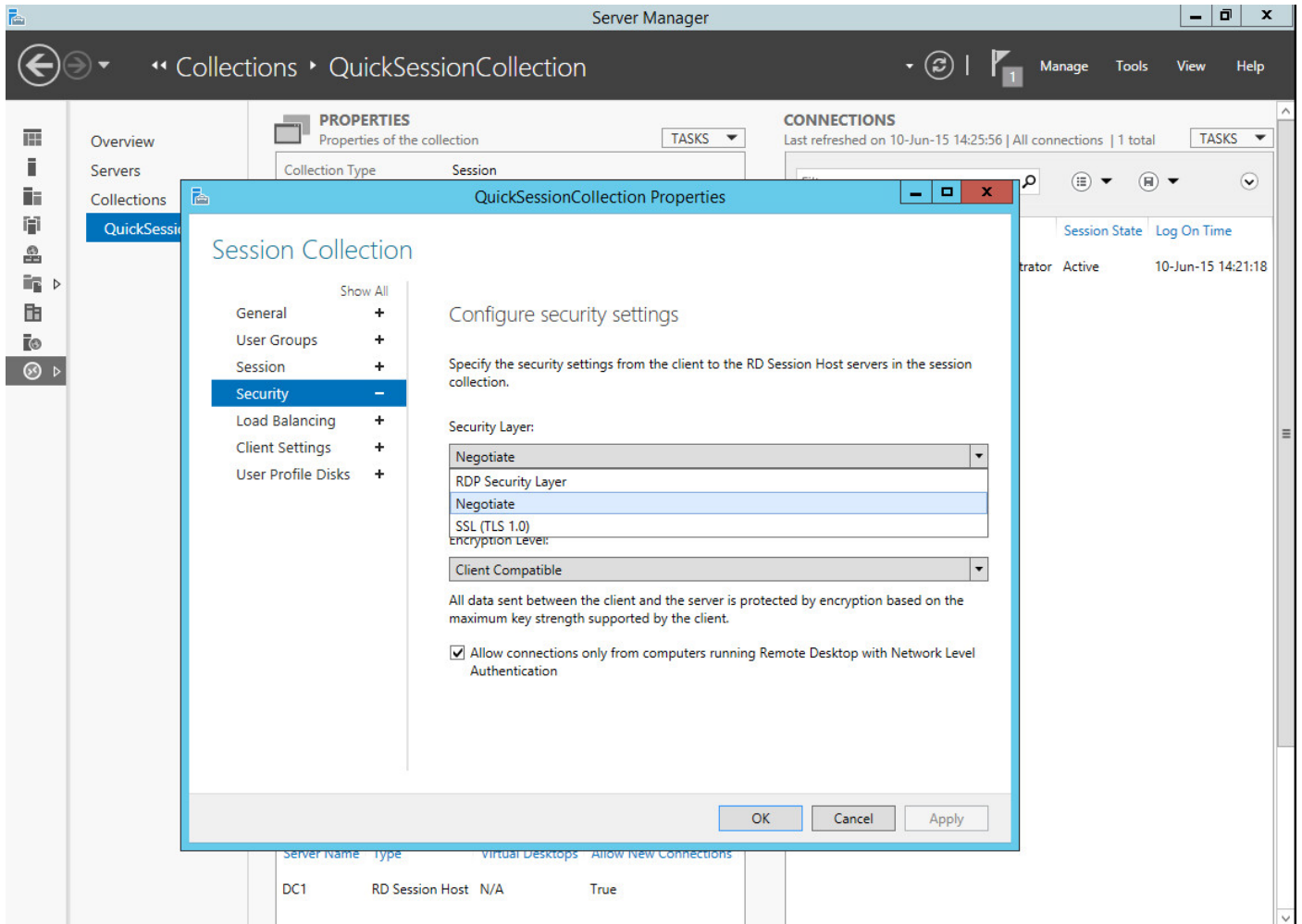
In order to use Remote Desktop protection, RD Session Host must be configured to use *SSL (TLS 1.0)* or *Negotiate*.

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*



11.2 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.

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.

To change the module configuration navigate in ESA Web Console to **Componentst**, click **RDP** and the **Computer list** window will appear listing all computers where Remote Desktop Protection of ESA is installed.

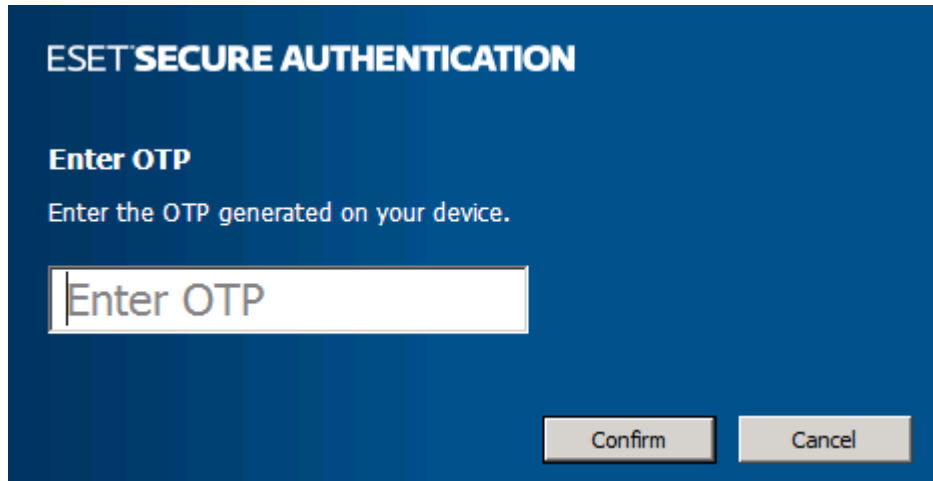
11.3 Usage

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

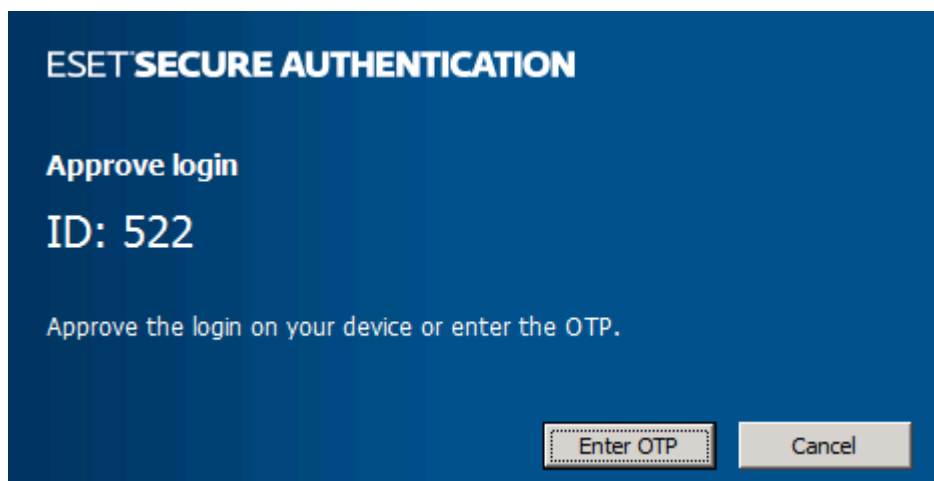
A user that has ESA 2FA enabled in the ESA Web Console, and has access to the remote computer, is required for testing. In an Active Directory environment, a domain user that has ESA 2FA enabled and is added as an allowed Remote Desktop user on the remote computer, is required for testing.

A computer that has Remote Desktop Access enabled is also required.

1. Connect to the remote computer using a Remote Desktop client, and authenticate as normal using the login credentials of the test user.
2. 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.
- c. If the user has installed the ESA mobile application on their phone and is allowed to use both OTP and Push authentication, the screen will indicate approval of the push notification. Alternatively the user can proceed to OTP authentication by clicking **Enter OTP**.



3. If a valid OTP is entered, then the user will be granted access to the computer they attempted to connect to.
4. 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.

11.4 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 Web Console navigate to **Settings > IP Whitelisting**.
2. Select the check-box next to **Allow access without 2FA from:**

3. Enter the localhost IP address: 127.0.0.1,::1 in the text box
4. Select the check-box next to **RDP**
5. Click **Save**.



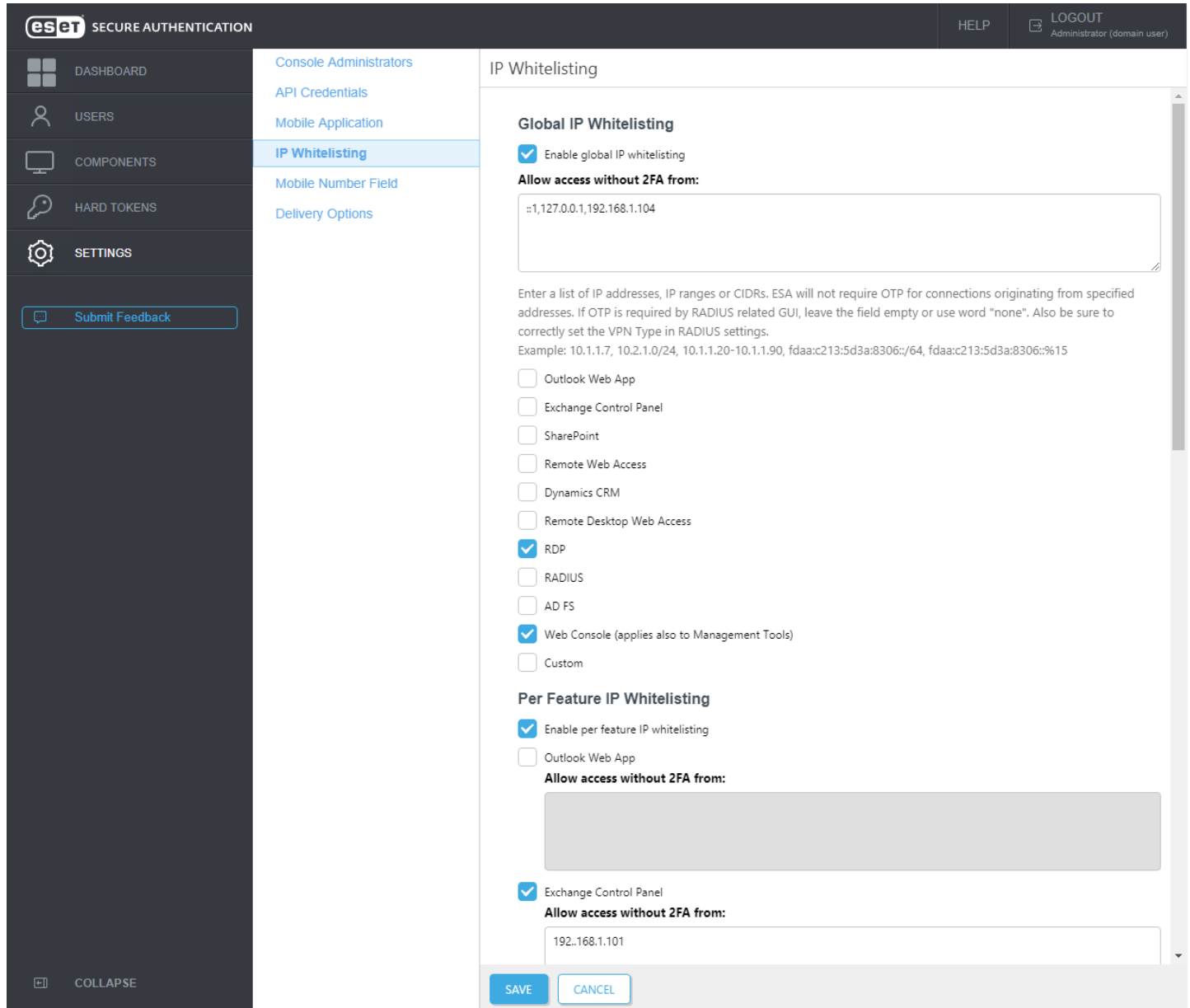
If RDWA is hosted on a different machine than ESA Authentication Server, you must whitelist the IP address of the RDWA host.

To make sure that you whitelist the correct IP address, look it up in the *Esa.Core.log* log file located at *C:\ProgramData\ESET Secure Authentication\Esa.Core.log*.

1. Clear the content of the log file.
2. Attempt to log in to RDWA with a user account protected by 2FA.
3. In that log file search for "_RDWeb".
4. A few rows below you should see a row saying "Starting two-factor authentication for user: *username* with ip *1.2.3.4*" where "1.2.3.4" will be replaced with the real IP address of your RDWA host.

12. 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 Web Console and navigate to **Settings > IP Whitelisting**.



The screenshot shows the ESET Secure Authentication console interface. The left sidebar contains navigation options: DASHBOARD, USERS, COMPONENTS, HARD TOKENS, and SETTINGS. The 'SETTINGS' section is expanded, showing a list of settings: Console Administrators, API Credentials, Mobile Application, IP Whitelisting (selected), Mobile Number Field, and Delivery Options. The main content area is titled 'IP Whitelisting' and contains the following configuration options:

- Global IP Whitelisting**
 - Enable global IP whitelisting
 - Allow access without 2FA from:**
 - Enter a list of IP addresses, IP ranges or CIDRs. ESA will not require OTP for connections originating from specified addresses. If OTP is required by RADIUS related GUI, leave the field empty or use word "none". Also be sure to correctly set the VPN Type in RADIUS settings.
Example: 10.1.1.7, 10.2.1.0/24, 10.1.1.20-10.1.1.90, fdac:c213:5d3a:8306::/64, fdac:c213:5d3a:8306::%15
 - Outlook Web App
 - Exchange Control Panel
 - SharePoint
 - Remote Web Access
 - Dynamics CRM
 - Remote Desktop Web Access
 - RDP
 - RADIUS
 - AD FS
 - Web Console (applies also to Management Tools)
 - Custom
- Per Feature IP Whitelisting**
 - Enable per feature IP whitelisting
 - Outlook Web App
 - Allow access without 2FA from:**
 - Exchange Control Panel
 - Allow access without 2FA from:**

At the bottom of the page, there are 'SAVE' and 'CANCEL' buttons.

Select the check box next to **Enable global IP whitelisting**, define the appropriate IP addresses (IPv6 version too, if applicable), select the services to whitelist and then click **Save**.

To define different whitelisting for specific [ESA components](#) along the global one, select the check box next to **Enable per feature IP whitelisting**, select the services to whitelist, define the appropriate IP addresses (IPv6 version too if applicable), and then click **Save**.

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](#) for **VPN Type** select **VPN validates AD username and password** and select the checkbox next to **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](#)

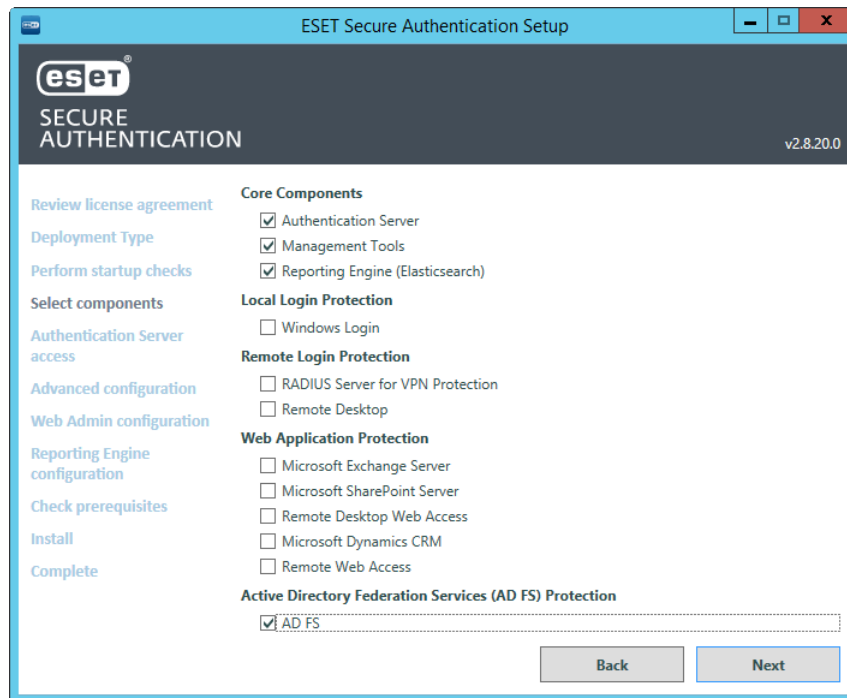
If these criteria are met, the user can access the VPN without entering a password or using the word **none** as password

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

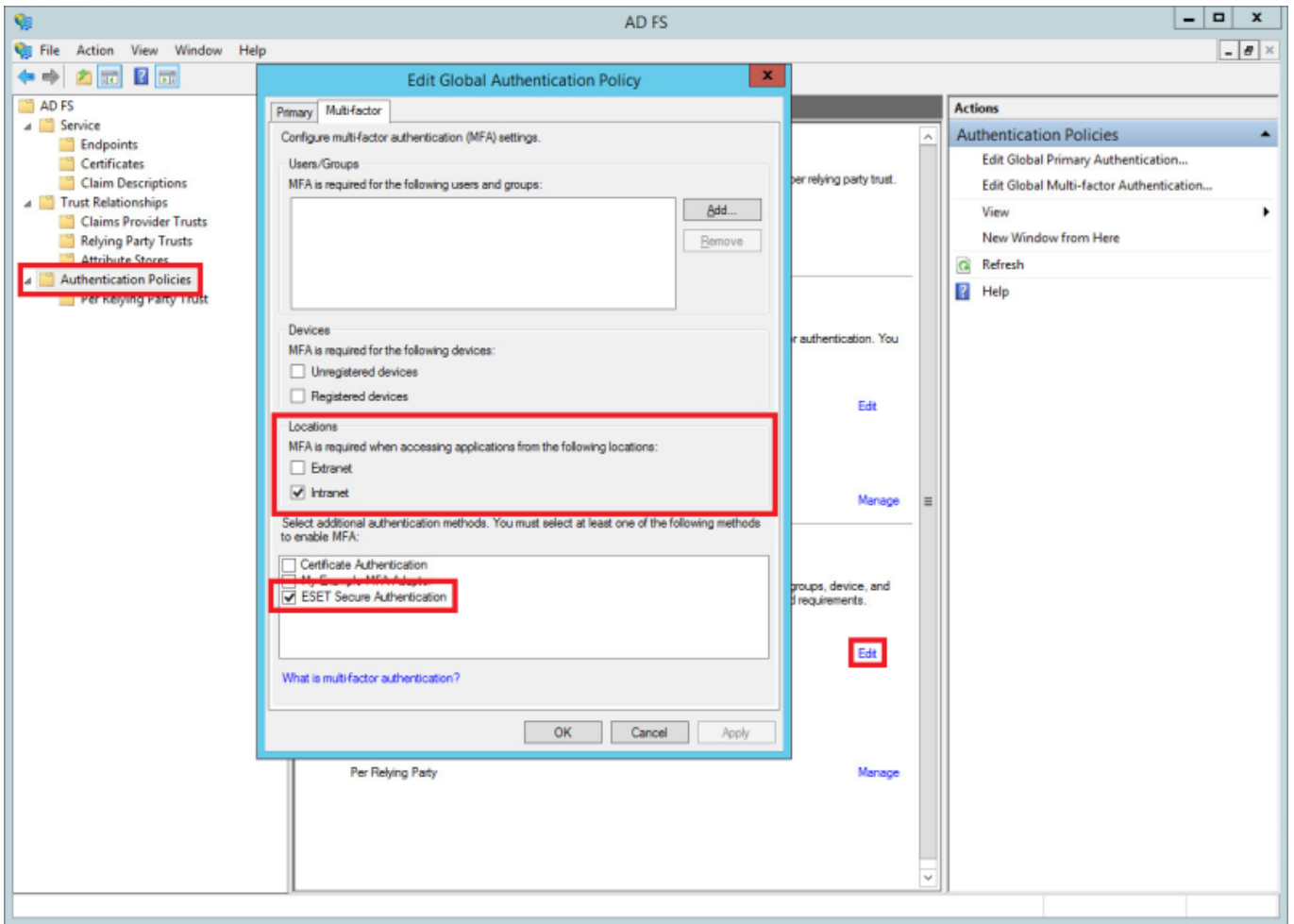
13. AD FS

ESA is a great choice for security if you are using Active Directory Federation Services (AD FS) 3 or 4 and want to secure it with 2FA.

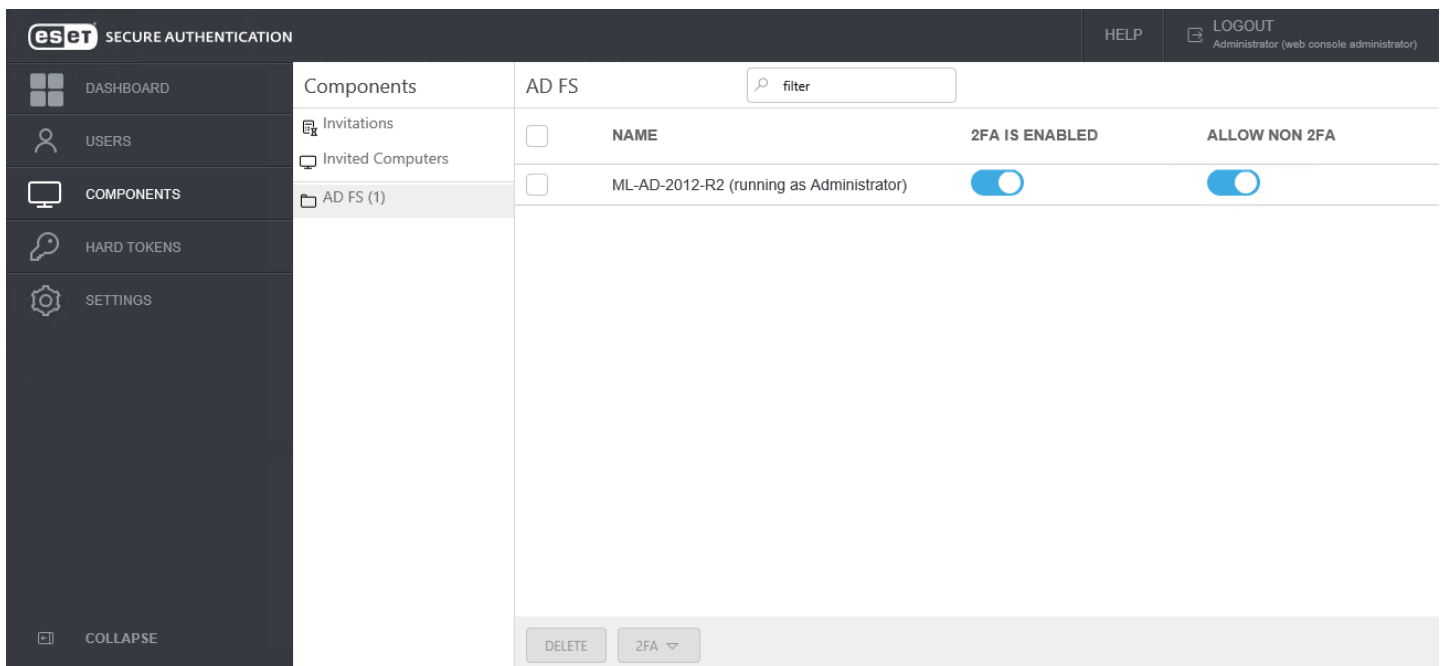
During the installation of ESA on the computer running AD FS, select the **AD FS** component and complete the installation.



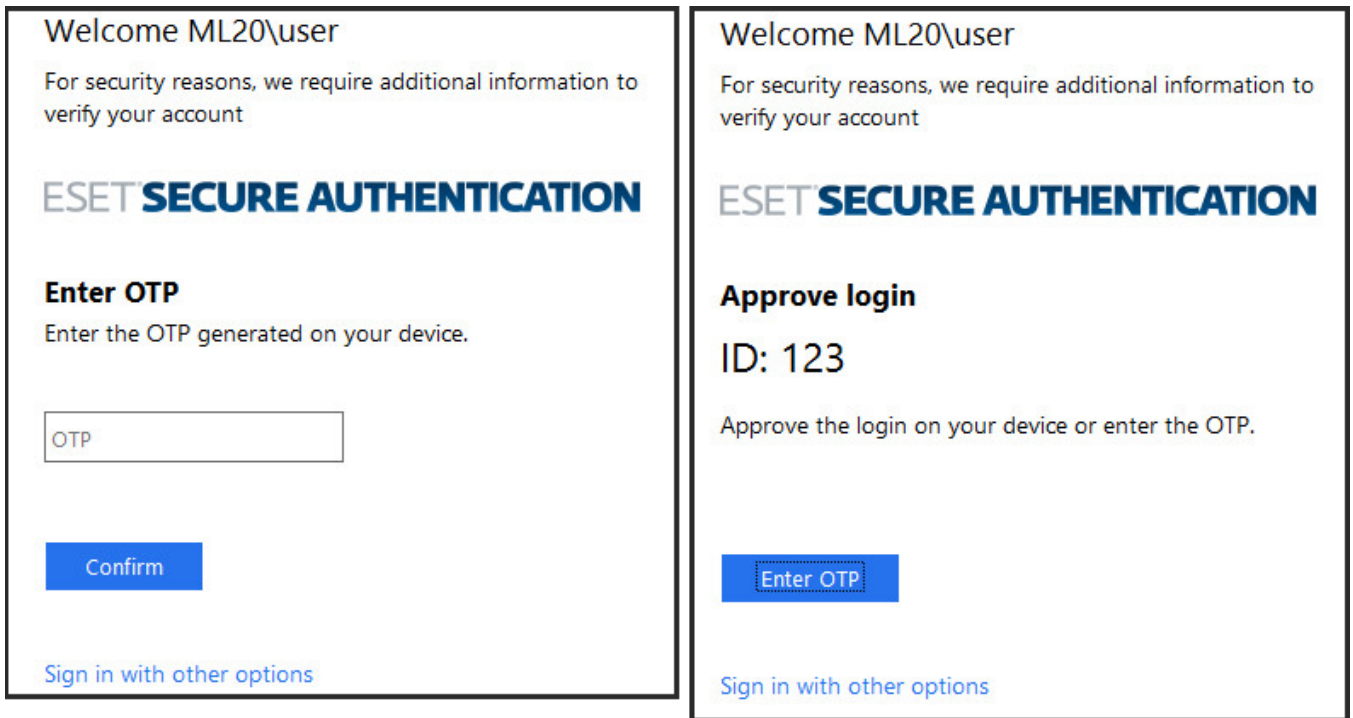
During the installation of AD FS configuration is modified - the ESET Secure Authentication authentication method is added and if no location is specified both Intranet and Extranet locations will be included. The image below shows the configuration changes with the **Intranet** location selected prior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



Once the installation is complete, open the ESA Web Console, navigate to **Components**, click **ADFS** and you will see the **2FA is enabled** and **Allow non 2FA** options enabled.



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



OTP required (on the left); Approval of push notification required (on the right)

If you want a custom logo to be displayed in the screen waiting to enter OTP, or approve a notification instead of the default ESET Secure Authentication logo, follow the steps below. All the steps are performed on the computer where compatible ESA component ([Web App plugin](#), [ADFS protection](#)) is installed.

1. Save the desired logo as a .png image file. Recommended maximum dimension is 350px x 100px (width x height).
2. Place the logo to `C:\ProgramData\ESET Secure Authentication\Customization\` and name it "logo.png".



Note

Along the [supported web browsers](#), Internet Explorer version 9 and 10 are also supported.

14. 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 on the same URL address as [ESA Web Console](#), but followed by `/apidoc` without quotation marks. For example, if the ESA Web Console is available at <https://120.0.0.1:8001/>, the API documentation is available at <https://127.0.0.1:8001/apidoc>

What is new in API for ESET Secure Authentication 2.8

- Managing ESET Secure Authentication settings
- Managing users
- More authentication options: [MRK](#), whitelisting, [Push Authentication](#)
- [Self-enrollment](#)
- Support of user realms: users from another domain, non-domain users

14.1 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 Auth API) is for user authentication and the second endpoint (the 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, unless you changed the port during [installation of Authentication Server](#).

The authentication API is available on URLs of the form <https://127.0.0.1:8001/auth/v2/> and the Management API is available on URLs of the form <https://127.0.0.1:8001/manage/v2/>. Both endpoints are protected from unauthorized access via standard HTTP Basic Authentication, requiring a valid set of API Credentials before processing any request.

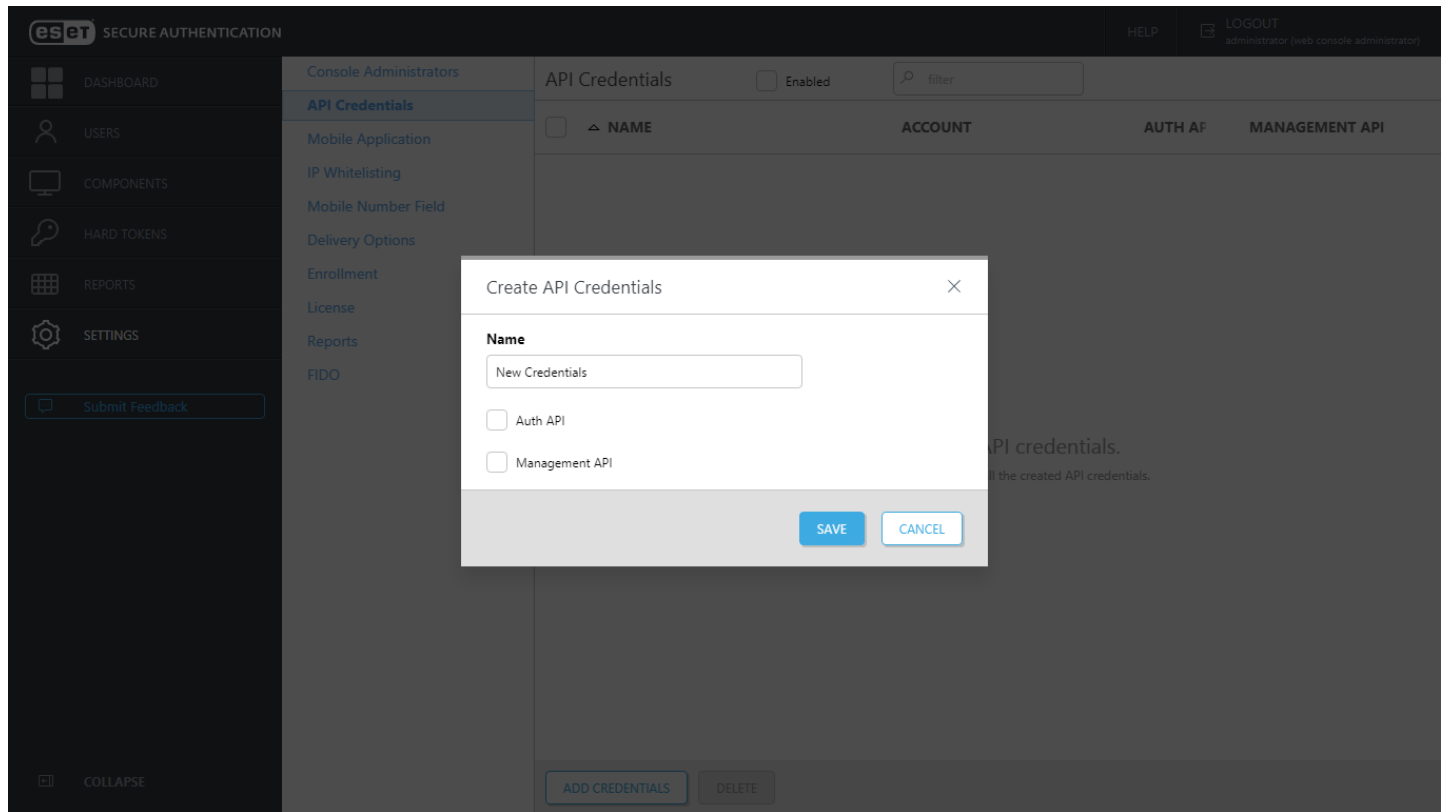
The ESET Secure Authentication installer automatically uses an appropriate SSL security certificate installed on the machine, or generates a new self-signed certificate if another cannot be found.

14.2 Configuration

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

Enabling API and configuring API credentials in ESA Web Console

1. Launch the ESET Secure Authentication Web Console and navigate to the **Settings > API Credentials**.
2. Select the **Enabled** check box. Save the changes.
3. Click the **Add Credentials** action to create a new set of credentials.



Enter the desired name, select the **Auth API** or **Management API** check box or both. Click **Save**.

4. The account ID and password displays.



Be sure to save the password securely, it cannot be displayed again.

Enabling API and configuring API credentials in MMC Console

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 Server component installed will respond to authorized API requests after they are restarted. There is no need to restart the ESACore service when credentials are created or deleted.

14.3 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.

Prerequisites

In order to follow this guide you will need:

- An installation of the ESA Authentication Server 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



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

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):
 - a. Start -> Type "mmc.exe" and press the **Enter** key
2. Add the Certificates snap-in:
 - a. Click **File** -> **Add/Remove Snap-in**
 - b. Select **Certificates** from the left-hand column
 - c. Click the **Add** button
 - d. Select **Computer account**
 - e. Click **Next**
 - f. Select **Local computer**
 - g. Click **Finish**
 - h. 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.

Replacing the ESA Certificate



The ESACore (Authentication Server) service will not start up without a certificate configured. If you remove the certificate, you must add another before the ESACore 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 2008+

1. Click **Start -> Type "cmd.exe"**.
2. In the list of programs, right-click the **cmd.exe** item and select **Run as administrator**.
3. Type **"netsh http show sslcert ipport=0.0.0.0:8001"** and press the **Enter** key.
4. Copy and paste the **Certificate Hash** field somewhere safe, in case you want to re-add the existing certificate.
5. Type **"netsh http delete sslcert ipport=0.0.0.0:8001"** and press the **Enter** key.
6. You should see **SSL Certificate successfully deleted**.
7. 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.
8. You should see **SSL Certificate successfully added**.
9. Restart the ESACore service for the new certificate to take effect.

14.4 Generate custom SSL Certificate

The following steps describe the process of generating a custom SSL certificate of your choosing and importing it to the essential stores on Windows Server 2012 R2.

1. Open **Window PowerShell**.
2. Execute the following commands:
 - a. `$customcertificate = New-SelfSignedCertificate -DnsName "<FQDN>" -CertStoreLocation "cert:\localmachine\my"`

In the command above, replace **<FQDN>** with the corresponding version of subject name you can see in ESA Web Console at **Components > Invitations > Server info**.

b. `$exportpassword = ConvertTo-SecureString -String '<password>' -Force -AsPlainText`

In the command above, replace <password> with a password of your choice.

c. `$certPath = 'cert:\localMachine\my\' + $customcertificate.thumbprint`

d. `Export-PfxCertificate -cert $certPath -FilePath $env:USERPROFILE\Desktop\ESACustomCertificate.pfx -Password $exportpassword`

This final command will place the `ESACustomCertificate.pfx` certificate on your desktop.

3. Press the *Windows key + R* keyboard shortcut to open the **Run** dialog.
4. Type `mmc`, and press **Enter** to open MMC.
 - a. Navigate to **File > Add/Remove Snap-in**.
 - b. Select **Certificates > Add**.
 - c. Select **Computer Account**, click **Next**, then click **Finish**. Click **OK** to close the Add or Remove Snap-ins window.
5. In the left pane of MMC expand **Certificates (Local Computer) > Personal**, and right-click **Certificates**.
6. Select **All Tasks > Import...**
 - a. In the import wizard click **Next**, click **Browse**, from the file extension list-box select "Personal Information Exchange (*.pfx, *.p12)", locate the exported certificate file, click **Open**, and then click **Next**.
 - b. Enter the password used in command no. 2 and click **Next**.
 - c. Make sure the **Place all certificates in the following store** is selected and the defined store name is "Personal". Click **Next** and click **Finish**.
7. In the left pane of MMC expand **Certificates (Local Computer) > Trusted Root Certification Authorities**, and right-click **Certificates**.
8. Select **All Tasks > Import...**, and repeat steps 6a to 6c.
9. Double-click the certificate in **Certificates (Local Computer) > Personal > Certificates** and make sure the line **You have a private key that corresponds to this certificate** is displayed.

15. Auditing and Licensing

15.1 Reports

To be able to use the **Reports** screen in the ESA Web Console, it is essential to have an [Elasticsearch installation](#) available.

The Reports will display:

- Everything the [Audit log](#) includes
- Provisioning of users
- Self-enrollment activity
- Sent SMS OTPs
- Error messages
- ESA Web Console actions

The Reports screen provides various filtering options.

- **Date**—Today, Last 7 Days, This Month, This Year, Custom Date
- **Presets**—All Authentications, Auto Register Users, Denied Authentications, Provision Users, Sent SMS OTPs, Successful Authentications
- **Custom filter**—Click **Select** to reveal the available list of custom filtering options. You can combine the available filtering options.

TIME	EVENT	RESULT	CALLER	USER	COMPONENT	INFO
3/14/2019, 10:58:28 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/14/2019, 10:30:12 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/14/2019, 9:45:08 AM	Set Core Setting	Success	a (web console administr...			self_enrollment_enabled: -> True
3/14/2019, 9:26:09 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/14/2019, 9:23:02 AM	Error					Error while executing command with l...
3/14/2019, 9:23:02 AM	Error					Error while executing command with l...

Example - filter successful Web Console logins

1. Click **Select** in the custom filter window, select **Event**.
2. Click the **Event** box, select **Web Console Login**. You can start typing "Web" and it will show available options matching that string.
3. Click an empty area in the custom filter box, select **Result**.

4. Click the **Result** box, select **Success**.

5. Click **Apply**.

Reports - Showing 21 filtered items.

Result: Success

Top actions

Web Console Login Register Component License Activation License Activation Start Set Core Setting

TIME	EVENT	RESULT	CALLER	USER	COMPONENT	INFO
3/14/2019, 9:45:08 AM	Set Core Setting	Success	a (web console administr...			self_enrollment_enabled: -> True
3/14/2019, 9:26:09 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/14/2019, 7:29:41 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/13/2019, 12:11:11 PM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/13/2019, 11:58:41 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...
3/13/2019, 10:51:25 AM	Web Console Login	Success	ML20\ESASrv_MLAD201...	a (Web Console)	Web Console (ESA Server)	user_type: web admin credentials, user...

REFRESH EXPORT

Click **Export** to save the filtered reports to a .csv file.

15.2 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.

If you [install the Reporting Engine \(Elasticsearch\)](#), you can view these logs in the **Reports** screen of ESA Web Console.

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.

15.3 License Overview

Your ESA license has three parameters:

- License Validity
- Users
- OTP 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.

Warnings are communicated to the ESA Administrator in the **Dashboard** section of ESA Web Console.

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

15.4 License States

The full license state is displayed in the **License** tile in the **Dashboard** screen of ESA Web Console. Review the following ESA server license states:

- **OK:** All license parameters are within the prescribed limits
- **Warning:** At least one license parameter is close to the allowed limit
- **SMS Credits Expired:** SMS credits have run out and no OTP or Provisioning SMSes will be sent.
- **Violation (full functionality):** One of the licensed parameters has exceeded allowed limits, but no enforcement is imposed
- **Violation (limited functionality):** A license parameter has been exceeded for more than 7 days, certain user management functions are disabled
- **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	No more than 7 days after expiration	more than 7 days after expiration	more than 30 days after expiration
User count	less than 10% or 10 seats available, whichever is lowest	N/A	Active users exceed licensed users	more than 7 days after active users exceed license	Never
SMS Credits	less than 10 SMS credits remaining	0 SMS credits remain	Never	Never	Never

15.5 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).

	ESA Not Activated	OK	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
Enable Users for 2FA	Disabled	Allowed	Allowed	Allowed	Allowed	Disabled	Disabled
Provision Users	Disabled	Allowed	Allowed	Disabled	Allowed	Disabled	Disabled
Authenticate with SMS OTP	Disabled	Allowed	Allowed	Disabled	Allowed	Allowed	Disabled
Authenticate with mobile app (OTP, Push)	Disabled	Allowed	Allowed	Allowed	Allowed	Allowed	Disabled
Authenticate with hard token	Disabled	Allowed	Allowed	Allowed	Allowed	Allowed	Disabled
Manage system configuration	Disabled	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
Disable Users for 2FA	Disable	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed

16. High Availability View

When utilizing the Active Directory Integration deployment type in an [AD](#) environment, all installed servers are displayed in the **Servers** tile of the **Dashboard** screen in the ESA Web Console. When more than one core service is detected on the network, all servers are displayed.

Servers		
ENDPOINT	STATUS	VERSION
win-s2012-2.acswin2012.com:8000	Inactive	2.7.29.0
acs-winsrv2012.acswin2012.com:8000	Active	2.7.29.0

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.

17. Troubleshooting

If you experience installation or system issues with ESET Secure Authentication, and you have a case open with ESET Technical Support, you may be asked to provide logs from your computer. See our guide on collecting logs: <https://support.eset.com/kb6845/>

Troubleshoot other issues using the following operations:

- [Domain authentication](#)
- [Connection to RADIUS server](#)
- [Configuration of VPN to connect to RADIUS](#)
- [Login via RDP secured by 2FA \(installation of Remote Desktop plugin\)](#)

18. Glossary

2FA - Two-factor authentication

AD - Active Directory

ADI - Active Directory Integration

ADUC - Active Directory Users and Computers management interface

COS - Client operating system

ESA - ESET Secure Authentication

ESA component - [Windows Login plugin](#), [Remote Desktop plugin](#), [Web App plugin](#), [ADFS protection](#)

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

FQDN - Fully qualified domain name

GPO - [Group Policy Object](#)

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.

OS - Operating System.

OTP - an one time password with limited time validity

Mobile Application Push - push notification 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