ESET Secure Authentication

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

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

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 4/15/2024

Overview

ESET Secure Authentication (ESA) adds Two Factor Authentication (2FA) to Microsoft Active Directory domains or local area network, meaning a one-time password (OTP) is generated and provided along with 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 after the user has successfully authenticated using their general access credentials.

Push notifications require Android 4.1 and later, along with Google Play services 10.2.6 and later, or iOS.

The ESA product consists of the following components:

- The Windows Login plug-in provides 2FA for Windows computers
- The Remote Desktop plug-in provides 2FA for the Remote Desktop Protocol
- The RADIUS Server for VPN Protection adds 2FA to VPN authentication
- The Web Application plug-ins provide 2FA to various Microsoft Web Applications
- The AD FS plug-in provides 2FA for Active Directory Federation Services
- The Identity Provider Connector
- The ESA Authentication Server 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 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 or 2.8.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, allow accessing the Web Console (also applies to Management Tools) through IP address whitelisting, or 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 Web Console.

        - ESA Web Console, an all-in-one management tool, is the preferred way 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.

Changelogs

To update to a later version, see upgrade installation.

Requirements

An Active Directory domain, local area network or publicly available Authentication Server 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 installing ESA in Active Directory Integration mode.

If you use a custom DNS in your Active Directory environment, you must create an SRV record in your DNS before 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 Authentication Server installation. 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.

If installing ESA in Standalone mode, ensure ESA components and the Authentication Server will see (ping) each other.

> **Limited support for end-of-life third-party products**
> ESET Secure Authentication provides limited support for compatible third-party products that reached the end of their support lifecycle.

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 (server OS)

- Windows Server 2008 *
- Windows Server 2008 R2 SP1*
- 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
- Windows Server 2022

* Change the default TLS version to use

Client operating systems (client OS)

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10 (including 22H2 Update)
- Windows 11 (including 23H2 Update)

RADIUS Server on Windows Small Business Server

When you install a RADIUS Server on Windows Small Business Server 2008 or 2011, change the default NPS port from 1812 to 1645. Verify that no processes are listening on port 1812 before installing ESA by running the following command: `C:\> netstat -a -p udp | more`
Alternatively, when installing ESA RADIUS, change the RADIUS port in the **Advanced configuration** screen.

ℹ ESA Core and RADIUS on a client operating system (client OS)

Installing ESA Core (Authentication Server) and RADIUS Server on a client OS 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 client OS may present other limitations (for instance, the number of maximum concurrent TCP connections) compared to an server OS.

Supported CPU platforms

- x86
- x64

Deprecated TLS 1.0 and 1.1

As of March 31, 2020, Transport Layer Security (TLS) versions 1.0 and 1.1 are no longer supported.

If the Authentication Server runs on Windows Server 2008 or Windows Server 2008 R2, it uses old TLS by default. To use TLS 1.2, you have to install all available Windows updates first, then edit the Registry.

To edit the Registry:

1. Click **Start** > **Run**.
2. Type `regedit` in the **Open** box, then click **OK**.
3. In the **Registry Editor**, expand **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > SecurityProviders > SCHANNEL > Protocols > TLS 1.2 > Server**.
4. In the menu, click **Edit**, select **New > DWORD value**.
5. Name it `DisabledByDefault`, press **Enter**.
6. Double-click the `DisabledByDefault` entry, make sure **Value data** is set to 0. Click **OK**.
7. Close the Registry Editor and restart the operating system.

Supported Web Browsers and Resolution regarding ESA Web Console

The 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

Functional details

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.

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
- Microsoft Exchange 2019
    - Outlook Web App - Exchange Mailbox Server Role (MBX)
    - Exchange Admin Center

Where is 2FA applicable

ESA adds 2FA protection only to the 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.

- 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 2019
- Microsoft SharePoint Foundation 2010
- Microsoft SharePoint Foundation 2013
- Microsoft Remote Desktop Web Access
- Microsoft Terminal Services Web Access
- Microsoft Remote Web Access

> i Internet Explorer
> Internet Explorer version 9 and 10 are supported web browsers.

Supported Mobile Phone Operating Systems

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

- iOS 12 to iOS 17
- Android 4.4 to Android 14 - Google Play Services 10.2.6 are required for push notifications.
    - The permission to access the camera and flashlight is required to scan the QR code

Installation Requirements

Quick links: Installation access rights, ESA components in a distributed environment, Prerequisites of each component, .NET requirements, DB requirements in Standalone mode

Installation requires outbound connectivity to esa.eset.com on TCP port 443 and the licensing servers.

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.

Windows Firewall exceptions 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 essential exceptions that you will need to create.

Installation access rights:

- Active Directory environment:
    - Domain administration rights: The installer must be run by a member of the "Domain Administrators" security group or by a user with administrator privileges.

Domain administration rights can be omitted when installing/uninstalling ESA Components in an AD environment via .MSI installer using command line parameters. In this case, use the `NO_DOMAIN_ADMIN_MODE=1` parameter and then check the installation logs for further instructions marked as "Manual configuration needed.

oSchema extension rights: Essential when installing the Authentication Server. The installer must be run by a user member of the "Schema Admins" security group.

- Standalone deployment:

oLocal administrator rights

ESA components in a distributed environment:

ESA supports the installation of components in a distributed environment. Available models:

- Authentication Server (AS) installed in *Active Directory Integration* mode

oComponents installed in *Active Directory Integration* mode must be within the same domain, and they connect to AS automatically

oComponents installed in *Standalone* mode connect to AS via invitations

- Authentication Server (AS) installed in *Standalone* mode

oComponents must be installed in *Standalone* mode, and they connect to AS via invitations

Table of compatibility of ESA Components and Supported Operating Systems

Prerequisites for each component installation:

- **Authentication Server**:

oWindows Server 2008 or later server OS in the list of Supported Operating Systems

- **Management Tools**:

oWindows7 or later client OS in the list of Supported Operating Systems, Windows Server 2008 or later server OS in the list of Supported Operating Systems

o.NET Framework version 3.5

oWindows Remote Server Administration Tools, Active Directory Domain Services component (RSAT AD DS)

> RSAT
>
> RSAT was previously known as the Remote Administration Pack (adminpack) and is downloadable from Microsoft. In Windows Server 2008 and later, you can install this component through the **Add Feature** wizard in the **Server Manager**. All Domain Controllers already have these components installed.

- **Reporting Engine (Elasticsearch)**:

oWindows7 or later client OS in the list of Supported Operating Systems, Windows Server 2008 or later server OS in the list of Supported Operating Systems

oServer JRE (Java SE Runtime Environment) version 1.8.0_131 and later versions of 1.8.x, Java SE 11, or OpenJDK 11 or 13

oJAVA_HOME and PATH system environment variables contain the path to your installation of Server JRE or OpenJDK

o.NET Framework version 4.7.2

o2GB free RAM

- **Identity Provider Connector**:

  oWindows7 or later client OS in the list of Supported Operating Systems, Windows Server 2008 R2 or later server OS in the list of Supported Operating Systems

  oIIS 7 or later with ASP.NET Framework version 4.7.2

- **RADIUS Server**:

  oWindows7 or later client OS in the list of Supported Operating Systems, Windows Server 2008 or later server OS in the list of Supported Operating Systems

- **Web App Plug-in for Microsoft Exchange Server**:

  oMicrosoft Exchange Server 2007 or later (64-bit only), with the Client Access role (Outlook Web App / Outlook Web Access) installed

  o.NET Framework version 3.5

  oInternet Information Services 7 (IIS7) or later

- **Web App Plug-in for Microsoft SharePoint Server**:

  oMicrosoft SharePoint Server 2010, 2013, 2016, 2019 (64-bit only)

  oMicrosoft SharePoint Server 2010, 2013 Foundation (64-bit only)

  o.NET Framework version 4.5

- **Web App Plug-in for Microsoft Dynamics CRM**:

  oMicrosoft Dynamics CRM 2011, 2013, 2015 or 2016

  o.NET Framework version 4.5

- **Web App Plug-in for Microsoft Terminal Services Web Access**:

  oThe Terminal Services role with the Terminal Services role service installed on Windows Server 2008 R2

  o.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 server OS 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, Windows Server 2012 Essentials R2 and Windows Server 2016 Essentials

  - .NET Framework version 4.5

- **Remote Desktop Protection**:
  - Windows Server 2008 R2 or later server OS in the list of Supported Operating Systems
  - Microsoft Windows 7 or later client OS in the list of Supported Operating Systems
  - Only 64-bit operating systems are supported
- **Windows login protection**:
  - Windows Server 2008 R2 or later server OS in the list of Supported Operating Systems
  - Windows 7 or later client OS in the list of Supported Operating Systems
- **AD FS protection**:
  - Windows Server 2012 R2 or later server OS in the list of Supported Operating Systems

.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
- Identity Provider Connector: .NET Framework version 4.6.2

ESA Core and RADIUS on a client operating system (client OS)

Installing ESA Core (Authentication Server) and RADIUS Server on a client OS 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 client OS may present other limitations (for instance, the number of maximum concurrent TCP connections) compared to an server OS.

Database requirements in Standalone mode:

If the Authentication Server is installed in Standalone mode, it uses a built-in database by default. If you prefer an external database, the minimum database requirements are:

- Microsoft SQL / Microsoft SQL Express 2012 (11.0.2100.60)

- Postgre SQL 9.4.24

ESA components and OS compatibility

The following table displays the supported Windows operating systems for each ESET Secure Authentication component.

See installation requirements for further details.

Server operating systems

	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012	Windows Server 2012 R2	Windows SBS 2008	Windows SBS 2011	Windows Server 2012 Essentials	Windows Server 2012 R2 Essentials	Windows Server 2016	Windows Server 2016 Essentials	Windows Server 2019	Windows Server 2019 Essentials	Windows Server 2022
Authentication Server	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Management Tools	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Reporting Engine (Elasticsearch)	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
RADIUS Server	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Web App Plug-in for Microsoft Exchange Server	▯*	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Web App Plug-in for Microsoft SharePoint Server			✔	✔		✔	✔	✔	✔	✔	✔	✔	✔
Web App Plug-in for Microsoft Dynamics CRM			✔	✔		✔	✔	✔	✔	✔	✔	✔	✔
Web App Plug-in for Microsoft Remote Desktop Services Web Access	▯**	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔
Web App Plug-in for Microsoft Remote Web Access					✔	✔	✔	✔		✔			
Remote Desktop Protection		✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔
Windows login protection		✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔
AD FS				✔			✔	✔	✔	✔	✔	✔	✔
Identity Provider Connector		✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔

* 64-bit version of the operating system is required

** Microsoft Terminal Services on Windows Server 2008

Client operating systems

	Windows 7	Windows 8	Windows 8.1	Windows 10	Windows 11
Authentication Server	✔	✔	✔	✔	✔
Management Tools	✔	✔	✔	✔	✔
Reporting Engine (Elasticsearch)	✔	✔	✔	✔	✔
RADIUS Server	✔	✔	✔	✔	✔
Web App Plug-in for Microsoft Exchange Server *					

	Windows 7	Windows 8	Windows 8.1	Windows 10	Windows 11
Web App Plug-in for Microsoft SharePoint Server *					
Web App Plug-in for Microsoft Dynamics CRM					
Web App Plug-in for Microsoft Terminal Services Web Access					
Web App Plug-in for Microsoft Remote Desktop Services Web Access					
Web App Plug-in for Microsoft Remote Web Access					
Remote Desktop Protection*	✔	✔	✔	✔	✔
Windows login protection	✔	✔	✔	✔	✔
AD FS					
Identity Provider Connector	✔	✔	✔	✔	✔

* 64-bit version of the operating system is required

RADIUS Server on Windows Small Business Server

When you install a RADIUS Server on Windows Small Business Server 2008 or 2011, change the default NPS port from 1812 to 1645. Verify that no processes are listening on port 1812 before installing ESA by running the following command: `C:\> netstat -a -p udp | more`
Alternatively, when installing ESA RADIUS, change the RADIUS port in the **Advanced configuration** screen.

ESA Core and RADIUS on a client operating system (client OS)

Installing ESA Core (Authentication Server) and RADIUS Server on a client OS 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 client OS may present other limitations (for instance, the number of maximum concurrent TCP connections) compared to an server OS.

Performance recommendations

The performance of the Authentication Server may vary and depends on several factors.

Most important factors:

- Number or authentication requests per defined interval (average, but also peaks)
- Number of total user count
- Integration mode (**Active Directory Integration** or **Standalone**)
- Authentication method used
- Number of Authentication Servers used

- External databases used in case of **Standalone** integration mode
- HW and SW (OS) used in the whole ecosystem

It is impossible to define some single number representing the performance, but we tried to narrow the range of possible answers based on our tests.

Testing environment

Reference HW used for the Authentication Server (AS):

- CPU: 2,5 GHz, 8 Cores,
- RAM: 32GB
- Hard disk: SSD

Further details:

- One Authentication Server used
- External database on separate HW (similar to HW used for AS) when testing **Standalone** deployment type with an external database
- When testing **Active Directory Integration** mode, Domain Controller (DC) was on separate HW (similar to HW used for AS)
- Reporting Engine was not used during these tests

When comparing speed, the **Active Directory Integration** mode was the slowest in our tests, though it also depends on DC performance and some other parameters.

Standalone mode with a built-in database was as fast as if using an external database; however, a built-in database does not allow multiple Authentication Servers.

Standalone mode with external database is the most suitable for very large user bases.

Considering the performance described above, we have to consider what number of clients authenticate in what time interval.

For example, if all clients authenticate within one minute, then the **Standalone** mode with external database in our environment is ready to manage ~4800 clients.

Deployment type	Requests per second
Active Directory Integration mode	30
Standalone mode with built-in database	80
Standalone mode with an external database	80

However, if they authenticate evenly within one hour, it can theoretically manage more than 100.000.

The table below is based on the assumption that 10% of all clients authenticate in one minute and consider other deployment constraints.

If there is no ✓ in the table below, you may expect some performance issues unless you tune-up your environment.

User range	AD Integration mode	Standalone mode with built-in database	Standalone mode with an external database	Memory	HDD Storage
up to 5000	✓	✓	✓	450 MB	800 MB
5000 - 20000		✓	✓	1 GB	2 GB
more			✓		

*Assuming multiple Authentication Servers are used

Supported Active Directory Environments

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

Single Domain, Single Forest

The most straightforward 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 forest domains, but there is no cross-communication between the installations. There is no sharing of credentials across child and parent domains.

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. ESET Secure Authentication installations in separate domains are not aware of each other.

Benefits of installing ESA in Active Directory Integration mode

If you install the authentication server in **Active Directory Integration** mode:

- Users of the same domain are automatically visible in ESA Web Console
- ESA components within the same domain register automatically (no invitation needed)

Users and components form other domains

You can add users from other domains manually or import them using self-enrollment or synchronization with LDAP.

To add components from other domains, use invitations.

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, define the below exceptions in that firewall manually.

Exception Name: ESET Secure Authentication Core Service

- Scope: Any
- Protocol: TCP
- Local Port: 8000 and 8001
- 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

Policies

The information below applies only to Active Directory Integration mode.

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**, where the <computer name> is replaced with 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 a 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:

- Either press the **Windows key** ⊞ and **E** simultaneously so that the **File Explorer** shows up
- Or in the right pane, right-click **This PC** or **Computer** and select **Properties**.

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

Handling cloned computers

Suppose you want to have cloned computers in your network where ESET Secure Authentication (ESA) will be used. In that case, the attributes below must be unique for each computer to be protected by ESA.

- For correct registration of ESA components (Windows Login plugin, Remote Desktop plugin), which communicate in Active Directory Integration mode with the Authentication Server:
  - Computer name
  - Computer SID
  - Computer AD object SID
- For correct registration of ESA components (Windows Login plugin, Remote Desktop plugin) that are installed in Standalone mode:
  - Computer name
  - API username in *C:\ProgramData\ESET Secure Authentication\ESA.config*
- For correct registration of realms for local users:
  - Computer name
  - Computer SID

Use Microsoft's SysPrep tool to ensure unique attributes are applied to cloned computers.

1. In the SysPrep, use the **Generalize** option to create a generalized Windows image to be cloned later. Each image is configured during its first boot.
2. If the cloned computers are used in a domain:
   a.On the cloned machine, run the SysPrep tool.
   b.Reboot the computer.
   c.Connect the computer to the domain.
3. Install ESA (Windows Login plugin, Remote Desktop plugin) to each cloned computer either manually or through GPO.

IP addresses used by ESET Secure Authentication

ESET Secure Authentication connects automatically to the IP addresses listed in our knowledgebase article (sections ESET Data Framework, Services, ESET Secure Authentication Provisioning Server, ESET PROTECT) or below.

- 93.184.220.29 - Certificate revocation check based on publicly available Certificate Revocation Lists
- 23.42.27.27 - Certificate revocation check regarding EXE/DLL signatures

Installation

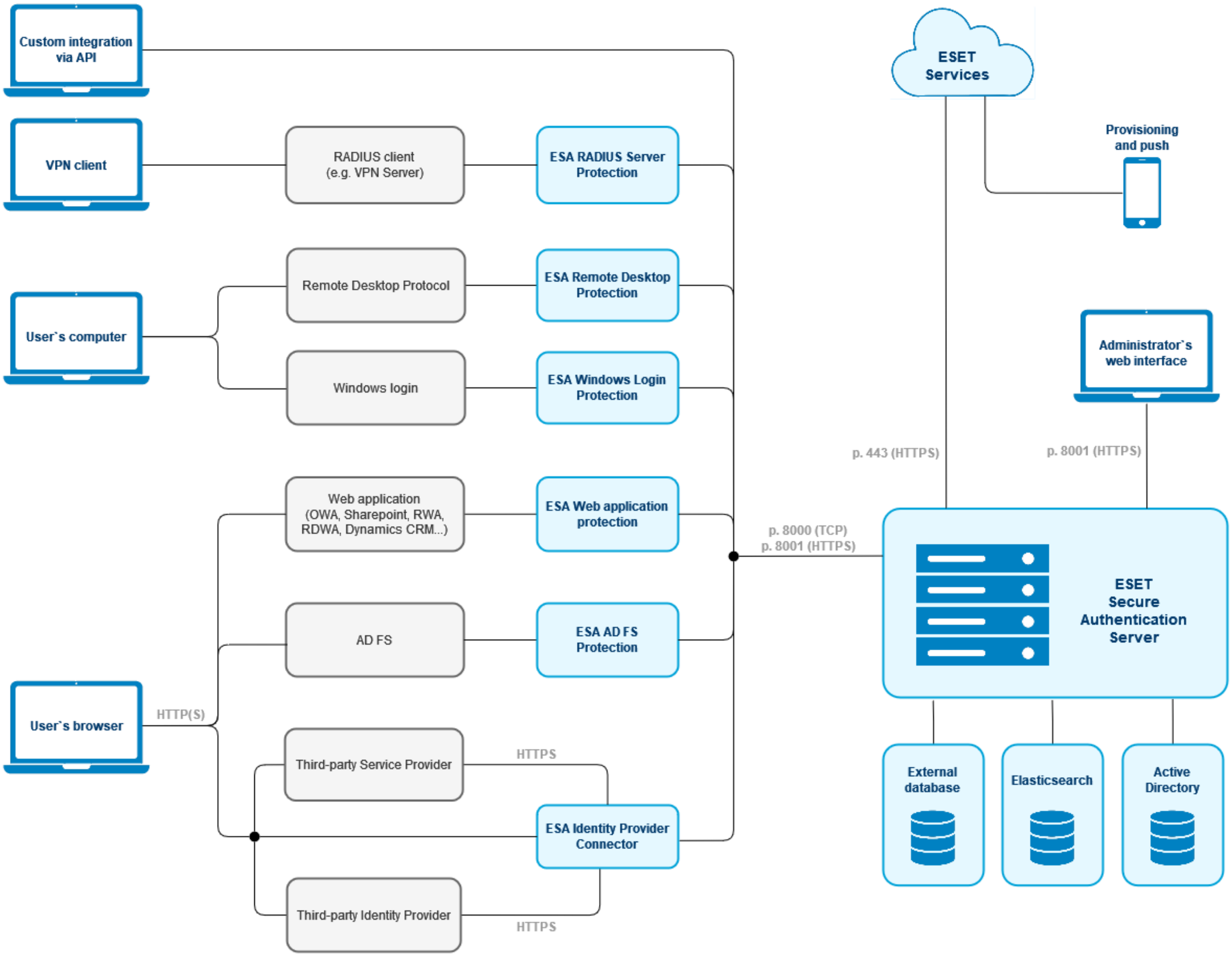
All of the following components are required for your first ESA installation:

- At least one instance of the Authentication Server
- At least one of the authentication endpoints (API, Windows Login, Web Application, AD FS, Remote Desktop, or RADIUS)

You can install all components on a single machine or across multiple machines in a distributed environment—however, the ESA Web Console is part of the Authentication Server. As is the case with distributed systems, there are many possible installation scenarios.

When installing ESA Authentication Server in an Active Directory environment, you do not have to install it on the domain controller specifically. It can be installed on any other machine, even in Standalone mode.

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.


Custom integration via API
VPN client
RADIUS client (e.g. VPN Server)
ESA RADIUS Server Protection
User`s computer
Remote Desktop Protocol
ESA Remote Desktop Protection
Windows login
ESA Windows Login Protection
Web application (OWA, Sharepoint, RWA, RDWA, Dynamics CRM...)
ESA Web application protection
AD FS
ESA AD FS Protection
User`s browser
HTTP(S)
Third-party Service Provider
HTTPS
ESA Identity Provider Connector
Third-party Identity Provider
HTTPS
ESET Services
Provisioning and push
Administrator`s web interface
p. 443 (HTTPS)
p. 8001 (HTTPS)
p. 8000 (TCP)
p. 8001 (HTTPS)
ESET Secure Authentication Server
External database
Elasticsearch
Active Directory

Install the Authentication Server

Windows Server 2008 and Windows Server 2008R2

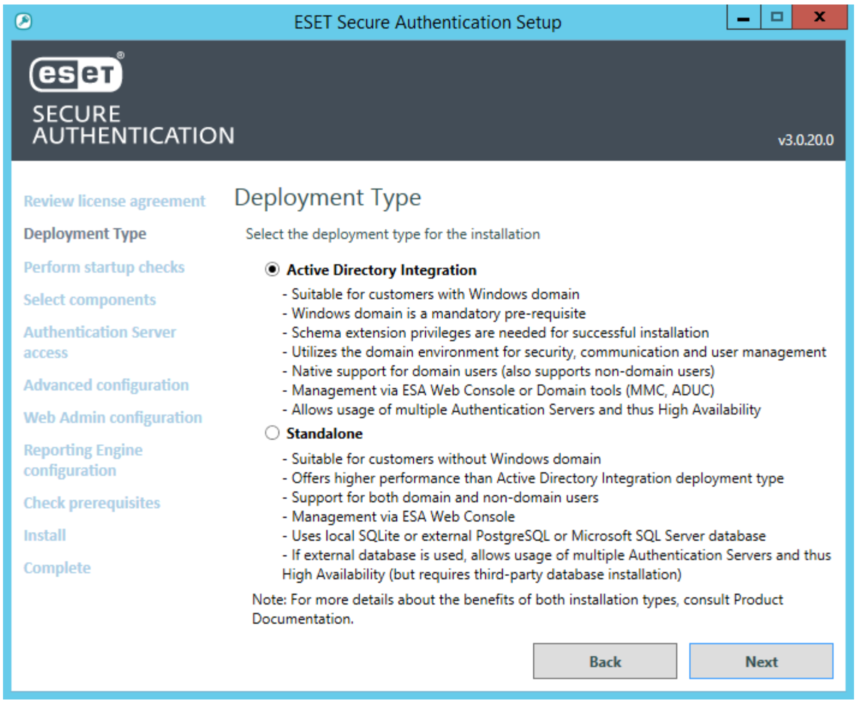
Before installing the Authentication Server on Windows Server 2008 or Windows Server 2008 R2, change the default TLS version to use.

1. Run the supplied *.EXE* file to install the Authentication Server on the machine that will host the ESA Authentication Service. NET Framework version 4.5 will be automatically installed if it is not detected.

2. Select a deployment type:

- **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. They can also invite computers from outside their network, as long as the Authentication Server is available online.

- **Standalone** - This type of deployment is also 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.



Deployment Type

Select the deployment type for the installation

● **Active Directory Integration**

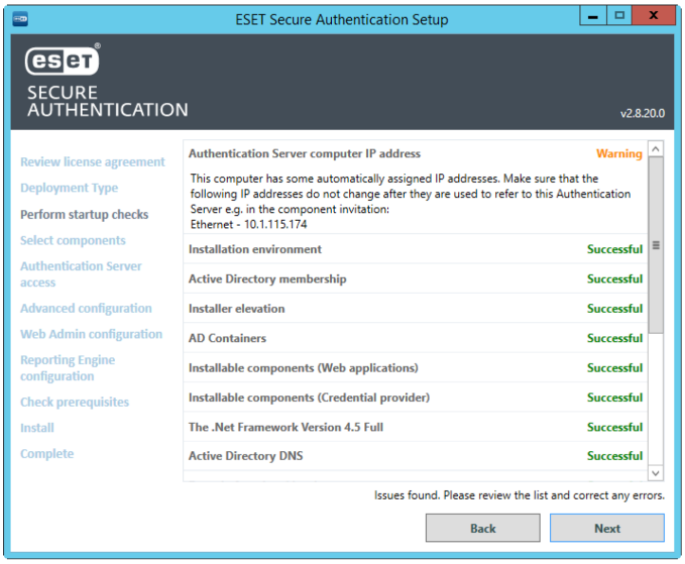
- Suitable for customers with Windows domain
- Windows domain is a mandatory pre-requisite
- Schema extension privileges are needed for successful installation
- Utilizes the domain environment for security, communication and user management
- Native support for domain users (also supports non-domain users)
- Management via ESA Web Console or Domain tools (MMC, ADUC)
- Allows usage of multiple Authentication Servers and thus High Availability

○ **Standalone**

- Suitable for customers without Windows domain
- Offers higher performance than Active Directory Integration deployment type
- Support for both domain and non-domain users
- Management via ESA Web Console
- Uses local SQLite or external PostgreSQL or Microsoft SQL Server database
- If external database is used, allows usage of multiple Authentication Servers and thus High Availability (but requires third-party database installation)

Note: For more details about the benefits of both installation types, consult Product Documentation.

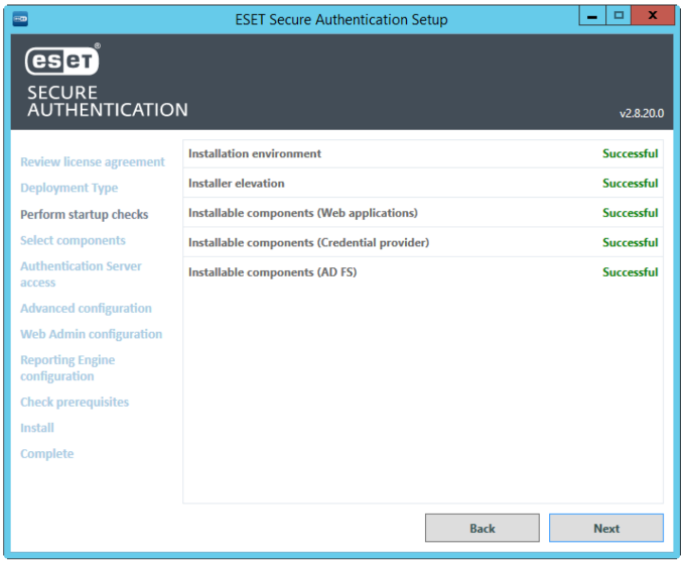
3. A number of prerequisite checks will be performed to ensure that the domain or installation environment is healthy and that ESA can be installed. Any failures must be corrected before installation can proceed. The installation will continue when all prerequisites are completed.
If the **Next** button is not available for more than 5 seconds, wait or scroll down to see which requirements are still being checked.



Authentication Server computer IP address	Warning
This computer has some automatically assigned IP addresses. Make sure that the following IP addresses do not change after they are used to refer to this Authentication Server e.g. in the component invitation: Ethernet - 10.1.115.174	
Installation environment	Successful
Active Directory membership	Successful
Installer elevation	Successful
AD Containers	Successful
Installable components (Web applications)	Successful
Installable components (Credential provider)	Successful
The .Net Framework Version 4.5 Full	Successful
Active Directory DNS	Successful

Issues found. Please review the list and correct any errors.

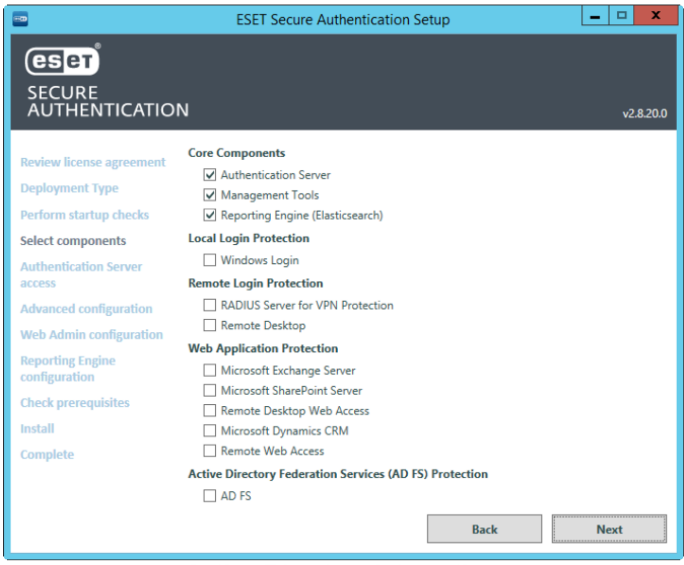
Active Directory Integration



Installation environment	Successful
Installer elevation	Successful
Installable components (Web applications)	Successful
Installable components (Credential provider)	Successful
Installable components (AD FS)	Successful

Standalone

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



ESET Secure Authentication Setup

v2.8.20.0

- Review license agreement
- Deployment Type
- Perform startup checks
- Select components
- Authentication Server access
- Advanced configuration
- Web Admin configuration
- Reporting Engine configuration
- Check prerequisites
- Install
- Complete

Core Components

☑ Authentication Server
☑ Management Tools
☑ Reporting Engine (Elasticsearch)

Local Login Protection

☐ Windows Login

Remote Login Protection

☐ RADIUS Server for VPN Protection
☐ Remote Desktop

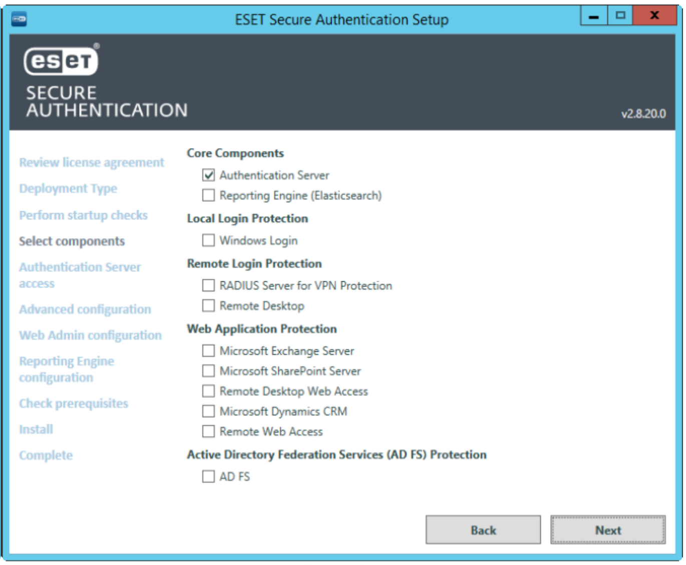
Web Application Protection

☐ Microsoft Exchange Server
☐ Microsoft SharePoint Server
☐ Remote Desktop Web Access
☐ Microsoft Dynamics CRM
☐ Remote Web Access

Active Directory Federation Services (AD FS) Protection

☐ AD FS

Active Directory Integration



ESET Secure Authentication Setup

v2.8.20.0

- Review license agreement
- Deployment Type
- Perform startup checks
- Select components
- Authentication Server access
- Advanced configuration
- Web Admin configuration
- Reporting Engine configuration
- Check prerequisites
- Install
- Complete

Core Components

☑ Authentication Server
☐ Reporting Engine (Elasticsearch)

Local Login Protection

☐ Windows Login

Remote Login Protection

☐ RADIUS Server for VPN Protection
☐ Remote Desktop

Web Application Protection

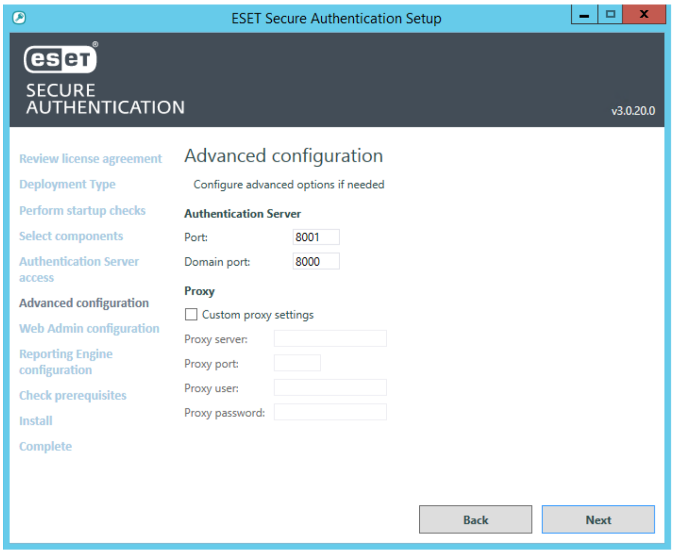
☐ Microsoft Exchange Server
☐ Microsoft SharePoint Server
☐ Remote Desktop Web Access
☐ Microsoft Dynamics CRM
☐ Remote Web Access

Active Directory Federation Services (AD FS) Protection

☐ AD FS

Standalone

5. If port number 8000 (Active Directory Integration only) or 8001 is already in use on your network, select a different **Domain port** or different **Port** for the ESA Web Console. If you prefer to use a transparent proxy, select **Custom proxy settings** and type in the corresponding values. Port number 8001 is also used for API. If installing the Authentication Server in Standalone mode and prefer to use an external database, select a supported external database from **Database Type** and type the existing database's connection details. Click **Next**.



ESET Secure Authentication Setup

v3.0.20.0

- Review license agreement
- Deployment Type
- Perform startup checks
- Select components
- Authentication Server access
- Advanced configuration
- Web Admin configuration
- Reporting Engine configuration
- Check prerequisites
- Install
- Complete

Advanced configuration

Configure advanced options if needed

Authentication Server

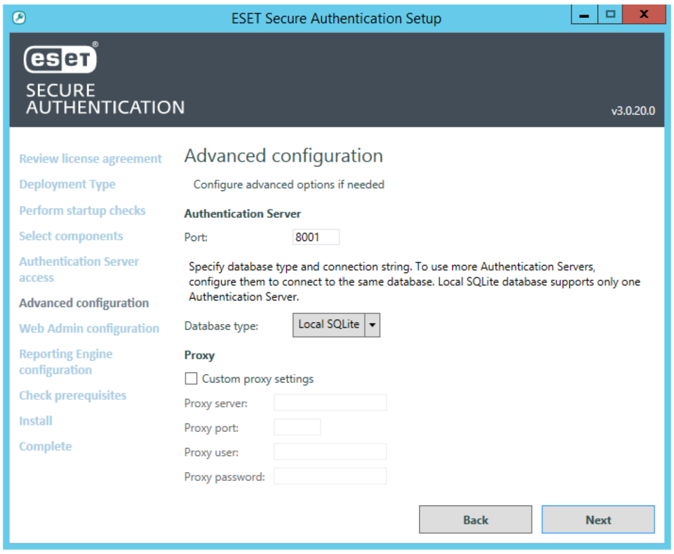
Port: 8001
Domain port: 8000

Proxy

☐ Custom proxy settings

Proxy server:
Proxy port:
Proxy user:
Proxy password:

Active Directory Integration



ESET Secure Authentication Setup

v3.0.20.0

- Review license agreement
- Deployment Type
- Perform startup checks
- Select components
- Authentication Server access
- Advanced configuration
- Web Admin configuration
- Reporting Engine configuration
- Check prerequisites
- Install
- Complete

Advanced configuration

Configure advanced options if needed

Authentication Server

Port: 8001

Specify database type and connection string. To use more Authentication Servers, configure them to connect to the same database. Local SQLite database supports only one Authentication Server.

Database type: Local SQLite

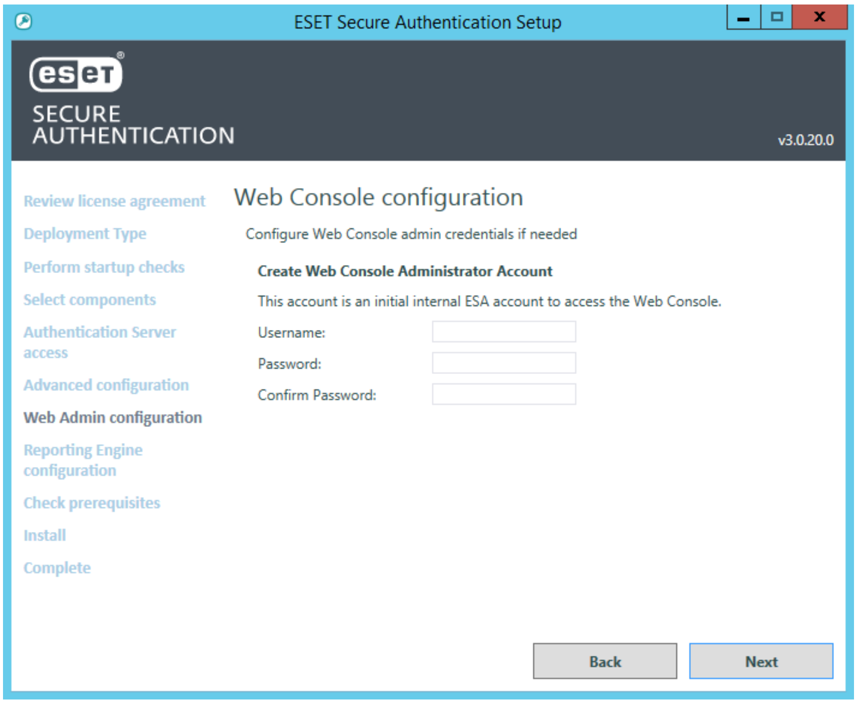
Proxy

☐ Custom proxy settings

Proxy server:
Proxy port:
Proxy user:
Proxy password:

Standalone

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



ESET Secure Authentication Setup

SECURE AUTHENTICATION v3.0.20.0

Web Console configuration

Configure Web Console admin credentials if needed

Create Web Console Administrator Account

This account is an initial internal ESA account to access the Web Console.

Username:

Password:

Confirm Password:

7. The subsequent **Check prerequisites** screen will reveal if the selected ports are available.

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

9. Use the ESA Web Console to configure your installation of ESET Secure Authentication and related components, users.

Custom proxy settings

If the administrator prefers to use a transparent proxy during the Authentication Server (AS) installation, select **Custom proxy settings** and type in the corresponding values. If **Custom proxy settings** is not selected, the default system proxy settings are used. Default settings are specified in the current user's **Internet Options** screen.

Determine the current user:

- If the AS is installed in Active Directory Integration mode, the current user is `ESASrv_<computer name>`
- If the AS is installed in Standalone mode, the current user is Local System
- During the Authentication Server installation, the current user is the user who ran the installer when the prerequisite check is running
- If **Custom proxy settings** is selected and the **Proxy server** is empty, the AS will not use a proxy

High Availability View - Active Directory

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 listed.

Each ESA Authentication Server 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.

Multiple Authentication Servers utilizing Standalone deployment type

High Availability View - Standalone mode

In ESET Secure Authentication (ESA) version 3.0, you can have multiple Authentication Servers even in **Standalone** installation mode.

1. When installing each Authentication Server, define the same external database connection details.
2. When installed, all Authentication Servers will be visible in the ESA Web Console.
3. Configure a proxy server as a load-balancer. Refer to "Sample configuration snippet - multiple authentication servers".
4. In invitations, use the the proxy server's IP address instead of the name of the Authentication Server.
5. If an Authentication Server is added/removed, update the proxy configuration.

All servers installed will be displayed in the **Servers** tile of the **Dashboard** screen in the ESA Web Console.

Multiple Authentication Servers in Active Directory environment.

Install the Reporting Engine (Elasticsearch)

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

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

> **2GB free RAM required**
> Elasticsearch requires 2GB of RAM permanently. Make sure you have enough free RAM; otherwise, the installation will fail. See how to set a different heap size.

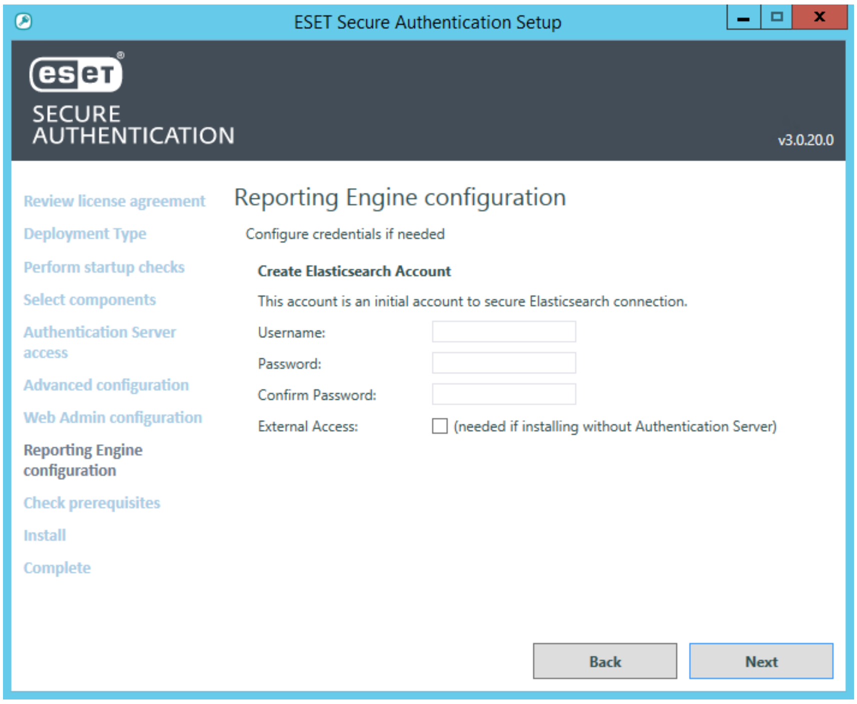
Installation from ESA installer

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 on installing the Authentication Server and 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**.



Reporting Engine configuration

Configure credentials if needed

Create Elasticsearch Account

This account is an initial account to secure Elasticsearch connection.

Username:

Password:

Confirm Password:

External Access: □ (needed if installing without Authentication Server)

3. If the installer warns you about missing requirements, make sure to fulfill the requirements before proceeding with the installation.

4. Follow the installer's instructions to complete the remainder of the steps and close the installer when you are finished.

Install the Elasticsearch separately

If you have already installed the Authentication Server and are installing the 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 installer's instructions to complete the remainder of the steps and close the installer when you are finished.

> **Silent mode installation**
>
> Silent mode installation is available via .MSI installer for both Active Directory Integration mode and Standalone mode.

Using 3rd party installation of Elasticsearch

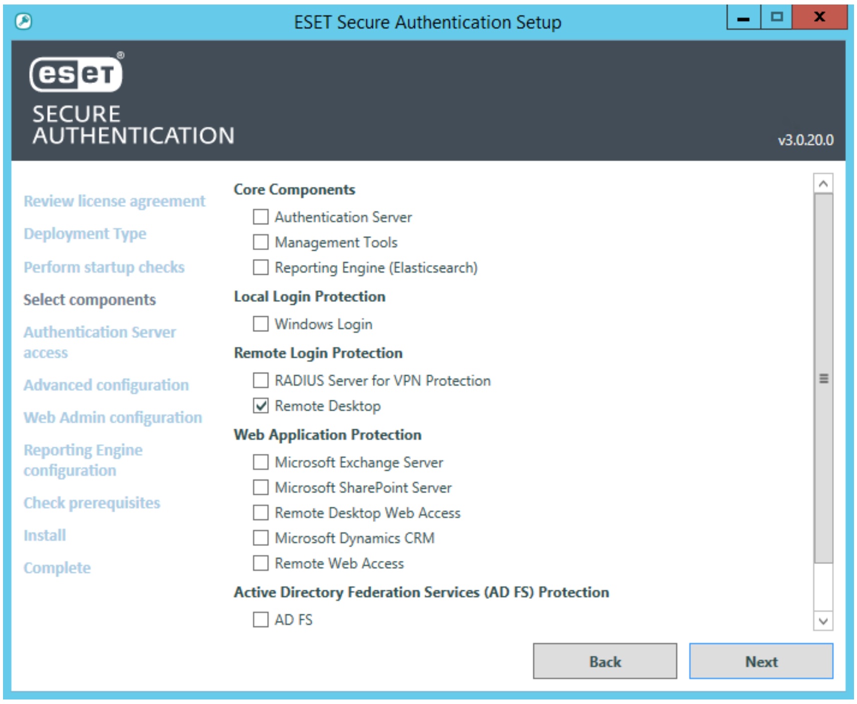
If you are using a 3rd party installation of Elasticsearch and want to use Reports in ESA Web Console, add the information about your Elasticsearch installation in the ESA Web Console at **Settings** > **Reports**.

If you access Elasticsearch via Kibana, you can generate various charts from the collected data.

Install the Remote Desktop plugin

1. To start the installation, on the appropriate Remote Desktop Access machine, run the supplied .EXE file. The installer will run several prerequisite checks as was done during the Authentication Server installation.

2. When prompted, select the check box next to **Remote Desktop** and click **Next**.



Core Components

□ Authentication Server
□ Management Tools
□ Reporting Engine (Elasticsearch)

Local Login Protection

□ Windows Login

Remote Login Protection

□ RADIUS Server for VPN Protection
☑ Remote Desktop

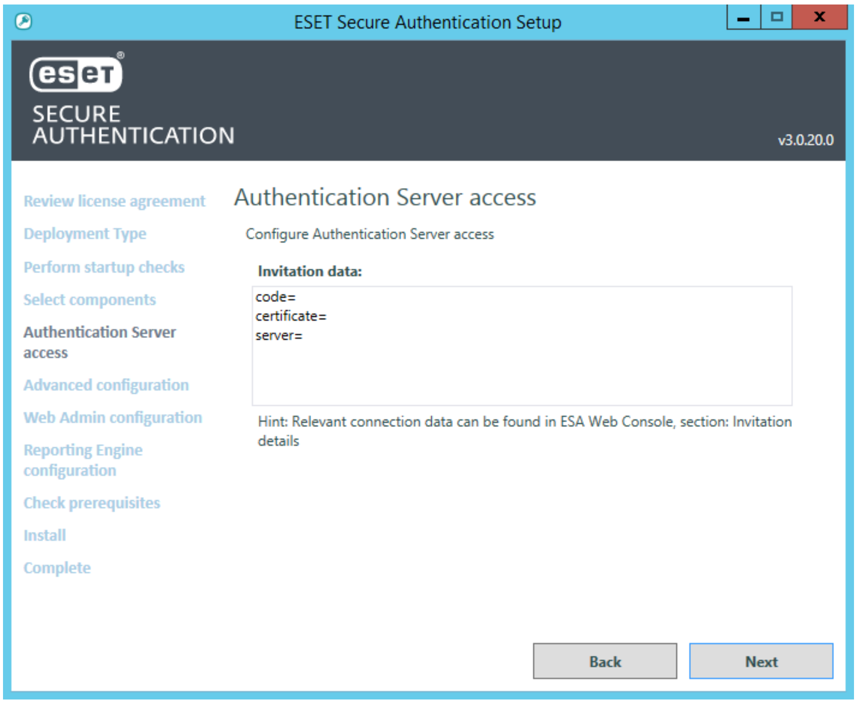
Web Application Protection

□ Microsoft Exchange Server
□ Microsoft SharePoint Server
□ Remote Desktop Web Access
□ Microsoft Dynamics CRM
□ Remote Web Access

Active Directory Federation Services (AD FS) Protection

□ AD FS

3. Type the connection information of the Authentication Server when prompted (applies to standalone installation mode). Click **Next**.



Authentication Server access

Configure Authentication Server access

Invitation data:

```
code=
certificate=
server=
```

Hint: Relevant connection data can be found in ESA Web Console, section: Invitation details

4. If the connection to Authentication Server is successful, and the server certificate has been verified, select

check box **Add certificate with this thumbprint to machine store** if available. Click **Next**.

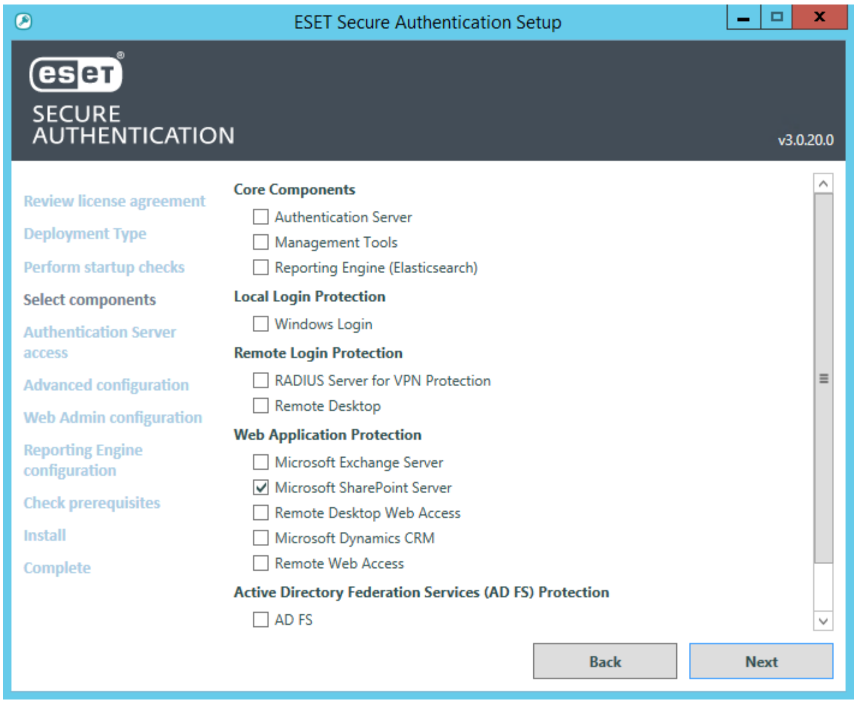
> **Correct failures reported by the prerequisite checks**
> Prerequisite checks will run to verify the ESA Remote Desktop plug-in can be installed. Any failures must be corrected before installation can proceed.

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

Install the Web App plugin

1. To start the installation, on the appropriate machine running the Web App, run the supplied .EXE file. The installer will run several prerequisite checks as was done during the Installation of the Authentication Server.

2. When prompted, select the check box next to the applicable Web App and click **Next**.



Core Components

- ☐ Authentication Server
- ☐ Management Tools
- ☐ Reporting Engine (Elasticsearch)

Local Login Protection

- ☐ Windows Login

Remote Login Protection

- ☐ RADIUS Server for VPN Protection
- ☐ Remote Desktop

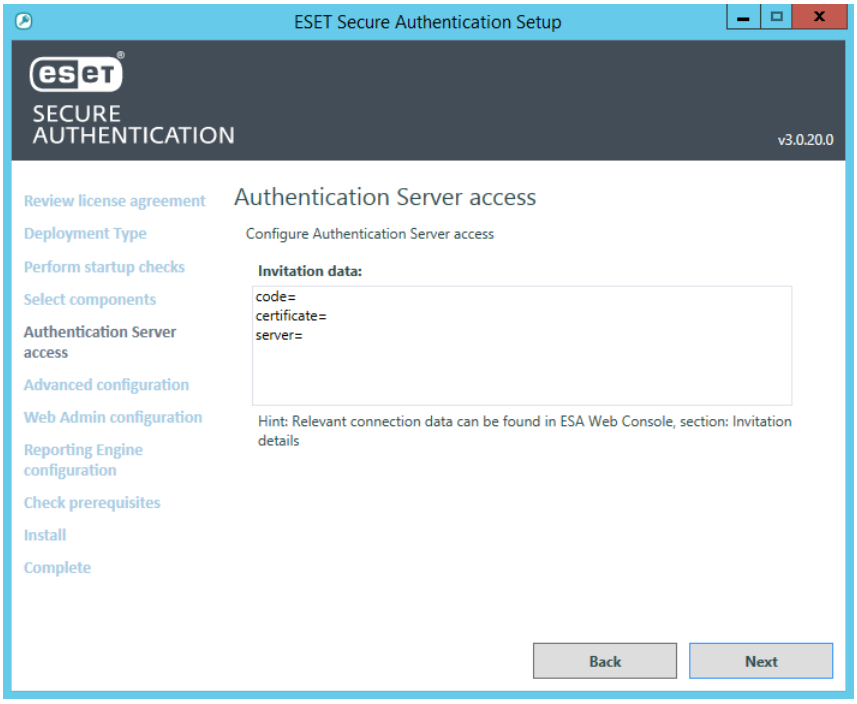
Web Application Protection

- ☐ Microsoft Exchange Server
- ☑ Microsoft SharePoint Server
- ☐ Remote Desktop Web Access
- ☐ Microsoft Dynamics CRM
- ☐ Remote Web Access

Active Directory Federation Services (AD FS) Protection

- ☐ AD FS

3. Type the connection information of the Authentication Server when prompted (applies to standalone installation mode). Click **Next**.



Authentication Server access

Configure Authentication Server access

Invitation data:

```
code=
certificate=
server=
```

Hint: Relevant connection data can be found in ESA Web Console, section: Invitation details

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

Prerequisite checks

Prerequisite checks will be run to ensure the Web App is running on the server and the ESA Web App plugin can be installed. Correct all failures to proceed with the installation.

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

MSI installer

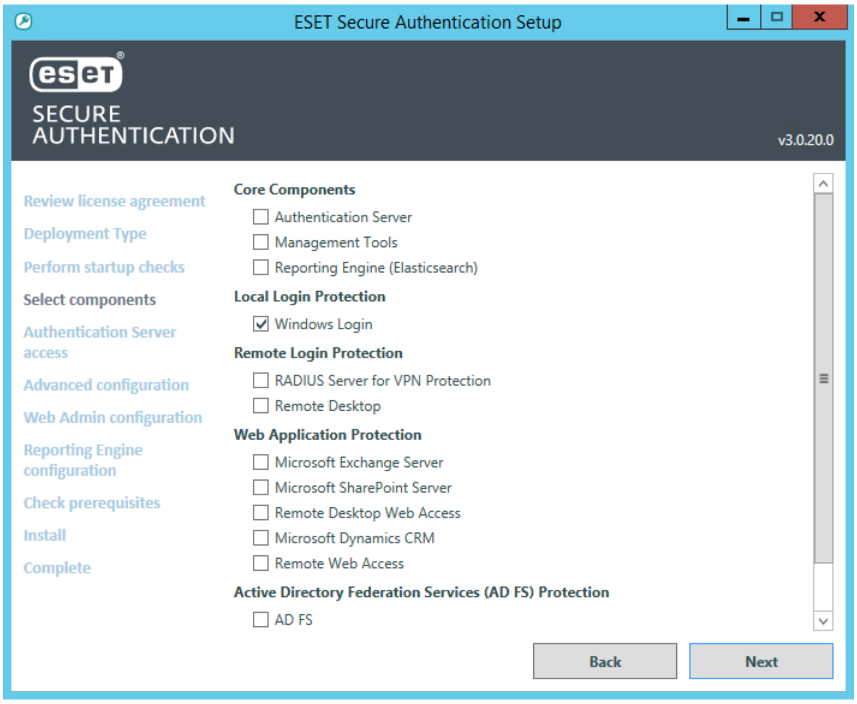
When using the .MSI installer to install 2FA protection for **Microsoft SharePoint Server**, **Remote Desktop Web Access**, or **Microsoft Dynamics CRM**, run the installer with elevated privileges.

Install the 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. If not detected, the .NET Framework version 4.5 is installed automatically.

2. When prompted, click **Select components**, select the check box next to **Windows Login**, and click **Next**.



ESET Secure Authentication Setup

ESET SECURE AUTHENTICATION v3.0.20.0

Review license agreement
Deployment Type
Perform startup checks
Select components
Authentication Server access
Advanced configuration
Web Admin configuration
Reporting Engine configuration
Check prerequisites
Install
Complete

Core Components
- □ Authentication Server
- □ Management Tools
- □ Reporting Engine (Elasticsearch)

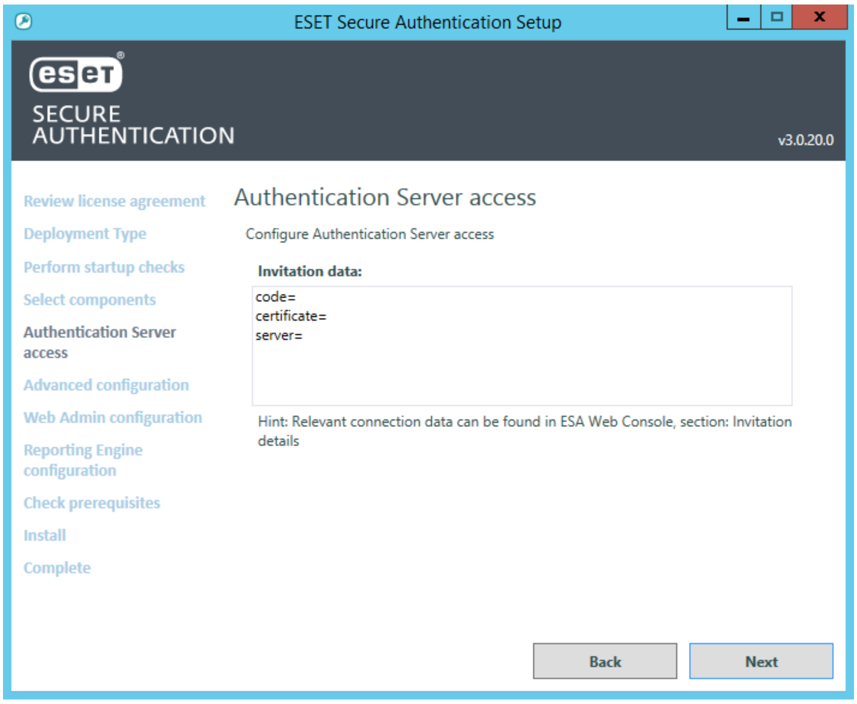
Local Login Protection
- ☑ Windows Login

Remote Login Protection
- □ RADIUS Server for VPN Protection
- □ Remote Desktop

Web Application Protection
- □ Microsoft Exchange Server
- □ Microsoft SharePoint Server
- □ Remote Desktop Web Access
- □ Microsoft Dynamics CRM
- □ Remote Web Access

Active Directory Federation Services (AD FS) Protection
- □ AD FS

3. Type the connection information of the Authentication Server when prompted (applies to standalone installation mode). Click **Next**.



ESET Secure Authentication Setup

ESET SECURE AUTHENTICATION v3.0.20.0

Review license agreement
Deployment Type
Perform startup checks
Select components
Authentication Server access
Advanced configuration
Web Admin configuration
Reporting Engine configuration
Check prerequisites
Install
Complete

Authentication Server access

Configure Authentication Server access

Invitation data:

```
code=
certificate=
server=
```

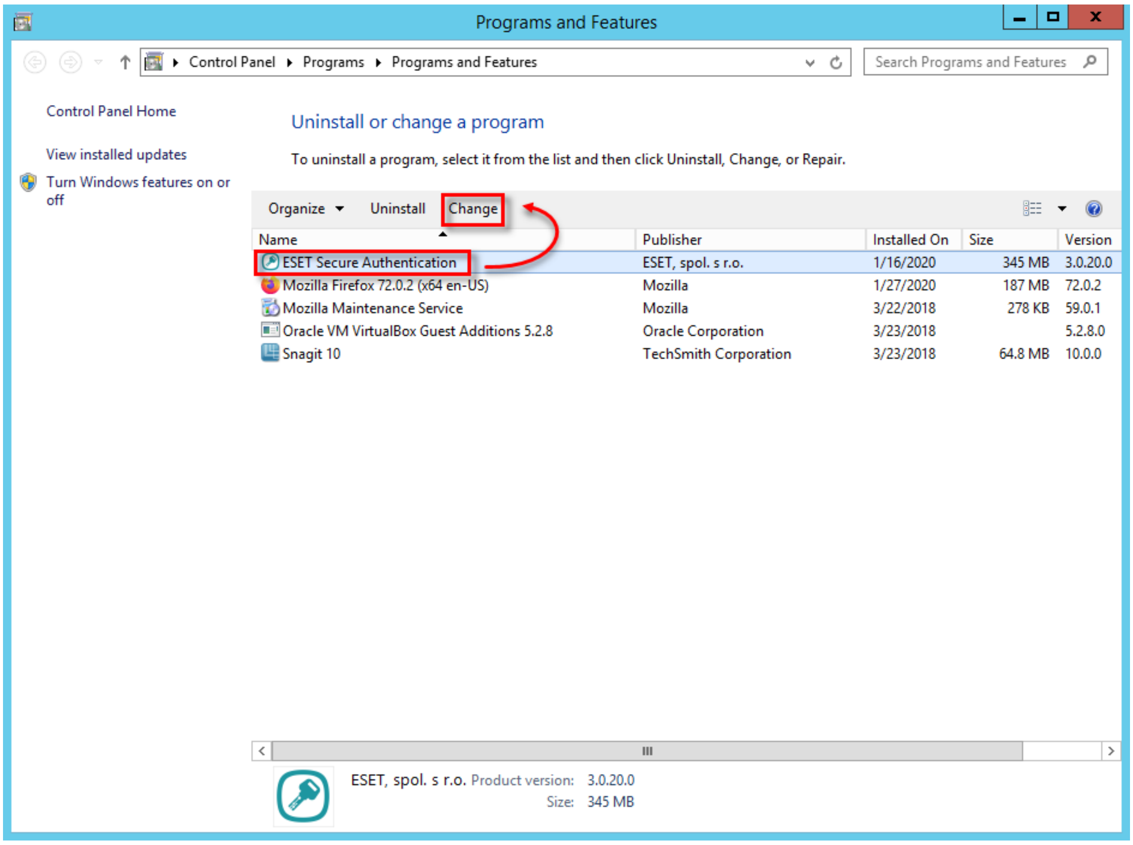
Hint: Relevant connection data can be found in ESA Web Console, section: Invitation details

4. If the connection to Authentication Server is successful, and the server certificate has been verified, select check box **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.

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**.



Programs and Features

Control Panel ▸ Programs ▸ Programs and Features

Search Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Uninstall or change a program

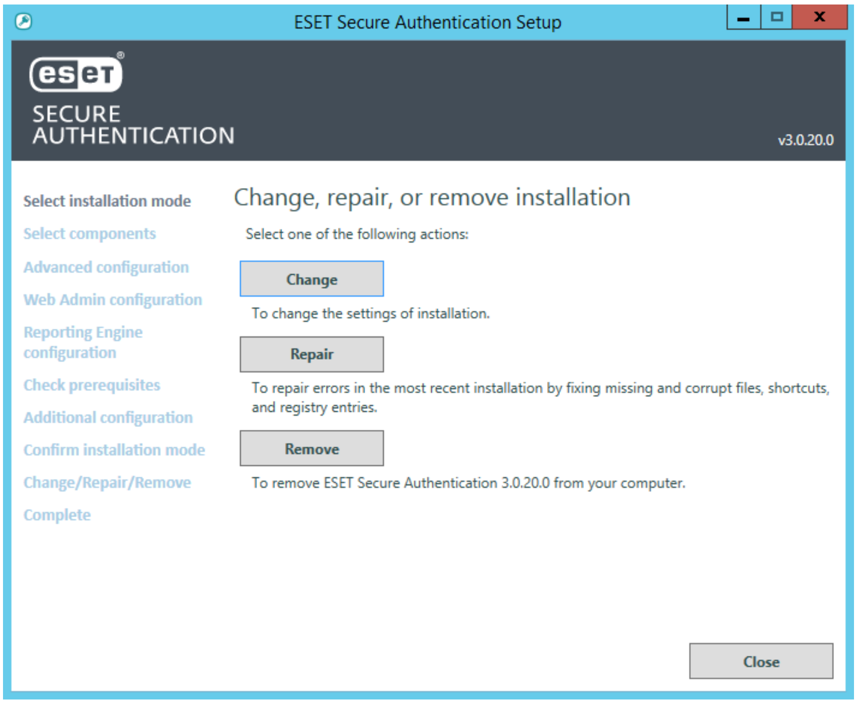
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize ▾ Uninstall Change

Name	Publisher	Installed On	Size	Version
ESET Secure Authentication	ESET, spol. s r.o.	1/16/2020	345 MB	3.0.20.0
Mozilla Firefox 72.0.2 (x64 en-US)	Mozilla	1/27/2020	187 MB	72.0.2
Mozilla Maintenance Service	Mozilla	3/22/2018	278 KB	59.0.1
Oracle VM VirtualBox Guest Additions 5.2.8	Oracle Corporation	3/23/2018		5.2.8.0
Snagit 10	TechSmith Corporation	3/23/2018	64.8 MB	10.0.0

ESET, spol. s r.o. Product version: 3.0.20.0
Size: 345 MB

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



ESET Secure Authentication Setup

eset SECURE AUTHENTICATION v3.0.20.0

- Select installation mode
- Select components
- Advanced configuration
- Web Admin configuration
- Reporting Engine configuration
- Check prerequisites
- Additional configuration
- Confirm installation mode
- Change/Repair/Remove
- Complete

Change, repair, or remove installation

Select one of the following actions:

Change

To change the settings of installation.

Repair

To repair errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.

Remove

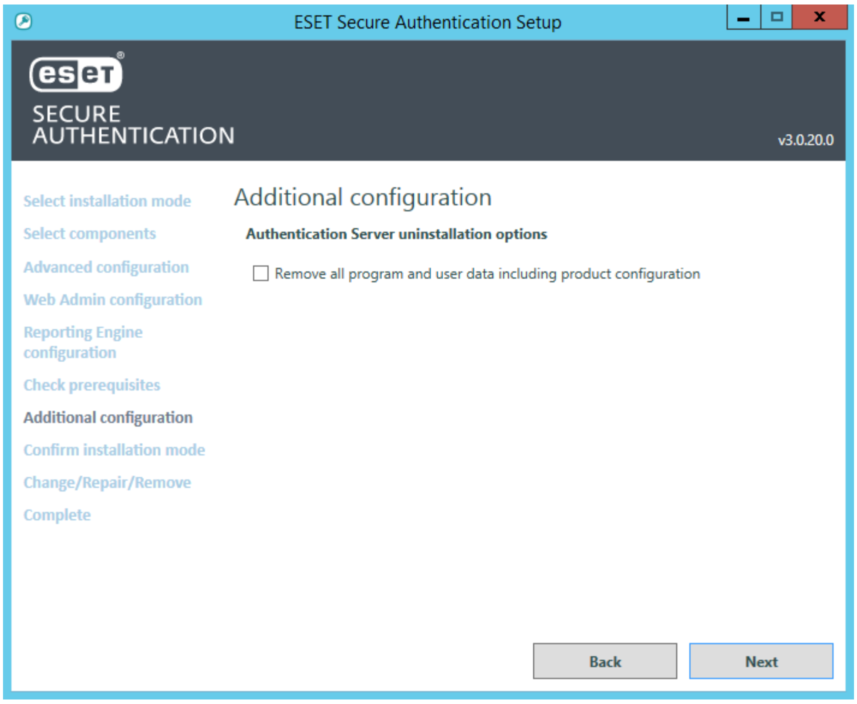
To remove ESET Secure Authentication 3.0.20.0 from your computer.

Close

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

Removal of Authentication Server

To uninstall the Authentication Server, 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 the Authentication Server is not the last component in the Active Directory domain you are preparing to uninstall or do not have Domain Admin uninstall privileges.



Additional configuration

Authentication Server uninstallation options

□ Remove all program and user data including product configuration

This option is available as **AUTHENTICATION_SERVER_CLEAN_DATA** parameter when executing a silent uninstall via .MSI package:

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

Domain admin privileges

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.

Remote Installation via ESET PROTECT

To install ESA components via ESET PROTECT:

1. Log in to the ESET PROTECT Web Console, navigate to **More** > **License Management**, and make sure an ESET Secure Authentication license is imported. See License Management for more information.

2. Navigate to **Tasks**, click **New**, and select **Client Task**.

3. In the **Basic** section, name the task, select **Software Install** from the **Tasks** drop-down menu and click **Continue**.

4. Click **Choose ESET License**, select **ESET Secure Authentication**, and click **Ok**.

5. Click **Choose package**, select **ESET Secure Authentication**, and click **Ok**.

6. Select the **I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy** check box.

7. In the **Installation Parameters**, define the .MSI arguments to install the desired ESA components.

8. Click **Continue**, then click **Finish**.

Examples of using ESA .MSI arguments when deploying ESA components through ESET PROTECT

Example - Install Windows Login and Remote Desktop (Standalone mode)

```
ADDLOCAL="Win_Credential_Provider,Credential_Provider" ESA_COMPUTER_CONFIG_INTEGRATI
ON_MODE=2 ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ADDRESS=192.168.0.15:8001 ESA_CO
MPUTER_CONFIG_AUTHENTICATION_SERVER_ACCESS=DKNO-XESE-WXUA-QNXW-
JAEI TRUSTED_CERT_HASH=2CD61594DDE3E63E6BEBB9BF3DC95B85550FD5D8
```

Example - Install Windows Login and Remote Desktop as a no domain admin user (Active Directory Integration mode)

```
ADDLOCAL="Win_Credential_Provider,Credential_Provider" NO_DOMAIN_ADMIN_MODE=1
```

Do not forget to add the computer(s) to EsaServices manually.

Install Windows Login and RDP protection via GPO

This article applies to **Active Directory Integration** deployment type only.

Prerequisites

Server (or main computer) where the Authentication Server is installed

- Must belong to the same Active Directory (AD) domain as 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. See the 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 later 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 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
- Remote Desktop connection must be enabled on the specific 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 Authenitcation**, right-click **EsaServices**, select **Properties**.

4. Click **Members** tab > **Add** > **Object Types** > select **Computers** > **OK**.

5. In the **Enter the object names to select** field, type the computer name you want to install Windows Login protection on. Click **Check Names** to ensure the computer name is correct.

6. If the computer name is correct, click **OK**, click **OK** again.

Obtaining the .MSI installation file

If the 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 `.MSI` installation file to a shared folder on your server (main computer) accessible by your AD domain members.

Proceed with one of the deployment options below:

- Startup script
- Software Installation task

The `.MSI` installer is also available in the ESET PROTECT repository.

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, type 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"
```

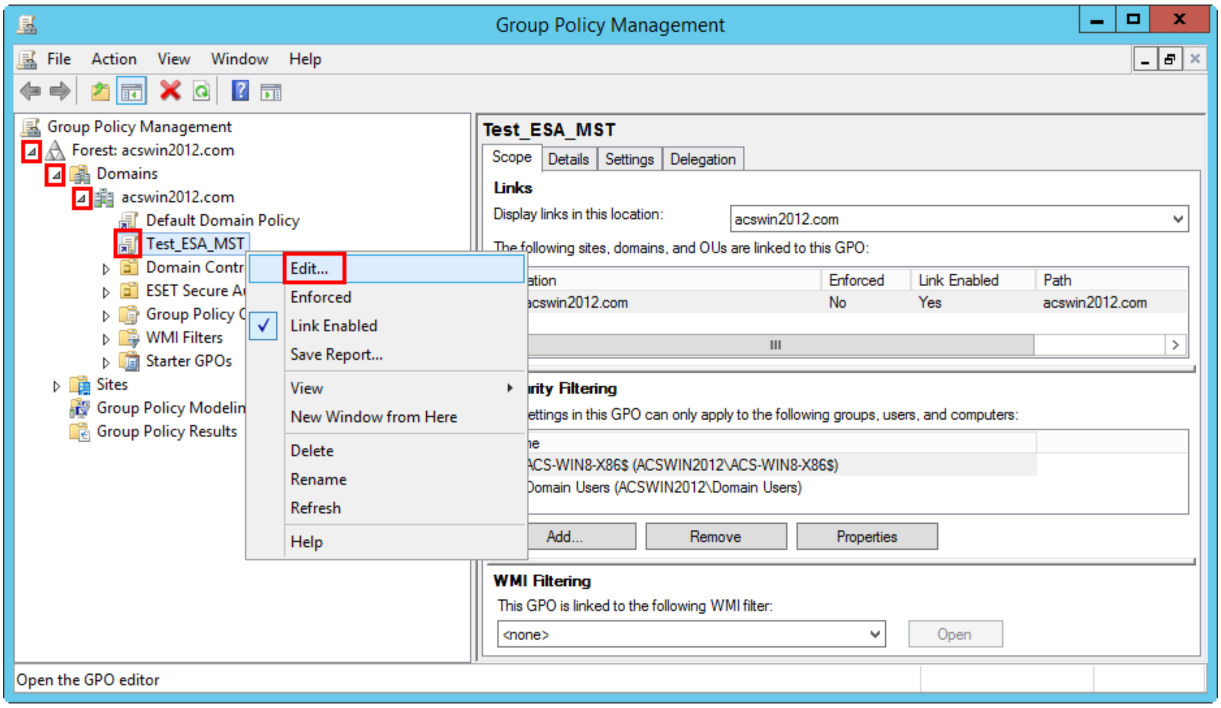
where the `<path_to_msi_file>` must be replaced with a valid Universal Naming Convention (UNC) path (network path) to the shared installer package (for example, \\*fileserver**share**filename.MSI*). The code must be in-line.

> **Terms**
> `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 type: **esainstall.bat** as the filename.

Deployment of startup script

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



Links

Display links in this location: acswin2012.com

The following sites, domains, and OUs are linked to this GPO:

ation	Enforced	Link Enabled	Path
acswin2012.com	No	Yes	acswin2012.com

rity Filtering

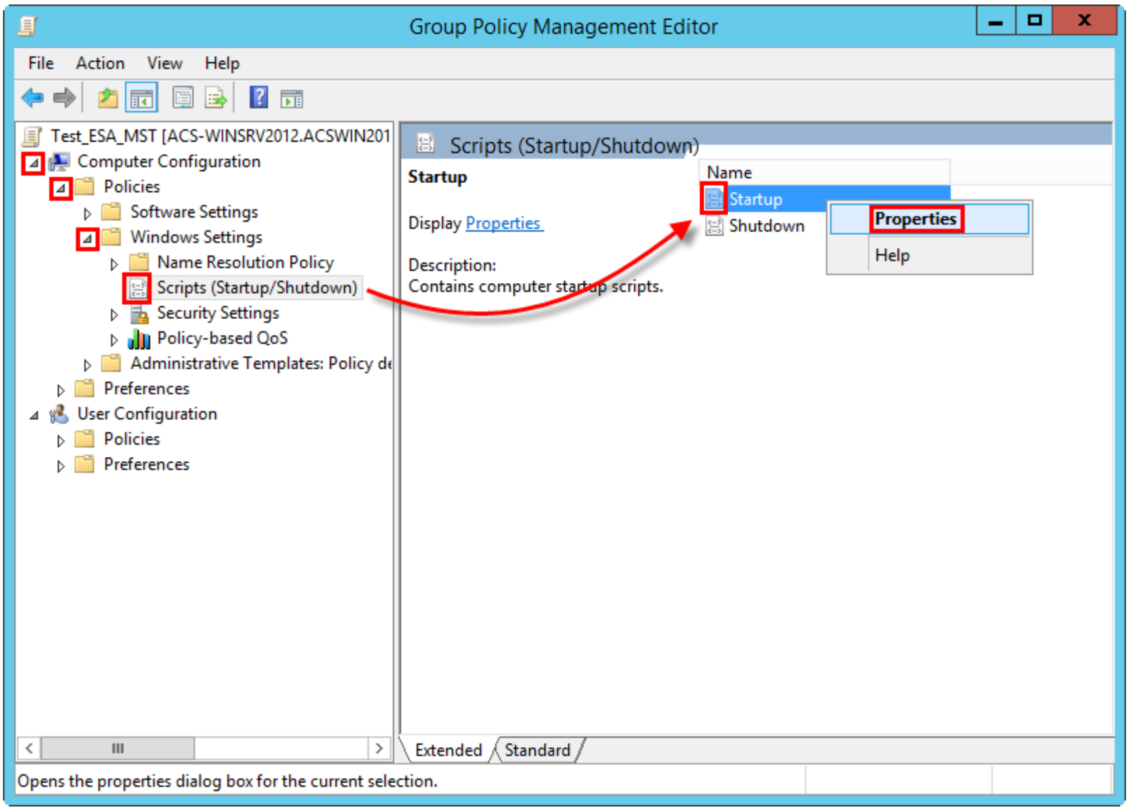
ettings in this GPO can only apply to the following groups, users, and computers:

e
ACS-WIN8-X86$ (ACSWIN2012\ACS-WIN8-X86$)
Domain Users (ACSWIN2012\Domain Users)

WMI Filtering

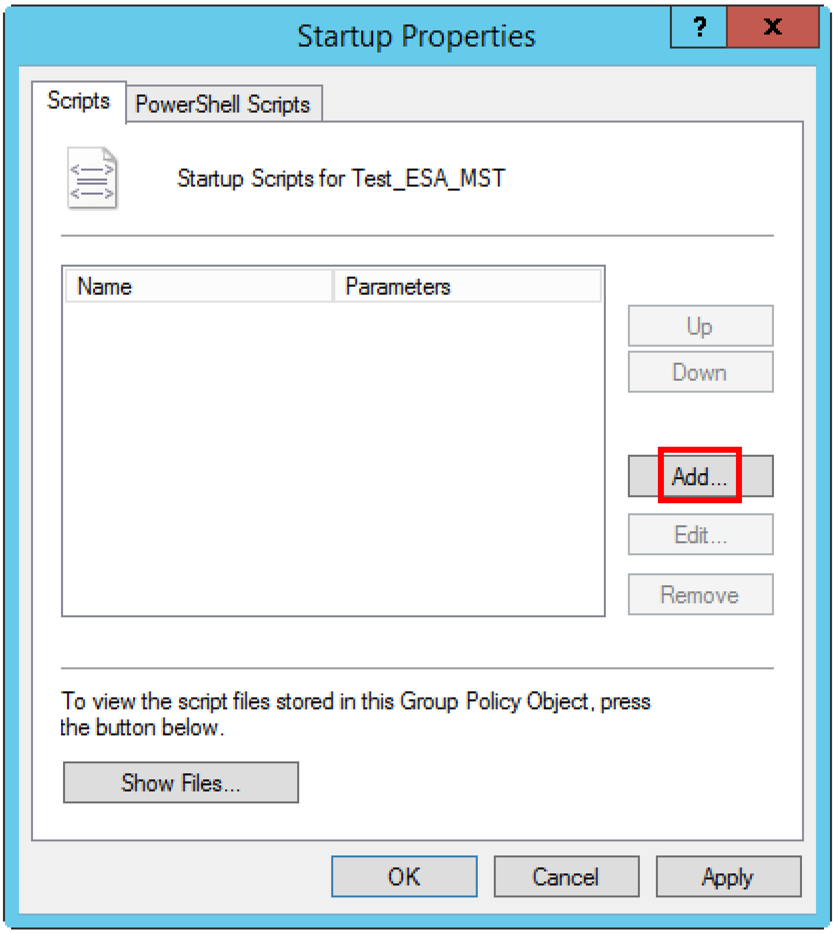
This GPO is linked to the following WMI filter: <none>

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



Opens the properties dialog box for the current selection.

3. 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**.



To view the script files stored in this Group Policy Object, press the button below.

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

Software Installation task

Before creating a **Software Installation** task via **GPO**, it is essential to create an `.MST` transform file.

Prerequisite

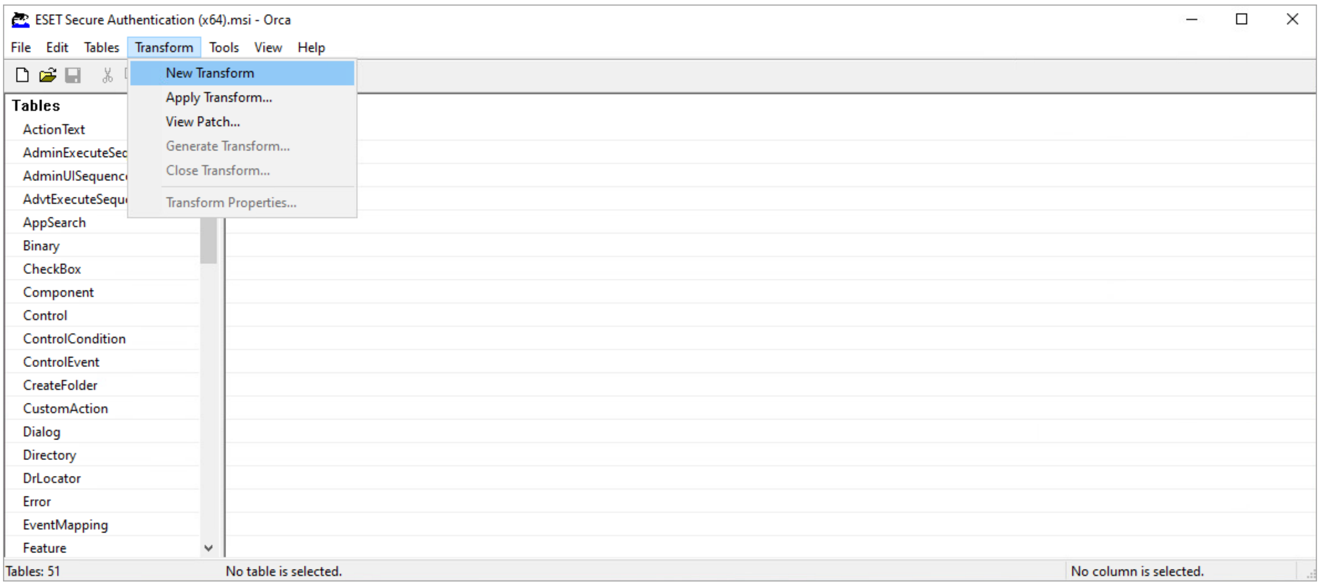
Install the Orca database editor tool on your computer. Orca is available as part of the Windows SDK. For instructions to download and install Orca, visit the following Microsoft Knowledge Base article: Orca.EXE.

Creating an .mst transform file

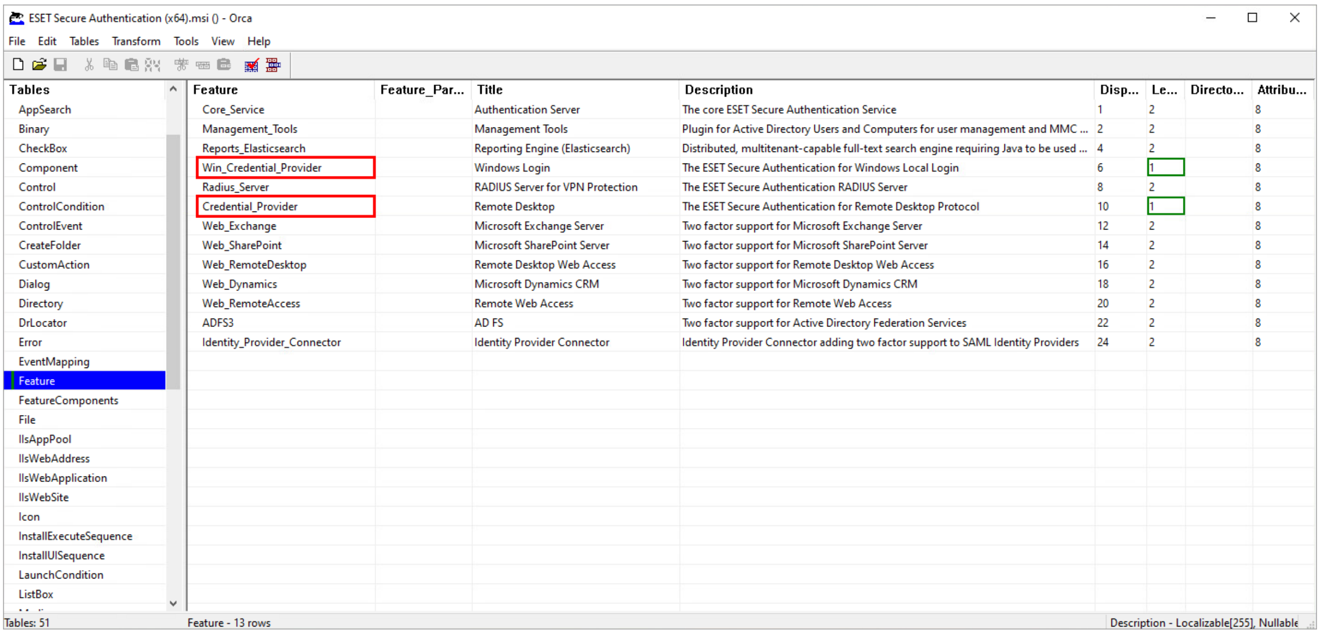
1. Click **Start** > **All Programs** > **Orca** to launch Orca database editor.

2. Click **File** > **Open**, navigate to the `.MSI` installer file you want to transform, select it, and click **Open**.

3. Click **Transform** > **New Transform**.



4. 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.

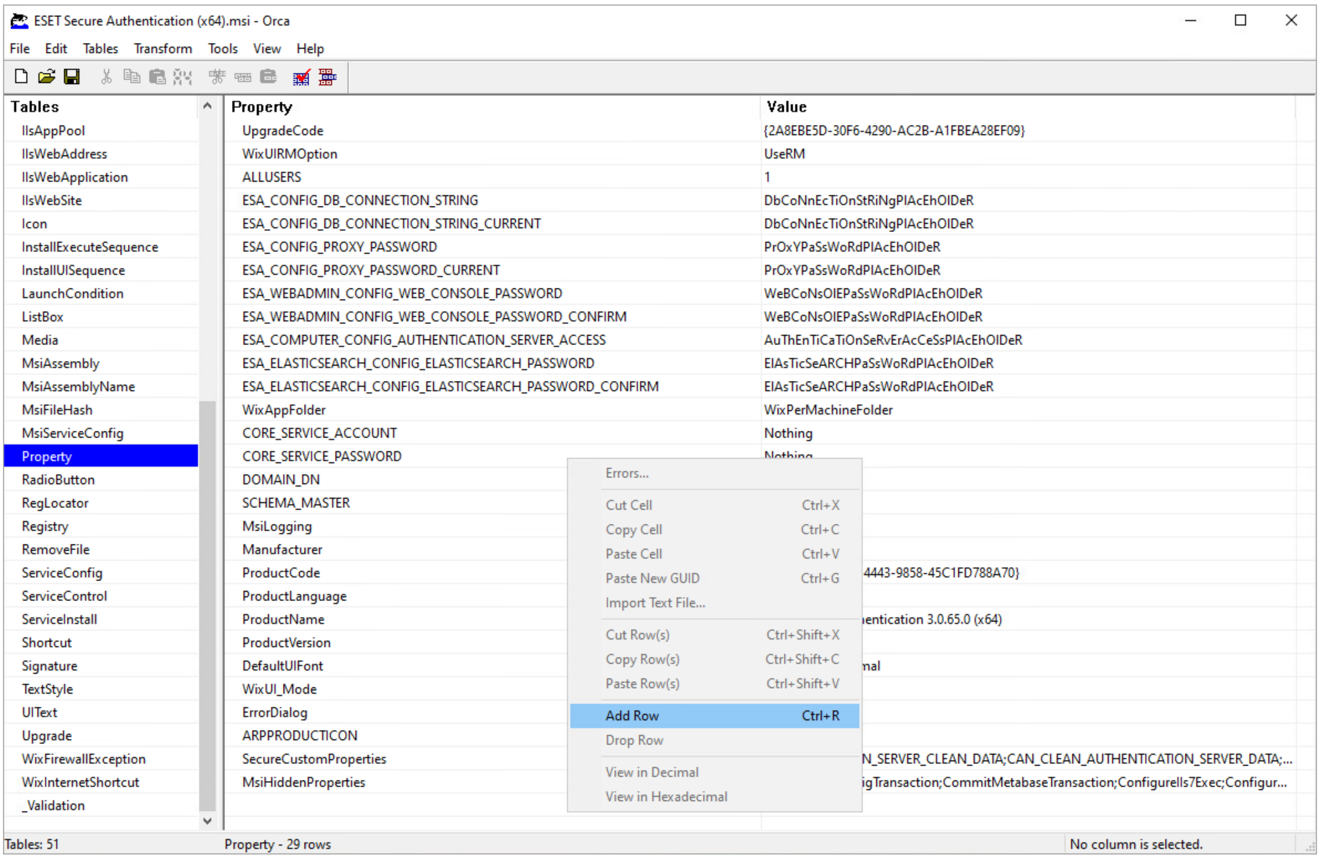


Feature	Feature_Par...	Title	Description	Disp...	Le...	Directo...	Attribu...
Core_Service		Authentication Server	The core ESET Secure Authentication Service	1	2		8
Management_Tools		Management Tools	Plugin for Active Directory Users and Computers for user management and MMC ...	2	2		8
Reports_Elasticsearch		Reporting Engine (Elasticsearch)	Distributed, multitenant-capable full-text search engine requiring Java to be used ...	4	2		8
Win_Credential_Provider		Windows Login	The ESET Secure Authentication for Windows Local Login	6	1		8
Radius_Server		RADIUS Server for VPN Protection	The ESET Secure Authentication RADIUS Server	8	2		8
Credential_Provider		Remote Desktop	The ESET Secure Authentication for Remote Desktop Protocol	10	1		8
Web_Exchange		Microsoft Exchange Server	Two factor support for Microsoft Exchange Server	12	2		8
Web_SharePoint		Microsoft SharePoint Server	Two factor support for Microsoft SharePoint Server	14	2		8
Web_RemoteDesktop		Remote Desktop Web Access	Two factor support for Remote Desktop Web Access	16	2		8
Web_Dynamics		Microsoft Dynamics CRM	Two factor support for Microsoft Dynamics CRM	18	2		8
Web_RemoteAccess		Remote Web Access	Two factor support for Remote Web Access	20	2		8
ADFS3		AD FS	Two factor support for Active Directory Federation Services	22	2		8
Identity_Provider_Connector		Identity Provider Connector	Identity Provider Connector adding two factor support to SAML Identity Providers	24	2		8

i **Color of change**

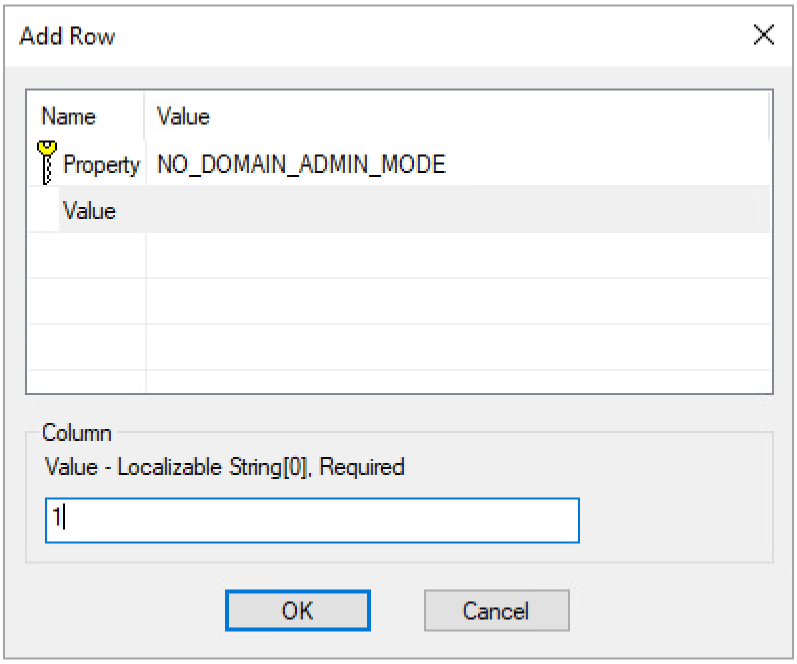
All changes are marked in green.

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



Property	Value
UpgradeCode	{2A8EBE5D-30F6-4290-AC2B-A1FBEA28EF09}
WixUIRMOption	UseRM
ALLUSERS	1
ESA_CONFIG_DB_CONNECTION_STRING	DbCoNnEcTiOnStRiNgPlAcEhOlDeR
ESA_CONFIG_DB_CONNECTION_STRING_CURRENT	DbCoNnEcTiOnStRiNgPlAcEhOlDeR
ESA_CONFIG_PROXY_PASSWORD	PrOxYPaSsWoRdPlAcEhOlDeR
ESA_CONFIG_PROXY_PASSWORD_CURRENT	PrOxYPaSsWoRdPlAcEhOlDeR
ESA_WEBADMIN_CONFIG_WEB_CONSOLE_PASSWORD	WeBCoNsOlEPaSsWoRdPlAcEhOlDeR
ESA_WEBADMIN_CONFIG_WEB_CONSOLE_PASSWORD_CONFIRM	WeBCoNsOlEPaSsWoRdPlAcEhOlDeR
ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ACCESS	AuThEnTiCaTiOnSeRvErAcCeSsPlAcEhOlDeR
ESA_ELASTICSEARCH_CONFIG_ELASTICSEARCH_PASSWORD	ElAsTicSeARCHPaSsWoRdPlAcEhOlDeR
ESA_ELASTICSEARCH_CONFIG_ELASTICSEARCH_PASSWORD_CONFIRM	ElAsTicSeARCHPaSsWoRdPlAcEhOlDeR
WixAppFolder	WixPerMachineFolder
CORE_SERVICE_ACCOUNT	Nothing
CORE_SERVICE_PASSWORD	Nothing
DOMAIN_DN	
SCHEMA_MASTER	
MsiLogging	
Manufacturer	
ProductCode	4443-9858-45C1FD788A70}
ProductLanguage	
ProductName	ientication 3.0.65.0 (x64)
ProductVersion	
DefaultUIFont	
WixUI_Mode	nal
ErrorDialog	
ARPPRODUCTICON	
SecureCustomProperties	N_SERVER_CLEAN_DATA;CAN_CLEAN_AUTHENTICATION_SERVER_DATA;...
MsiHiddenProperties	igTransaction;CommitMetabaseTransaction;Configurells7Exec;Configur...

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

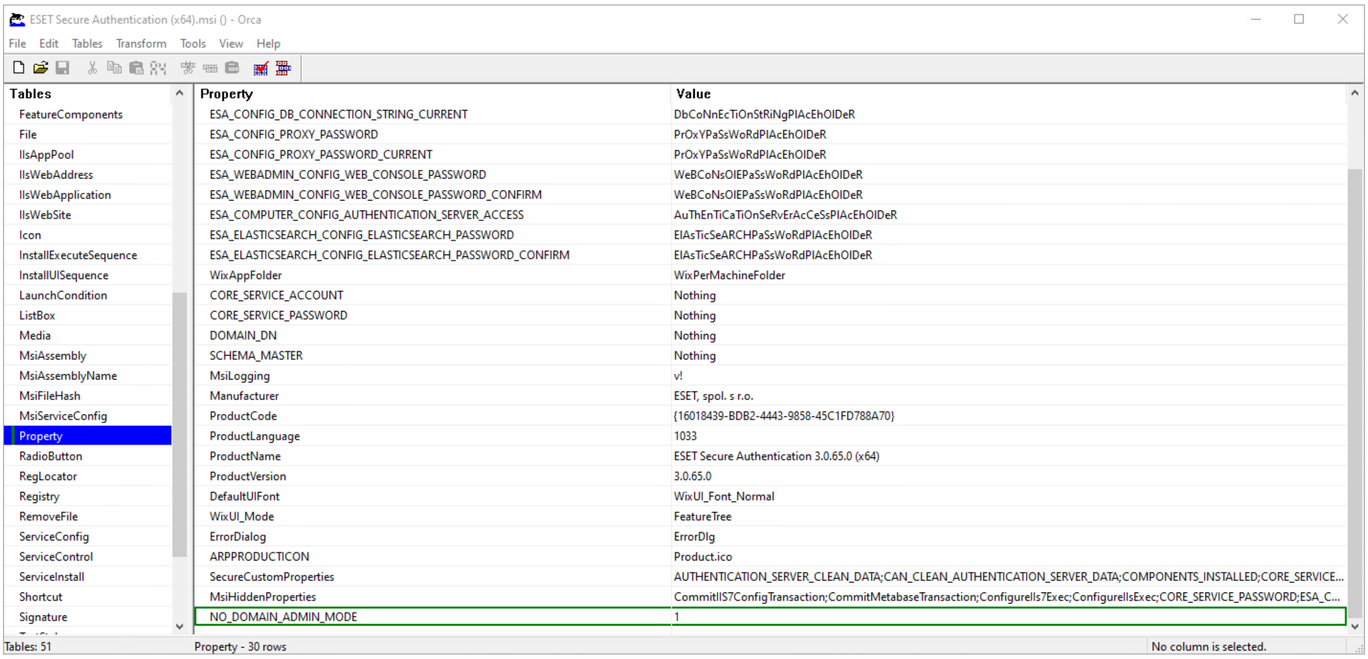


Name	Value
Property	NO_DOMAIN_ADMIN_MODE
Value	

Column

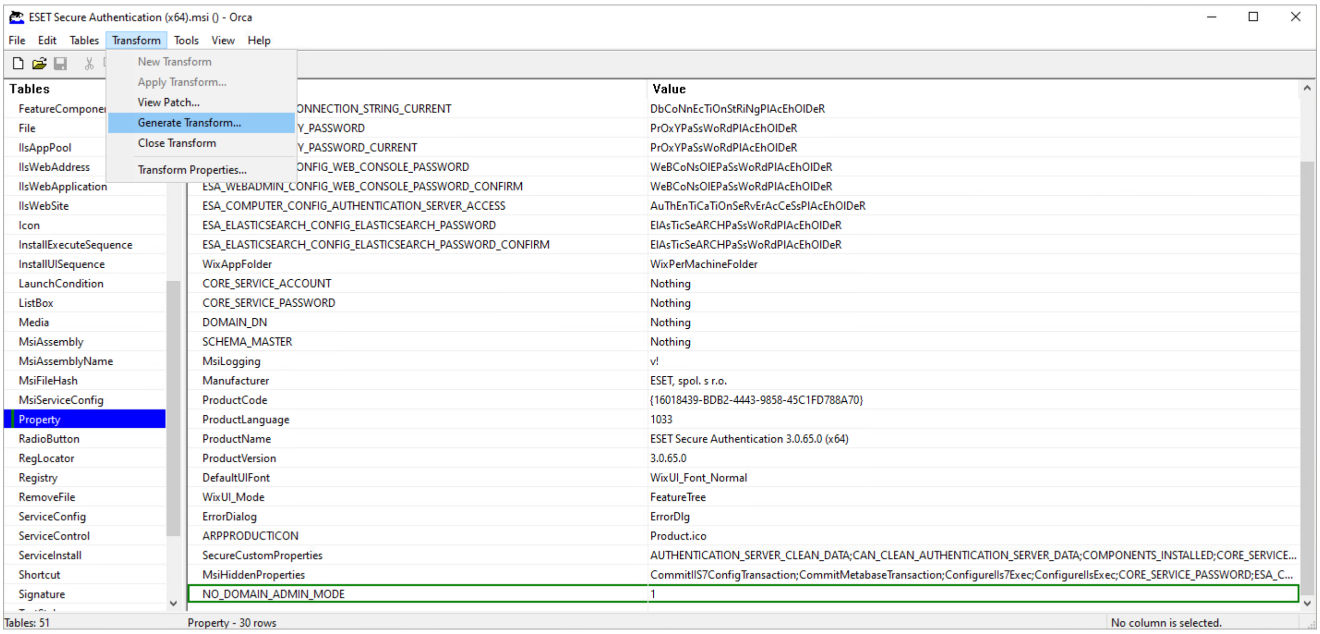
Value - Localizable String[0], Required

1



Property	Value
ESA_CONFIG_DB_CONNECTION_STRING_CURRENT	DbCoNnEcTiOnStRiNgPlAcEhOlDeR
ESA_CONFIG_PROXY_PASSWORD	PrOxYPaSsWoRdPlAcEhOlDeR
ESA_CONFIG_PROXY_PASSWORD_CURRENT	PrOxYPaSsWoRdPlAcEhOlDeR
ESA_WEBADMIN_CONFIG_WEB_CONSOLE_PASSWORD	WeBCoNsOlEPaSsWoRdPlAcEhOlDeR
ESA_WEBADMIN_CONFIG_WEB_CONSOLE_PASSWORD_CONFIRM	WeBCoNsOlEPaSsWoRdPlAcEhOlDeR
ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ACCESS	AuThEnTiCaTiOnSeRvErAcCeSsPlAcEhOlDeR
ESA_ELASTICSEARCH_CONFIG_ELASTICSEARCH_PASSWORD	ElAsTicSeARCHPaSsWoRdPlAcEhOlDeR
ESA_ELASTICSEARCH_CONFIG_ELASTICSEARCH_PASSWORD_CONFIRM	ElAsTicSeARCHPaSsWoRdPlAcEhOlDeR
WixAppFolder	WixPerMachineFolder
CORE_SERVICE_ACCOUNT	Nothing
CORE_SERVICE_PASSWORD	Nothing
DOMAIN_DN	Nothing
SCHEMA_MASTER	Nothing
MsiLogging	v!
Manufacturer	ESET, spol. s r.o.
ProductCode	{16018439-BDB2-4443-9858-45C1FD788A70}
ProductLanguage	1033
ProductName	ESET Secure Authentication 3.0.65.0 (x64)
ProductVersion	3.0.65.0
DefaultUIFont	WixUI_Font_Normal
WixUI_Mode	FeatureTree
ErrorDialog	ErrorDlg
ARPPRODUCTICON	Product.ico
SecureCustomProperties	AUTHENTICATION_SERVER_CLEAN_DATA;CAN_CLEAN_AUTHENTICATION_SERVER_DATA;COMPONENTS_INSTALLED;CORE_SERVICE...
MsiHiddenProperties	CommitIIS7ConfigTransaction;CommitMetabaseTransaction;ConfigureIIs7Exec;ConfigureIIsExec;CORE_SERVICE_PASSWORD;ESA_C...
NO_DOMAIN_ADMIN_MODE	1

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

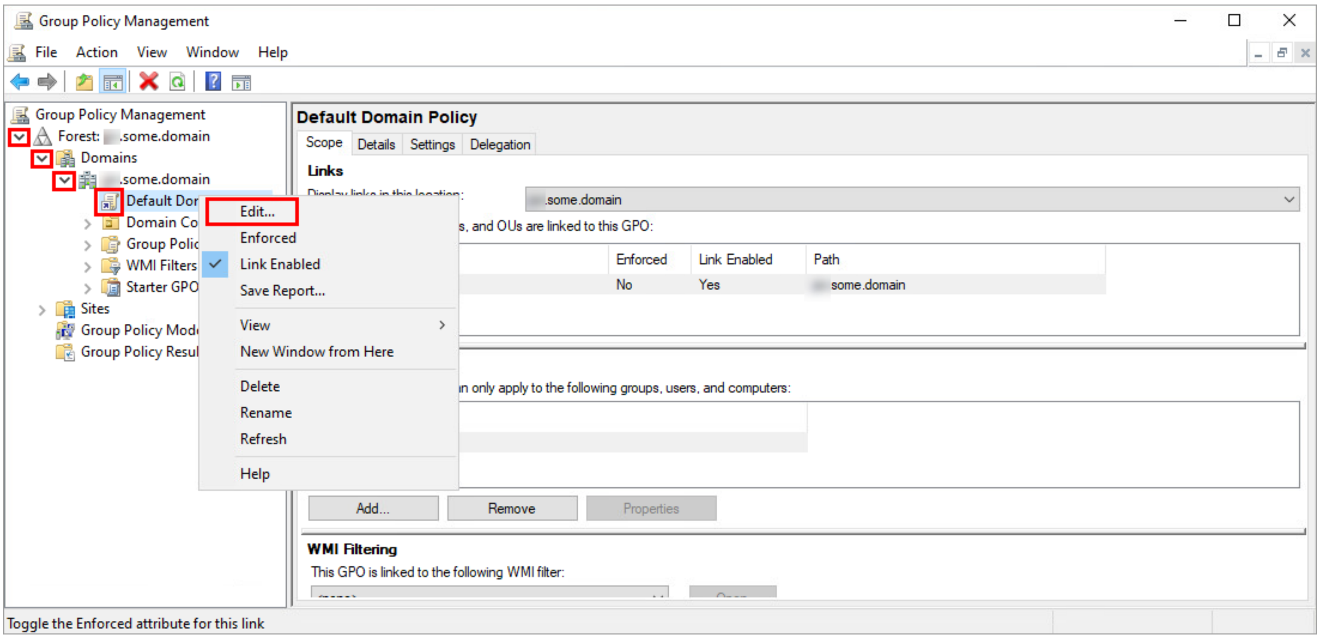


	Value
ONNECTION_STRING_CURRENT	DbCoNnEcTiOnStRiNgPlAcEhOlDeR
Y_PASSWORD	PrOxYPaSsWoRdPlAcEhOlDeR
Y_PASSWORD_CURRENT	PrOxYPaSsWoRdPlAcEhOlDeR
ONFIG_WEB_CONSOLE_PASSWORD	WeBCoNsOlEPaSsWoRdPlAcEhOlDeR
ESA_WEBADMIN_CONFIG_WEB_CONSOLE_PASSWORD_CONFIRM	WeBCoNsOlEPaSsWoRdPlAcEhOlDeR
ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ACCESS	AuThEnTiCaTiOnSeRvErAcCeSsPlAcEhOlDeR
ESA_ELASTICSEARCH_CONFIG_ELASTICSEARCH_PASSWORD	ElAsTicSeARCHPaSsWoRdPlAcEhOlDeR
ESA_ELASTICSEARCH_CONFIG_ELASTICSEARCH_PASSWORD_CONFIRM	ElAsTicSeARCHPaSsWoRdPlAcEhOlDeR
WixAppFolder	WixPerMachineFolder
CORE_SERVICE_ACCOUNT	Nothing
CORE_SERVICE_PASSWORD	Nothing
DOMAIN_DN	Nothing
SCHEMA_MASTER	Nothing
MsiLogging	v!
Manufacturer	ESET, spol. s r.o.
ProductCode	{16018439-BDB2-4443-9858-45C1FD788A70}
ProductLanguage	1033
ProductName	ESET Secure Authentication 3.0.65.0 (x64)
ProductVersion	3.0.65.0
DefaultUIFont	WixUI_Font_Normal
WixUI_Mode	FeatureTree
ErrorDialog	ErrorDlg
ARPPRODUCTICON	Product.ico
SecureCustomProperties	AUTHENTICATION_SERVER_CLEAN_DATA;CAN_CLEAN_AUTHENTICATION_SERVER_DATA;COMPONENTS_INSTALLED;CORE_SERVICE...
MsiHiddenProperties	CommitIIS7ConfigTransaction;CommitMetabaseTransaction;ConfigureIIs7Exec;ConfigureIIsExec;CORE_SERVICE_PASSWORD;ESA_C...
NO_DOMAIN_ADMIN_MODE	1

Create a Software Installation task via GPO

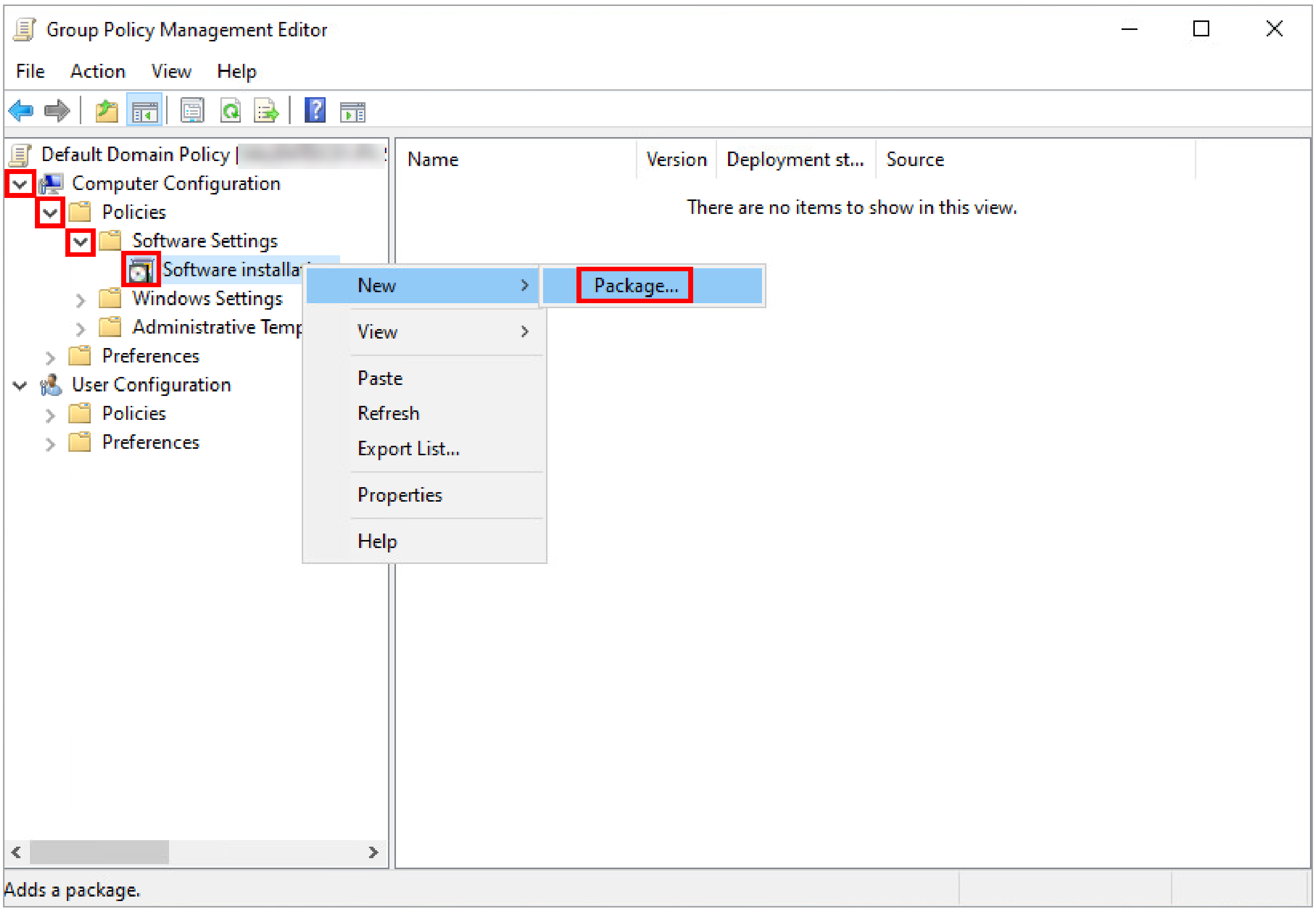
The steps below are demonstrated in Microsoft Server 2022.

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

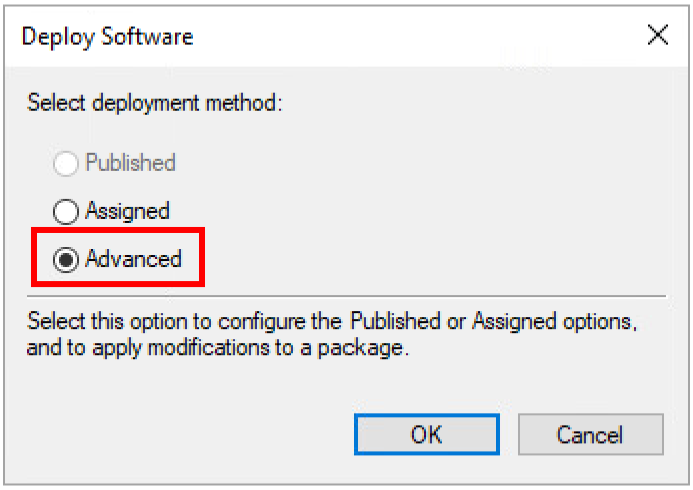


2. In **Group Policy Management Editor**, under your domain policy, expand **Computer Configuration** > **Policies** > **Software Settings**.

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**.



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



Select deployment method:

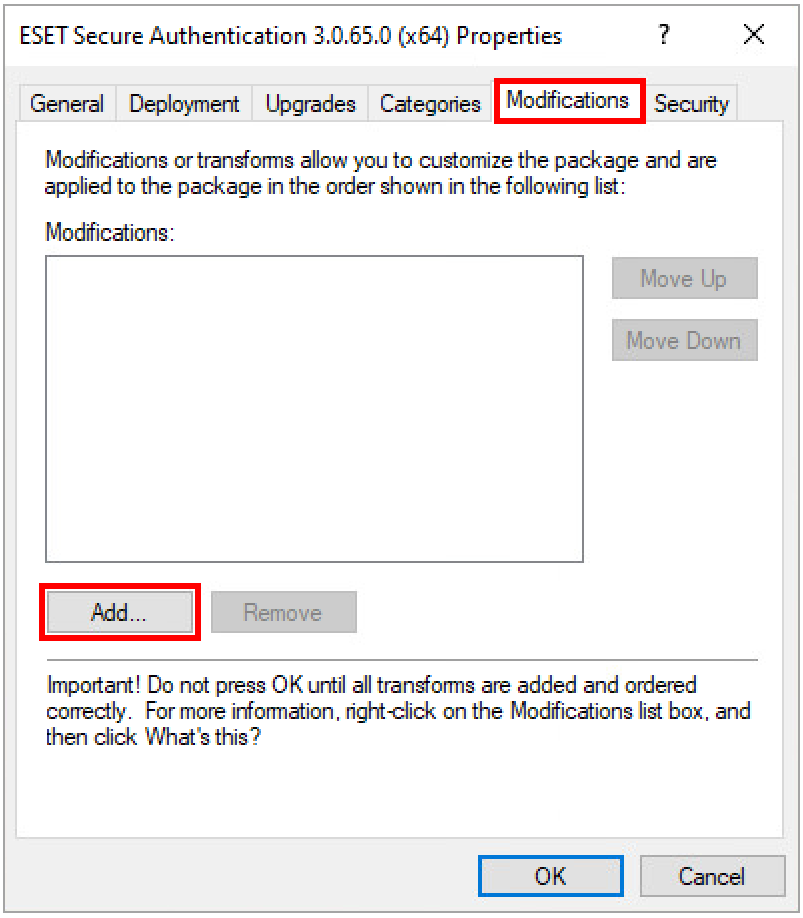
○ Published

○ Assigned

● Advanced

Select this option to configure the Published or Assigned options, and to apply modifications to a package.

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



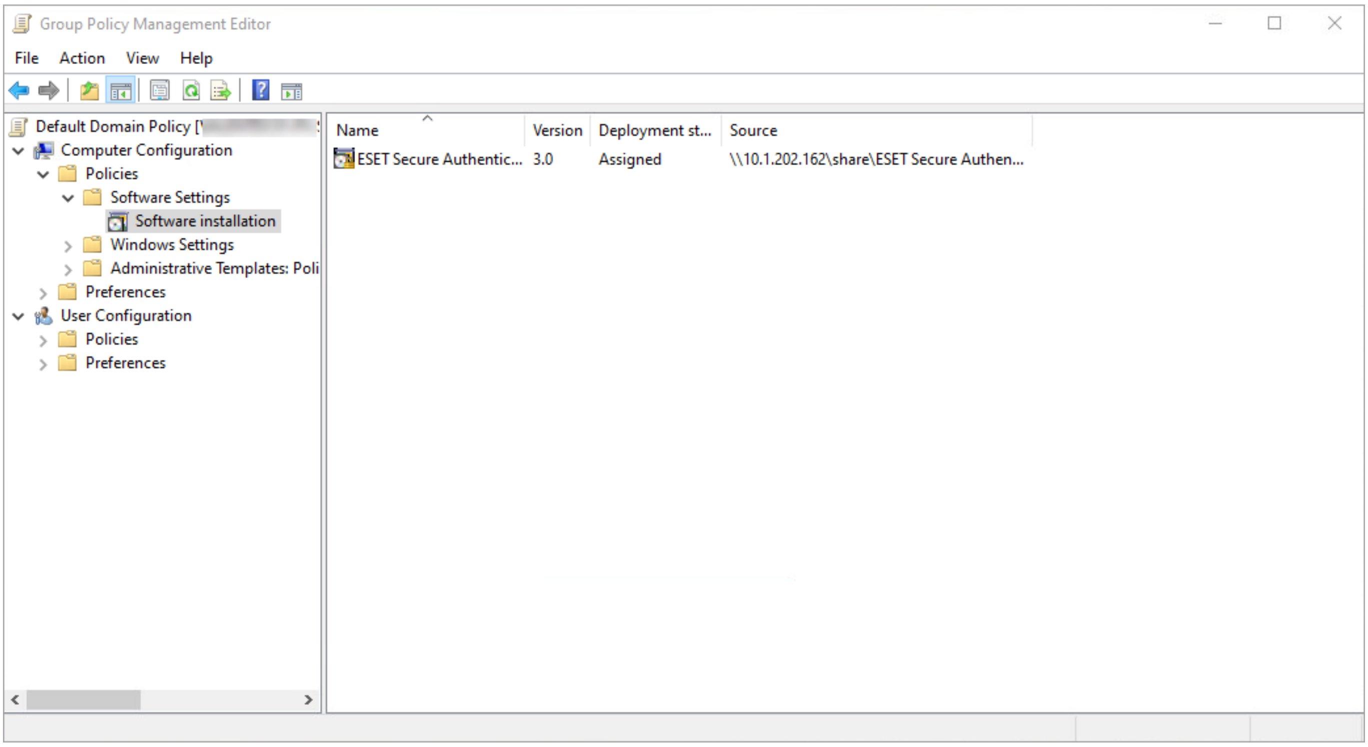
Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?

6. Navigate to the ESA installer transform file (in the same location you referenced in step 3), type 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**.



Name	Version	Deployment st...	Source
ESET Secure Authentic...	3.0	Assigned	\\10.1.202.162\share\ESET Secure Authen...

8. The package will be installed on 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.

MSI arguments

Several arguments can be used when using the .MSI installer either as a Logon script or Installation task.

Launch the `.MSI` installer to see all available arguments with an explanation and examples.

To install or remove ESA components without a Domain Admin user, use `NO_DOMAIN_ADMIN_MODE=1`. Then check the installation logs for further instructions marked as "Manual configuration needed".

Examples when deploying ESA components via ESET PROTECT

Partial list of ESA .MSI arguments

To specify ESA components to be installed, the `ADDLOCAL` argument is used. Possible values include the following:

- Core_Service - Authentication Server
- Reports_Elasticsearch - Reporting Engine (Elasticsearch)

- Win_Credential_Provider - Windows Login
- Radius_Server - RADIUS Server for VPN Protection
- Credential_Provider - Remote Desktop
- Web_Exchange - Microsoft Exchange Server
- Web_SharePoint - Microsoft SharePoint Server
- Web_RemoteDesktop - Remote Desktop Web Access
- Web_Dynamics - Microsoft Dynamics CRM
- Web_RemoteAccess - Remote Web Access
- ADFS3 - AD FS 3 or later
- Identity_Provider_Connector - Identity Provider Connector

To install more features, separate them by comma, for example:
`ADDLOCAL="Credential_Provider,Win_Credential_Provider"`

To specify a 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 you are 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.

To set an initial username and password for the ESA Web Console when installing the Authentication Server (`Core_service`), use:

- ESA_CONFIG_WEB_CONSOLE_USER
- ESA_CONFIG_WEB_CONSOLE_PASSWORD

`Core_Service` (Authentication Server) advanced configuration arguments:

- ESA_CONFIG_DB_TYPE (database type, Standalone mode only, use "sqlite", "postgresql", or "mssql")
  - ESA_CONFIG_DB_CONNECTION_STRING (database connection string, Standalone mode only)

- ESA_CONFIG_PROXY_ENABLED (use value true to enable custom HTTP proxy settings)
- ESA_CONFIG_PROXY_SERVER (leave blank to not use proxy)
- ESA_CONFIG_PROXY_PORT
- ESA_CONFIG_PROXY_USER
- ESA_CONFIG_PROXY_PASSWORD

To set a custom RADIUS port, use `ESA_CONFIG_RADIUS_PORT`.

For complete removal of the ESA Authentication Server, including configuration data, use `AUTHENTICATION_SERVER_CLEAN_DATA=1`.

Examples of using ESA .MSI arguments when deploying ESA components through ESET PROTECT

Example - Install Windows Login and Remote Desktop (Standalone mode)

```
ADDLOCAL="Win_Credential_Provider,Credential_Provider" ESA_COMPUTER_CONFIG_INTEGRATI
ON_MODE=2 ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ADDRESS=192.168.0.15:8001 ESA_CO
MPUTER_CONFIG_AUTHENTICATION_SERVER_ACCESS=DKNO-XESE-WXUA-QNXW-
JAEI TRUSTED_CERT_HASH=2CD61594DDE3E63E6BEBB9BF3DC95B85550FD5D8
```

Example - Install Windows Login and Remote Desktop as a no domain admin user (Active Directory Integration mode)

```
ADDLOCAL="Win_Credential_Provider,Credential_Provider" NO_DOMAIN_ADMIN_MODE=1
```

Do not forget to add the computer(s) to EsaServices manually.

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 uninstall the previous version manually.

> **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, upgrade all of them. Before upgrading any of them, the other ones must be stopped to maintain data compatibility.

1. Review the license agreement and privacy policy and click **I accept** to continue.
2. Type the desired username and password to be used to access ESA Web Console if prompted.
3. 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 `ESA Web Console` will be automatically created on your Windows OS desktop. Double-click the shortcut to open the Web Console.

ℹ ESA Web Console certificate

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

Type 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 would 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 the 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, AD FS, RADIUS) on the affected computers.

.EXE installer versus .MSI installer

You can combine the .EXE installer (also known as bootstrapper) and .MSI installer in some cases.

Original state	Operation	Supported
Installed via .MSI installer	Upgrade via .EXE installer	Yes
Installed via .MSI installer	Change via .EXE installer	No
Installed via .MSI installer	Repair via .EXE installer	No
Installed via .MSI installer	Uninstall via .EXE installer	Yes
Installed via .EXE installer	Upgrade via .MSI installer	Yes
Installed via .EXE installer	Change via .MSI installer	No
Installed via .EXE installer	Repair via .MSI installer	No
Installed via .EXE installer	Uninstall via .MSI installer	Yes

Compatibility of ESA Components

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

Compatibility table - component connecting to Authentication Server 3.0

Component	Component v2.4	Component v2.5	Component v2.6	Component v2.7	Component v2.8	Component v3.0
Windows Login	OK*	OK*	OK	OK	OK	OK
RDP	OK*	OK*	OK	OK	OK	OK
AD FS	OK*	OK*	OK	OK	OK	OK
RADIUS	FAIL	FAIL	OK	OK	OK	OK

Component	Component v2.4	Component v2.5	Component v2.6	Component v2.7	Component v2.8	Component v3.0
IIS	FAIL	FAIL	OK	OK	OK	OK
Management Tools (ADUC, MMC)	FAIL	FAIL	FAIL	FAIL	OK	OK
Identity Provider Connector						OK

* Works if the component was registered (used) with the corresponding version of Authentication Server (2.4 or 2.5) before upgrading Authentication Server to version 3.0.

> **Cannot register a new component with an old server**
> You cannot register later component versions with an earlier server version. The connection will fail due to compatibility issues and you will receive a notification of the error.

Database migration (Export Data)

Use the ESET Secure Authentication 3.0 and later database migration (**Export Data**) functionality to:

- Move from **Active Directory Integration** mode to **Standalone** mode

- Switch from a built-in database to an external database when the Authentication Server is installed in **Standalone** mode

> **Supported database types; Moving from Active Directory Integration mode to Standalone mode; Backing up Master Recovery Key for Windows Login**
> Migration is only available for supported database types.
> When moving from **Active Directory Integration** mode to **Standalone** mode, the information about ESA components connecting in **Active Directory Integration** mode is not migrated. These components must be re-installed using Standalone mode after the migration is complete.
> Master Recovery Key (MRK) for Windows Login can be requested after the migration. Back up your MRK for Windows Login before you start the migration.

> **Restoring an old backup**
> If you use **Export Data** to back up the Authentication Server's data, the backup contains authentication counters. Suppose you keep using the specific ESA instance, and later you restore the backup data or use it in a new ESA instance; the users will be able to log in using old OTPs (used before the backup). This is a security issue.

How to export data

1. Log in to the ESA Web Console.

2. Select **Settings** > **Export Data**.

3. Select a database type for **Target Database Type**:

- **SQLite**

  o Create a directory on the computer where the Authentication Server is installed.

oType the path leading to that directory in the SQLite Directory field.

- **Microsoft SQL Server**, **PostgreSQL**

oDefine the database connection information in the **Connection string** field. Click **Show examples** to display the correct format.

4. Click **Export**.

> Two-factor authentication is inactive during database migration
>
> i It is essential to disable the ESACore (Authentication Server) service to avoid migration issues. Because of this, two-factor authentication will not work during the migration.

Sample scenario for moving to another deployment type (Active Directory Integration mode to Standalone mode) or database type

1. Export data.

2. Stop the ESACore (Authentication Server) service in Windows Services.

3. Install the new Authentication Server in **Standalone** mode:

a.In the **Advanced Configuration** screen, select the **Database type** you used when exporting data.

- **SQLite**

oCopy the exported database files to *C:\ProgramData\ESET Secure Authentication\db* and continue the installation

- **Microsoft SQL Server**, **PostgreSQL**

oDefine the connection details of the database containing the exported data

b.Define new **Web Console Administrator Account** information if prompted by the installer.

c.Navigate through the remaining steps as prompted by the installer and close the installer when complete.

4. Remove the previous installation of the Authentication Server:

- Do not select **Remove all program and user data including product configuration** if you want to return to the previous installation later.

5. If **Remove all program and user data including product configuration** was selected in the previous step, re-activate your ESA license on your new Authentication Server.

6. If moving from Active Directory Integration mode, re-install all ESA Components in **Standalone** mode.

7. Make the new Authentication Server certificates trusted on computers where ESA Components are installed.

8. If old Authentication Server entries appear in the ESA Web Console, remove them.

Sample scenario on moving the Authentication Server to another computer

Active Directory Integration mode

1. Stop the ESACore (Authentication Server) service in Windows Services
2. Install the Authentication Server to the new computer belonging to the same Windows Domain
3. Remove the old Authentication Server.

Standalone mode

1. Stop the ESACore (Authentication Server) service in Windows Services.
2. Install the new Authentication Server to the new computer:
   - In the **Advanced Configuration** screen, select the original Authentication Server installation **Database type**:
     - **SQLite** (built-in database):
       1. Copy the content of the *C:\ProgramData\ESET Secure Authentication\db* directory to the target computer to the same location.
       2. Define new **Web Console Administrator Account** information, if prompted by the installer.
       3. Navigate through the remaining steps as prompted by the installer and close the installer when complete.
       4. In ESA Web Console, remove the old Authentication Server entry.
     - **Microsoft SQL Server**, **PostgreSQL**
       1. Define the external database's connection string.
       2. Navigate through the remaining steps as prompted by the installer and close the installer when complete.
3. Make the new Authentication Server certificates trusted on computers where ESA Components are installed.

External Access

What will be available?

- Authentication Server
  - Access to the Web Console
  - Components installed in Standalone mode can connect to the Authentication server using invitations

    - Custom solutions utilizing API:
        - New API (ESA 2.8 and later) endpoints: `/`, `/auth/v2`, `/manage/v2`
        - Old API (ESA 2.7 and earlier) endpoints: `auth/v1`, `manage/useres/v`
- Identity Provider Connector web page

Types of external access

- VPN
- Reverse proxy
- Transparent proxy

After setting up a reverse proxy or transparent proxy, you have to configure ESA to use the external address for invitations and Identity Provider Connector.

Configure ESA for external access

To make the Authentication Server or Identity Provider Connector publicly available:

I.**Authentication Server**

Configure the external address to use invitations when installing ESA Components in Standalone mode.

1. In the ESA Web Console, navigate to **Components** > **Invitations** > **Server Access**.
2. Click **Edit** (pencil icon) under **External Access**.
3. Type in the external address with the port included, and press **Enter**.
4. If you do not want the Authentication Server's internal address included in the invitation details, select the corresponding check box.
5. Click **Save**.

II.**Identity Provider Connector (IdP Connector)**

1. In the ESA Web Console, navigate to **Components** > **Identity Provider Connector** > select a configured IdP connector, click **Settings**.
2. Change the **Site URL** to the external address where the Authentication Server is available.
3. Click **Apply**.

Multiple addresses for the Authentication Server

ESA components connect to the Authentication Server (AS) via the address indicated in the invitation.

To provide multiple addresses the components can connect to, follow the steps below.

Installation using the .EXE installer

1. When the component has been installed, open `C:\ProgramData\ESET Secure Authentication\ESA.config`.

2. Add `<add key="AuthenticationServerAddress_Other" value="<desired_addresses>" />` right above `</appSettings>`.

3. Replace `<desired_addresses>` with the additional addresses of the AS, separate them with a semicolon.

4. Save the changes.

Silent installation (.MSI)

If you are using the .MSI installer, use the `ESA_COMPUTER_CONFIG_AUTHENTICATION_SERVER_ADDRESS_OTHER` argument to define the additional addresses of AS. Use a semicolon to separate multiple addresses.

Using reverse proxy

Reverse proxy has its certificate, decrypts the incoming communication, and encrypts its again using the target server certificate.

When using ESET Secure Authentication behind a reverse proxy server (for example, to make the Authentication Server accessible via public domain address), consider the information below.

- In invitation details:
  - Use the IP address of the proxy server instead of the name of the 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 the invitation, use the IP address of the proxy server instead of the name of the 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.

See how to configure proxy for ESA

Configure proxy for ESA

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

Configure the Nginx reverse proxy while applying the settings below. Use one of the sample configuration scripts below in the `nginx.conf` file, for example right after the `events { ... }` part.

1. Use **ip_hash** to ensure:

   - A component always connects to the same server
   - When accessing the Web Console, the browser always contacts the same server

2. Set the listening port to 443.

3. Define the SLL certificate you generated. [Example of generating a self-signed certificate](#).

The sample configuration snippets assume the custom generated certificate and certificate key are located at "`D:\ESAcustomCertificate.crt`" and "`D:\ESAcustomCertificate.key`".

Sample configuration snippet - single authentication server

```
http {
    sendfile on;

    upstream esa_servers {
        ip_hash;
        server esa01.local:8001;
    }
    server {
        listen 443 ssl;
        ssl_certificate D:\ESAcustomCertificate.crt;
        ssl_certificate_key D:\ESAcustomCertificate.key;
        location / {
            proxy_pass          https://esa_servers;
            proxy_redirect      off;
            proxy_set_header    Host $host;
            proxy_set_header    X-Real-IP $remote_addr;
            proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header    X-Forwarded-Host $server_name;
        }
    }
}
```

Sample configuration snippet - multiple authentication servers

```
http {
    sendfile on;

    upstream esa_servers {
        ip_hash;
        server esa01.local:8001;
        server esa02.local:8001;
    }
    server {
        listen 443 ssl;

        ssl_certificate D:\ESAcustomCertificate.crt;
        ssl_certificate_key D:\ESAcustomCertificate.key;

        location / {
            proxy_pass          https://esa_servers;
            proxy_redirect      off;
            proxy_set_header    Host $host;
            proxy_set_header    X-Real-IP $remote_addr;
            proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header    X-Forwarded-Host $server_name;
        }
    }
}
```

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 Nginx machine's certificate store, specifically to **Certificates (Local Computer)** > **Trusted People**.

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

Add Certificate exception

Mozilla Firefox

1. Click **Advanced** > **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 the address bar, click **Certificate error** > **View certificates** and then click **Install Certificate**.
3. In the Certificate Import Wizard window, select **Local Machine** for Store Location, click **Next**.
4. On the next screen, select **Place all certificates in the following store** and click **Browse**.
5. Select **Show physical stores** check box, select **Trusted Root Certification Authorities** and then click **OK**.
6. Click **Next** and click **Finish**.
7. Restart the computer.

Microsoft Edge

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.

Transparent proxy

A transparent proxy forwards the secure communication (HTTPS stream) without any change to it.

1. Re-generate the server certificate.
2. Replace the server certificate with the re-generated one.
3. Make the server certificate trusted where needed.

SSL Certificate

The Authentication Server and API utilize an SSL certificate to secure communications from eavesdropping. The installer automatically selects an appropriate certificate installed on the machine or generates a new self-signed certificate if none is found.

- Generate custom SSL Certificate
- Replace the SSL Certificate

Replacing the SSL Certificate

Quick links: Importing the New Certificate, Replacing the ESA Certificate, Replacing the ESA IdP Connector Certificate

The Authentication Server and API utilize an SSL certificate to secure communications from eavesdropping. The installer automatically selects an appropriate certificate installed on the machine or generates a new self-signed certificate if none is found.

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

Prerequisites

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 want to use in PKCS12 format (.pfx or .p12)

oThe certificate file must contain a copy of the private key as well as the public key

Importing the New Certificate

The new certificate must be placed in the Local Machine\Personal store before use.

1. Launch the Microsoft Management Console (MMC):

a.Click **Start** > type “mmc.EXE” and press **Enter**.

2. Add the Certificates snap-in:

a.Click **File** > **Add/Remove Snap-in**.

b.Select **Certificates** from the left-hand column.

c.Click **Add**.

d.Select **Computer account**.

e.Click **Next**.

f.Select **Local computer**.

g.Click **Finish**.

h.Click **OK**.

3. To save the snap-in for future use, click **File** > **Save**.

4. Select the **Certificates (Local Computer)** > **Personal** node in the tree.

5. Right-click and select **All tasks** > **Import**.

6. Follow the Import Wizard, be sure to add the certificate in the **Personal** certificate store location.

7. Double-click the certificate and verify the line **You have a private key that corresponds to this certificate** is displayed.

Replacing the ESA Certificate

> ℹ The Authentication Server does not start without a 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. In the **Personal** folder, double-click the applicable certificate.

3. In the **General** tab, verify the **You have a private key that corresponds to this certificate** message is displayed.

4. In 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 **Enter**.

4. Copy and paste the **Certificate Hash** field somewhere safe ifse 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=0.0.0.0:8001 appid={BA5393F7-AEB1-4AC6-B759-1D824E61E442} certhash=<THUMBPRINT>`, but replace `<THUMBPRINT>` with the values from the certificate thumbprint without any spaces and press **Enter**.

8. You should see **SSL Certificate successfully added**.

9. Restart the ESACore service for the new certificate to take effect.

Replacing the ESA IdP Connector Certificate

1. On your Windows Server, launch **Internet Information Services (IIS) Manager**.

2. Navigate to **<your_domain>** > **Sites**.

3. Right-click and select **ESA Identity Provider Connector** > **Edit Bindings**.

4. Double-click **https**.

5. Select the new certificate from **SSL certificate**.

6. Click **OK > Close**.

To change the port of ESA IdP Connector:

1. On your Windows Server, launch **Internet Information Services (IIS) Manager**.

2. Navigate to **<your_domain>** > **Sites**.

3. Right-click and select **ESA Identity Provider Connector** > **Edit Bindings**.

4. Double-click **https**.

5. Change the **Port** value.

6. Click **OK** > **Close**.

The IdP Connector certificate private key is readable only by the Local System user; therefore, there can be a problem in re-configuring binding in the IIS manager on some systems. If you encounter this problem, you can generate a custom certificate and replace the default one.

Generate a custom (self-signed) SSL Certificate

Generate self-signed certificate using Windows PowerShell

Generate a custom SSL certificate and import 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 subject name version displayed in the ESA Web Console at **Components** > **Invitations** > **Server access**.
   If you define multiple DnsNames, for example:
   `-DnsName "my.esa.installation.com", "my.authentication.server", "twofactor.auth"`

   The first entry ("`my.esa.installation.com`" in above example) will be used in the `Subject` field, and subsequent entries are used in the `Subject Alternative Name` field of the certificate.

   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. To open the **Run** dialog, press the Windows key + R.

4. Add the Certificate snap-in:

   a.Type `mmc` and press **Enter**.

   b.Click **File** > **Add/Remove Snap-in**.

   c.Select **Certificates** > **Add**.

   d.Select **Computer Account**, click **Next**, and then click **Finish**. Click **OK** to close the **Add or Remove Snap-ins** window.

5. Import the applicable certificate:

a.In the left pane of MMC, expand **Certificates (Local Computer)** > **Personal**, and right-click **Certificates**.

b.Select **All Tasks** > **Import**.

c.In the import wizard, click **Next**, click **Browse**; from the file extension drop-down menu, select **Personal Information Exchange (*.pfx, *.p12)**, locate the exported certificate file, click **Open**, and then click **Next**.

d.Type the password used in the second command above and click **Next**.

e.Select **Place all certificates in the following store** and type Personal for the store name. Click **Next** and click **Finish**.

6. In the left pane of MMC expand **Certificates (Local Computer)** > **Trusted Root Certification Authorities**, and right-click **Certificates**.

7. Select **All Tasks** > **Import**, and repeat steps 6a to 6c.

8. Double-click the certificate in **Certificates (Local Computer)** > **Personal** > **Certificates** and verify the line **You have a private key that corresponds to this certificate** is displayed.

If you need a .crt and .key file instead of .pfx, convert .pfx to .crt and .key using OpenSSL or other preferred method.

Convert .pfx to .crt, .key using OpenSSL

Verify OpenSSL for Windows is installed and then execute the commands below.

```
openssl pkcs12 -in D:\ESAcustomCertificate.pfx -clcerts -nokeys -
out D:\ESAcustomCertificate.crt
```

When the **Enter Import Password** is displayed, type the password defined in the Export-PfxCertificate command when generating the Certificate via Windows PowerShell.

```
openssl pkcs12 -in D:\ESAcustomCertificate.pfx -nocerts -
out D:\ESAcustomCertificate_encrypted.key
```

For **Enter PEM pass phrase**, define a new password at least four characters long.

```
openssl rsa -in D:\ESAcustomCertificate_encrypted.key -
out D:\ESAcustomCertificate.key
```

When prompted, type the same password you defined for **Enter PEM pass phrase**.

Generate self-signed certificate using OpenSSL

Verify OpenSSL for Windows is installed.

Create a configuration file

To avoid an "Invalid certificate" warning, the *ESAcustomCertificate.conf* file must 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 *ESAcustomCertificate.conf* file:

```
[ req ]
default_bits       = 4096
distinguished_name = req_distinguished_name
req_extensions     = req_ext
x509_extensions    = x509_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          = my.esa.installation.com

[ req_ext ]
subjectAltName = @alternative_names

[ x509_ext ]
subjectAltName = @alternative_names

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

DNS.3   = twofactor.auth

DNS.4   = 192.168.0.1

IP.1    = 192.168.0.1
```

Generate an OpenSSL certificate and key using Windows command line.

```
openssl req -config D:\ESAcustomCertificate.conf -new -x509 -sha256 -
newkey rsa:2048 -nodes -keyout D:\ESAcustomCertificate.key -days 365 -
out D:\ESAcustomCertificate.crt
```

If the `commonName` was pre-configured correctly in the configuration file, press **Enter** when the **CommonName** prompt is displayed.

Making Certificates Trusted

Certificates signed by a generally trusted certification authority will be automatically trusted everywhere.

Certificates that need to be made trusted:

- Self-signed certificates
- Certificates signed using some custom certification authority. The custom certification authority also has to be made trusted.

Most browsers can work with untrusted certificates while they display a warning. You can avoid the warning by adding a certificate exception; however, this is not recommended.

Adding certificates to the System Store

What does it work for?

- Components connecting to the Authentication Server
- Some browsers, for example, Internet Explorer, Microsoft Edge, Google Chrome

What does it not work for?

- Firefox
- Accessing the customer API through solutions that do not use the system store to check for certificates

Where to import within System Store?

- Current User / Local machine
  - **Current User** - Only works for the current user (for example, access from a browser)

  - **Local machine** - Works everywhere (for example, ESA components running as Local System)

- Trusted People / Trusted Root Certification Authorities
  - Use Trusted Root Certification Authorities if it is a certification authority certificate

How to import?

Use the certificate file:

1. Double-click the certificate file (for example, .crt).
2. Select **Install Certificate**, and follow the installation wizard instructions.

Use the MMC console:

1. Press ⊞ **+ R**, type `mmc.EXE`, and press **Enter**.
2. Click **File** > **Add/Remove Snap-in** > **Certificates** > **Add**.
3. Select **Computer account**, click **Next**.
4. Select **Local computer**, click **Finish**, then click **OK**.
5. In the left navigation pain expand one of these:

   a)**Certificates** > **Trusted people** to import a self-signed certificate

   b)**Certificates** > **Trusted Root Certification Authorities**
6. Right-click **Certificates**, select **All Tasks** > **Import**.
7. Follow the instructions of **Certificate Import Wizard**.

When installing an ESA component on a computer in **Standalone** mode, the invitation adds the certificate information received from the Authentication Server to the **Trusted People** store.

HTTP Strict Transport Security

The HTTP Strict-Transport-Security (HSTS) response header enables a website (domain) to tell browsers that it should only be accessed using HTTPS instead of HTTP. This mechanism helps to protect websites against cyberattack.

To turn HSTS on for the ESA Authentication Server:

1. Open the `C:\Program Files\ESET Secure Authentication\EIP.Core.WindowsService.exe.config` file with a text editor, for example, Notepad.
2. Add `<add key="StrictTransportSecurityEnabled" value="true" />` to that file after the `<appSettings>` tag.

Example of an altered EIP.Core.WindowsService.EXE.config file

```
<?xml version="1.0" encoding="utf-8"?>
...
<configuration>
  <appSettings>
    <add key="StrictTransportSecurityEnabled" value="true" />
 ...
  </appSettings>
   ...
</configuration>
...
```

`...` represent existing code in the `.config` file to be left intact.

3. Restart the **ESACore** service

To turn HSTS on for ESA Identity Provider Connector, apply the above mentioned changes in the `C:\Program Files\ESET Secure Authentication\IdentityProviderConnector\Web.config` file.

> ℹ Beware of browsers remembering the HSTS setting per domain. Enabling HSTS in your ESA instance may influence other websites accessible from the same domain (or hostname) as your ESA instance.
> To avoid such an issue, make your ESA instance accessible at a separate domain (hostname) . Add the domain to the DNS records or hosts file and regenerate the ESA certificate to include that domain in the certificate's subject name (and/or Subject Alternative Name).

Geo located DNS support

This topic only applies if ESA is installed in Active Directory Integration mode.

If there are several sites in your Active Directory domain based on geographic location, each computer connected to your domain belongs to a specific site.

If an Authentication Server is installed on each site, verify the appropriate computers authenticate against the corresponding authentication server.

The steps below describe how to add a Service Location (SRV) record in a Windows Server 2012 R2 operating system.

1. On your main computer, which is the domain controller, click **Start** > **Administrative Tools** > **DNS**.

2. In the **DNS Manager**, expand **Forward Lookup Zones** > **<your domain>** > **_sites**.

3. Look up **_tcp** for each site under**_sites**.

4. Right-click a **_tcp**, select **Other New Records** > **Service Location (SRV)**, click **Create Record**.

5. Type `_esetsecauth` in the **Service** field, and `_tcp` in the **Protocol** field.

6. Set the **Priority** and **Weight** to 100.

7. Set the **Port number** to `8000`, unless you changed the port number during Authentication Server installation.

8. Type the fully qualified domain name (FQDN) of the applicable Authentication Server in the corresponding site.

9. Click **OK**, click **Done**.

Getting started with ESET Secure Authentication Web Console

When 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 Authentication Server machine, 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** > **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

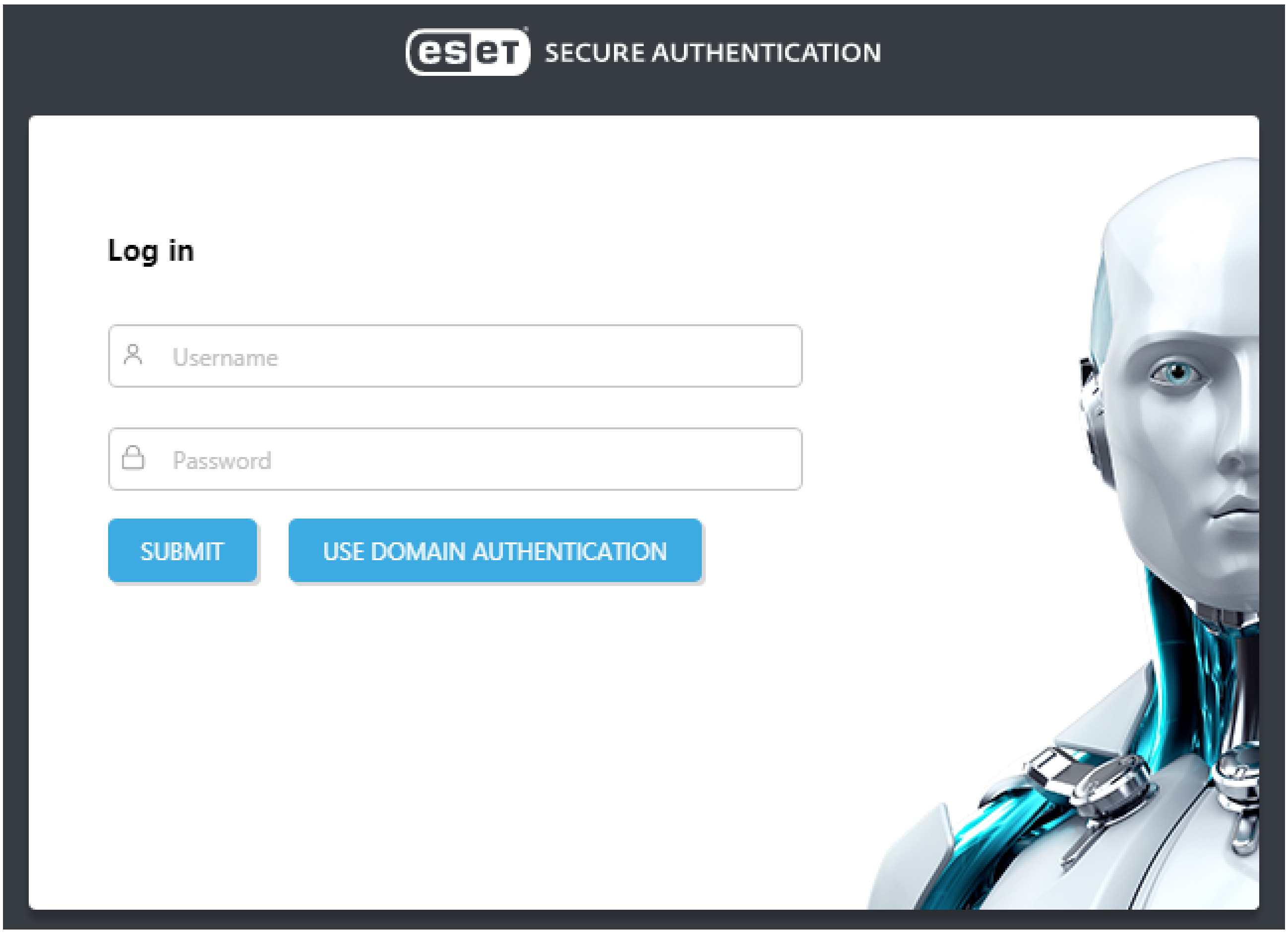
1. Click **Continue to this website (not recommended)**.
2. In the right section of the address bar, click **Certificate error** > **View certificates** and then click **Install Certificate**.
3. In the Certificate Import Wizard window, select **Local Machine** for Store Location, click **Next**.
4. On the next screen, select **Place all certificates in the following store** and click **Browse**.
5. Select **Show physical stores** check box, select **Trusted Root Certification Authorities** and then click **OK**.
6. Click **Next** and click **Finish**.
7. Restart the computer.

Microsoft Edge

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 the ESA Web Console

Log in using the access credentials you created for the ESA Web Console during the Authentication Server install. In an Active Directory (AD) environment, if the Active Directory Integration type of deployment has been used, log in by clicking **Use domain authentication** in a supported browser. Domain authentication uses the user's identity who is currently logged on the machine.



Activate your installation of ESET Secure Authentication.

The Web Console provides a quick overview of:

- **Users**: Total number of users, number of users with activated 2FA, number of users with incomplete setup of 2FA, number of users locked out. If the number of **2FA enabled**, **Setup Incomplete**, or **Locked Out** is higher than 0, click the number to list the related users.
- **Servers**: Status (online/offline) and version of the Authentication Server (AS) installed. If there are several sites in your Active Directory domain an AS installed in each site, the **Servers** section will list each AS.
- **Components**: A list and number of ESA components in use, number of outdated ESA components. Click the number in the **Out of date** column to display the related computers/services.
- **License**: User numbers, remaining SMS credits, remaining license days.

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. To protect Windows login with 2FA, refer to the installation of Windows Login. To add 2FA to a single sign-on process, refer to Identity Provider Connector.

> **Feedback**
> 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 or FIDO for the ESA Web Console

To enable or disable 2FA for the ESA Web Console, navigate to **Components** > **ESA Web Console**, and toggle the **Enable 2FA for Web Console** or FIDO.

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

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.

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 (or EMA) username and password are required. Also if you want to use SMS OTPs, you need this type of activation to be able to add SMS Credits.

- **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, and ESA will be used in an offline environment. In this case, the provisioning server is unavailable, and only some authentication methods are available.

3. When 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. Type 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 specific license or a site (license pool) to active ESA.

5. Click **Activate**.

More information on activating ESA via EBA.

i License seat consumption

Every user with an enabled authentication method (even if not functional) consumes a license seat.
If any default authentication type is enabled at **Settings** > **Enrollment** > **Default authentication types**, every new user will consume a license seat.

User Management - Provisioning

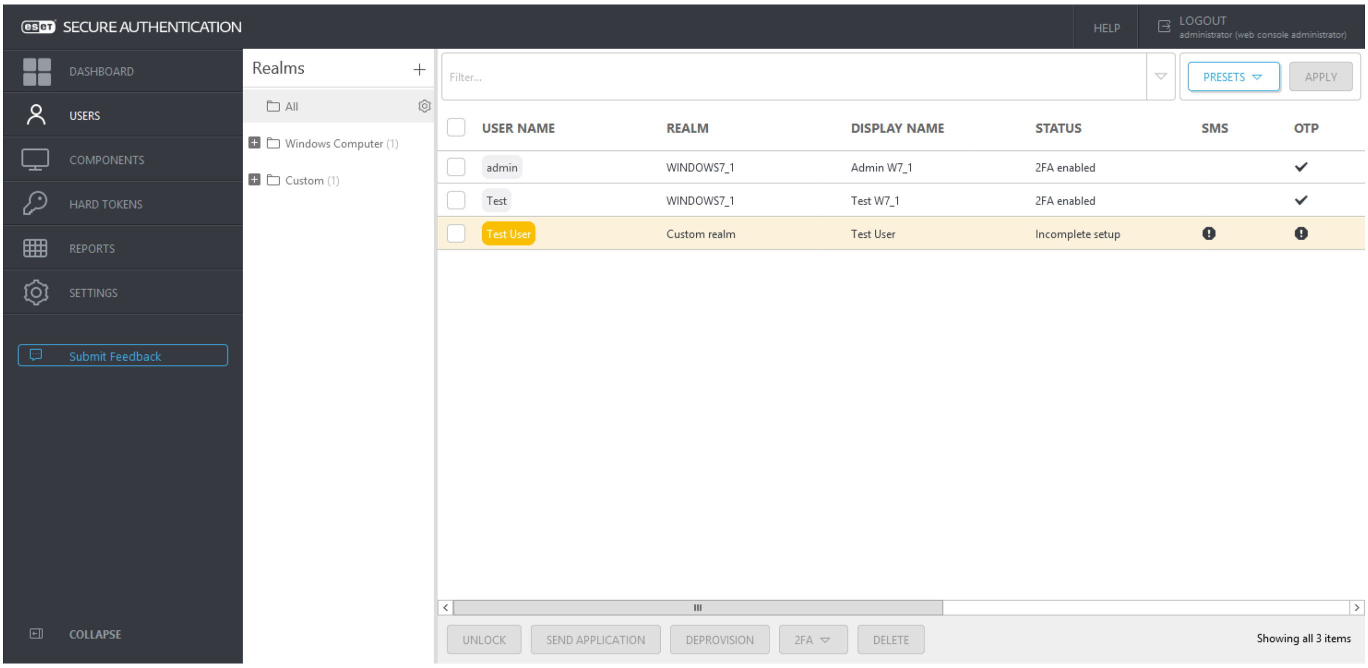
All user management takes place in the **Users** section of the Web Console.

Provisioning is the process of providing users with the ability to authenticate with a second factor when accessing devices/services protected by ESET Secure Authentication.

Since ESA version 3.0, phone number is not essential to use the ESA mobile application unless SMS provisioning is used. The phone number for each user is typed either manually when creating/editing the user in the Web Console, or imported automatically along with the user information if synchronizing with LDAP, or typed 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 two users were created automatically (admin, Test). The realm name was derived from the computer where the Windows Login protection is installed, and the two users logged on. The status column indicates if the user has 2FA enabled (and used 2FA at least once) or 2FA setup is pending. The **Display Name** column shows the value of the **Display Name** field. It can either be defined manually per user or automatically synchronized from Active Directory (or LDAP) based on the configuration at **Settings** > **Default Fields** > select **Default display name field** as the **Field type**.



□	USER NAME	REALM	DISPLAY NAME	STATUS	SMS	OTP
□	admin	WINDOWS7_1	Admin W7_1	2FA enabled		✓
□	Test	WINDOWS7_1	Test W7_1	2FA enabled		✓
□	Test User	Custom realm	Test User	Incomplete setup	!	!

Create a custom realm manually

1. Click the + icon next to **Realms** and click **Create custom Realm**.

2. Type the desired string for both **Realm ID** and **Realm Name**, select **Category**,and click **Save**.

To create a realm corresponding to an Active Directory domain manually, you must find the GUID.

Obtain domain GUID from ADUC

1. Open **Active Directory Users and Computers**.

2. Right-click the domain name, select **Properties**.

3. Click the **Attribute Editor** tab, look up **ObjectGUID**.

4. Use the **ObjectGUID** value in the **Realm ID** field when creating the realm manually.

Obtain domain GUID via PowerShell

1. Open **Windows PowerShell**.

2. Run one of the following commands:

```
Get-ADDomain | select -Property ObjectGUID
```

or

```
wmic ntdomain list full
```

To manually create a realm that corresponds to a local computer (non-domain users), you need the SID.

1. Download PsGetSid.

2. Run PsGetsid.EXE or PsGetsid64.EXE (depending on your Windows bit version) from Windows Command Prompt or Windows PowerShell.

Add user to a realm manually

1. Select the realm where you want to add the user.

2. Click **Add user**.

3. Type the name, phone number, and optionally email address of the user.

4. Click **Create user.**

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

You can also import users to a custom realm from a file.

Send the mobile application to users

The default provisioning method is **ESET servers**, meaning SMS delivery, which requires a valid phone to send the installation link.

1. Select the check box next to users who will receive the mobile application.

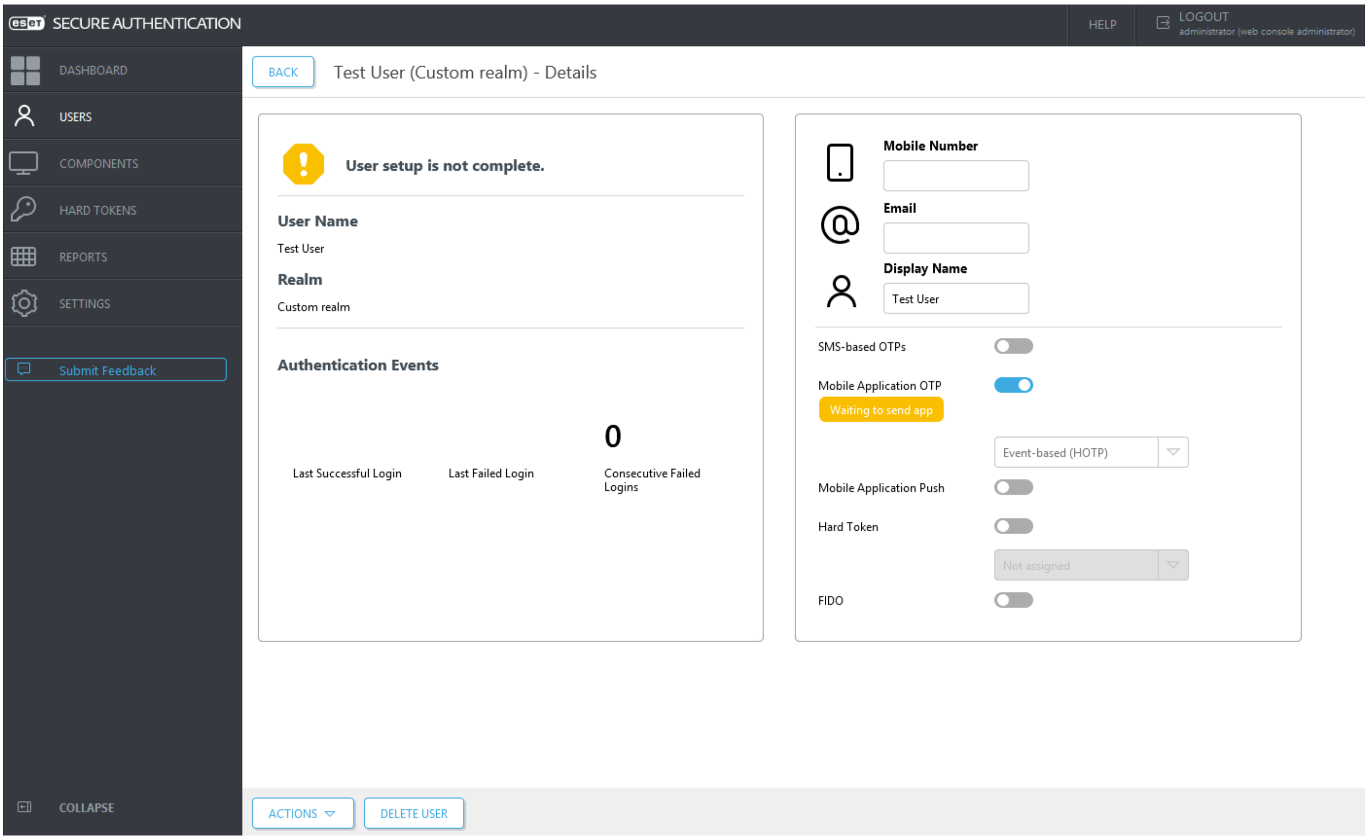
2. Click **Send application**.

3. Close the confirmation window.

> **The validity of the provisioning link**
> The time validity of the provisioning link is 24 hours or until first use.

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** toggle. Click **Save** to save the changes.



Test User (Custom realm) - Details

User setup is not complete.

User Name: Test User

Realm: Custom realm

Authentication Events

Last Successful Login	Last Failed Login	Consecutive Failed Logins
		0

Mobile Number:

Email:

Display Name: Test User

SMS-based OTPs: off

Mobile Application OTP: on — Waiting to send app — Event-based (HOTP)

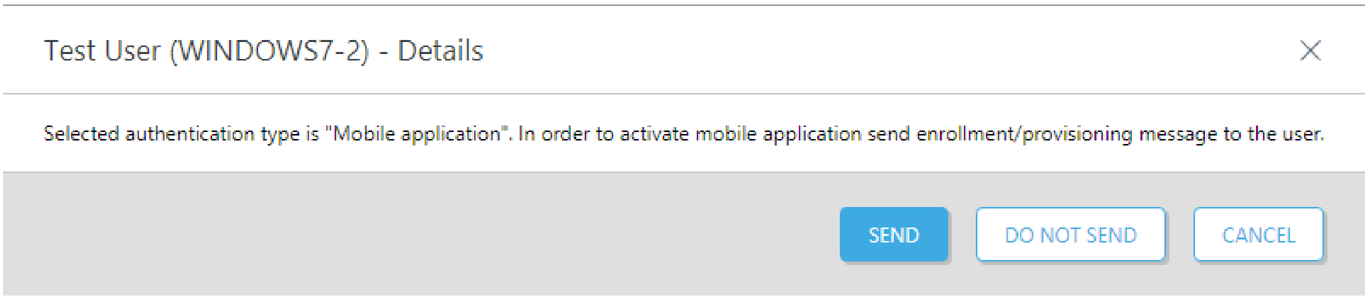
Mobile Application Push: off

Hard Token: off — Not assigned

FIDO: off

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 after 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.



Test User (WINDOWS7-2) - Details

Selected authentication type is "Mobile application". In order to activate mobile application send enrollment/provisioning message to the user.

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 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.

For instructions on installing and using the mobile application, click the desired mobile OS to be redirected to the corresponding article:

- Android
- iPhone

See a list of IP addresses and ports used for communication with ESET Secure Authentication Provisioning Server.

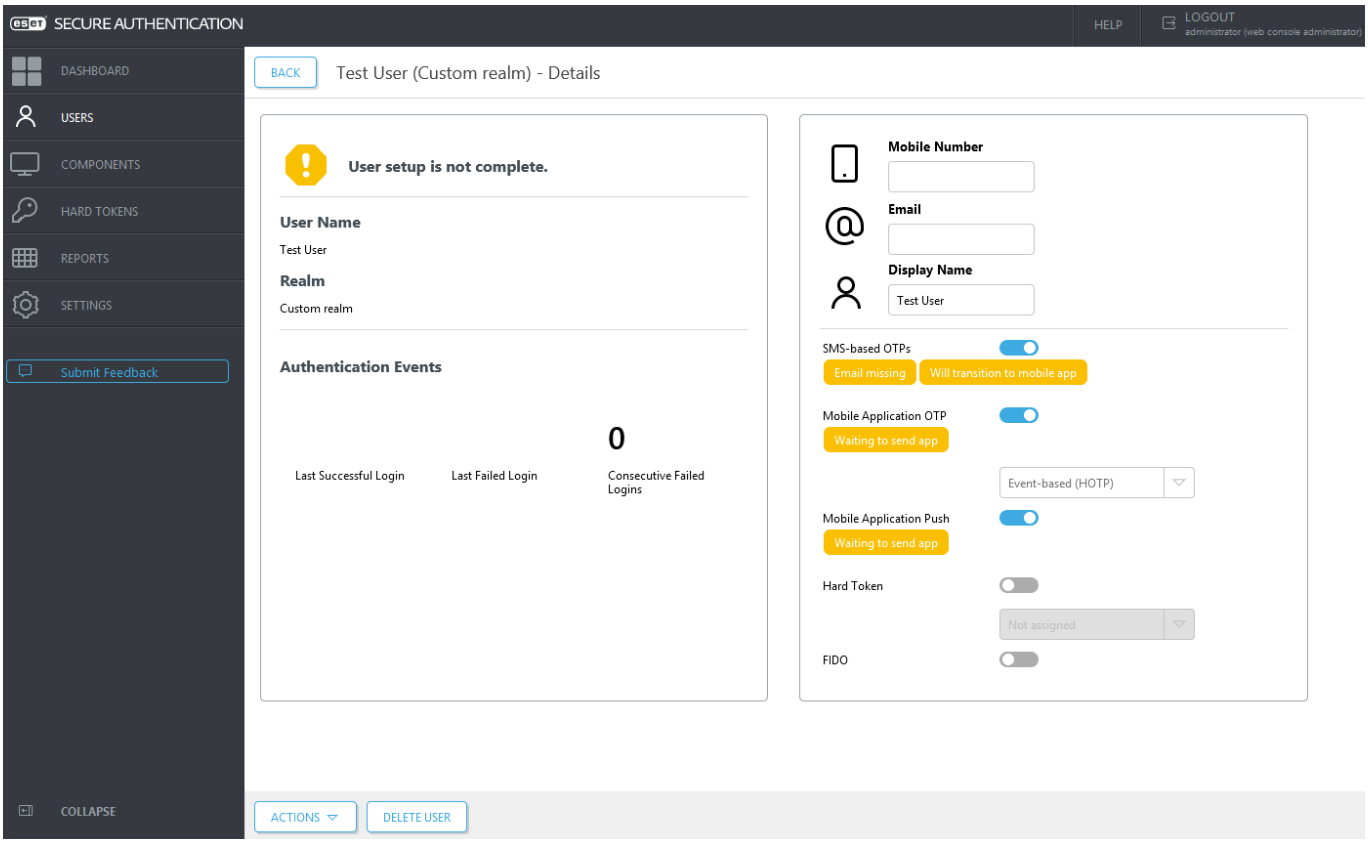
User Status

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 the user has not used any of the enabled methods to authenticate.
- **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.



Test User (Custom realm) - Details

User setup is not complete.

User Name
Test User

Realm
Custom realm

Authentication Events

Last Successful Login

Last Failed Login

0
Consecutive Failed Logins

Mobile Number

Email

Display Name
Test User

SMS-based OTPs ● Email missing Will transition to mobile app

Mobile Application OTP ● Waiting to send app

Event-based (HOTP)

Mobile Application Push ● Waiting to send app

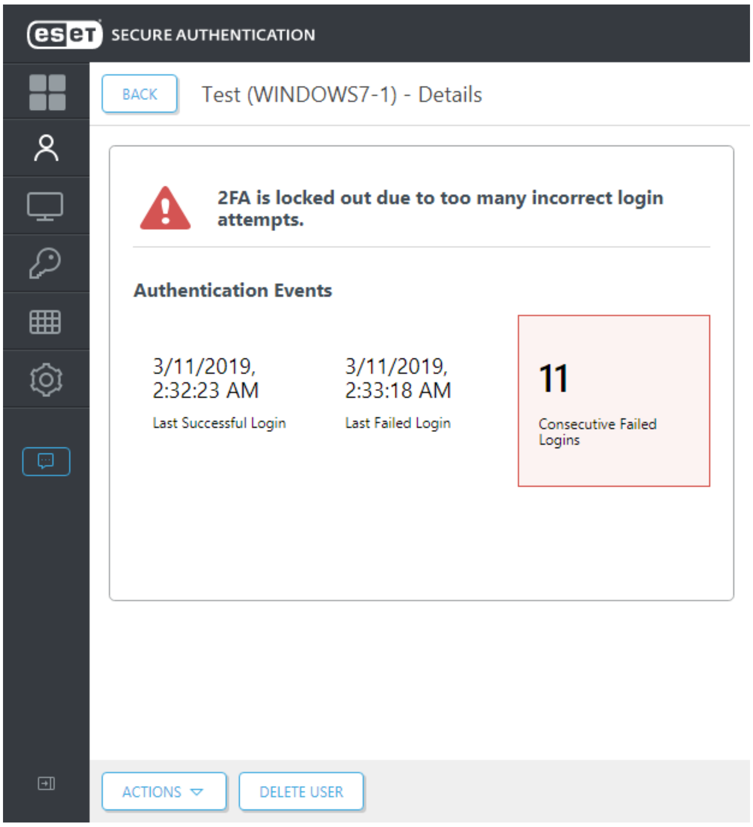
Hard Token ○

Not assigned

FIDO ○

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 type 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:



Test (WINDOWS7-1) - Details

2FA is locked out due to too many incorrect login attempts.

Authentication Events

3/11/2019, 2:32:23 AM	3/11/2019, 2:33:18 AM	11
Last Successful Login	Last Failed Login	Consecutive Failed Logins

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.

Synchronizing with LDAP

ESET Secure Authentication supports synchronization with LDAP.

> An administrator can synchronize either the entire AD domain or select only a specific OU subtree of the AD domain.
> In the case of a Windows domain, only one OU subtree can be synchronized per AD domain (directory service) because the entire AD GUID becomes the created realm's ID. If the administrator tries to synchronize another OU subtree of that AD (Windows domain), the "Realm '<ID>' already exists" error message will display.
> Sample **LDAP Server Path** to synchronize an OU subtree of "`esa.local`" AD domain (Windows domain):
> `LDAP://<serverName>/OU=sub_OU,OU=first_OU,DC=esa,DC=local`
>
> When synchronizing a different directory type, the entire **Server LDAP Path** becomes the created realm's ID.

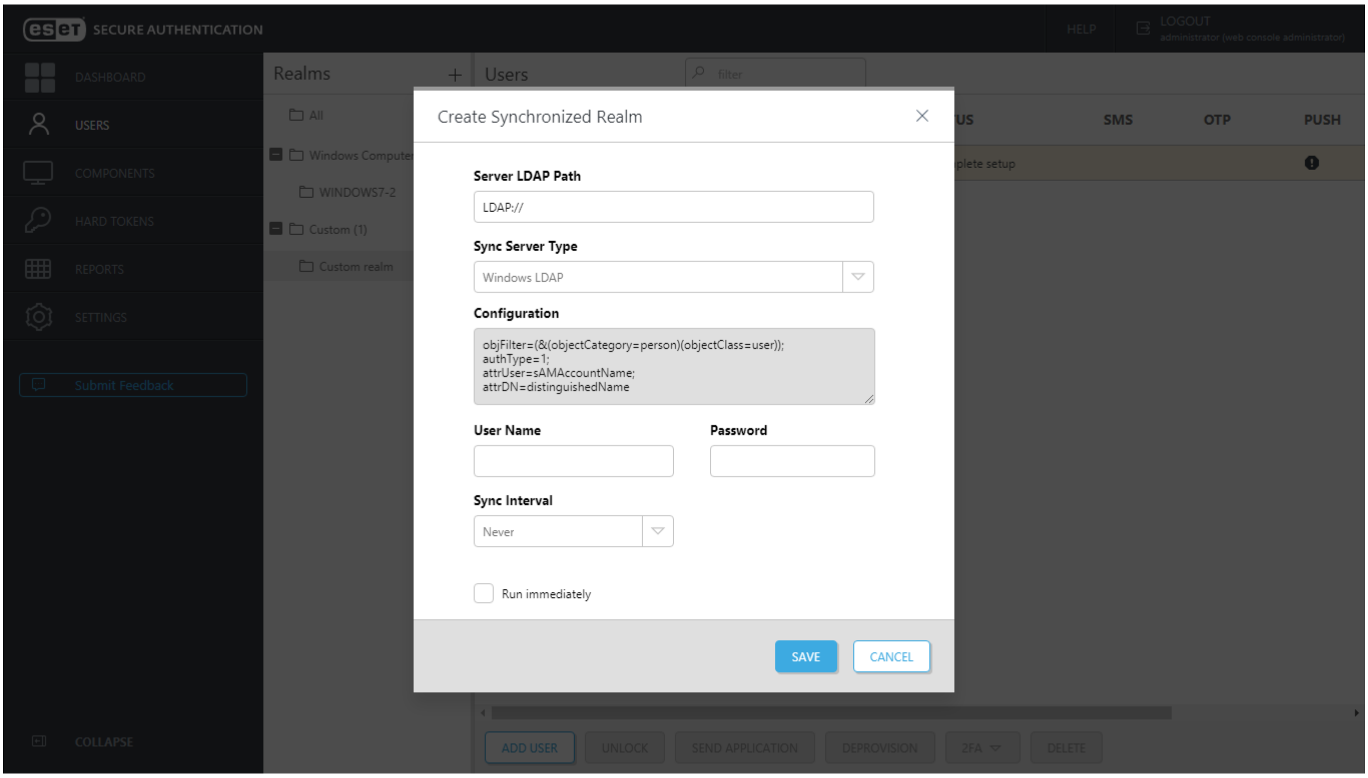
1. Access ESA Web Console and click **Users**.

2. Next to **Realms**, click +, select **Create Synchronized Realm**.

3. Type the address of your LDAP server, select the applicable LDAP server type from the **Sync Server type** drop-down menu, and type your LDAP username and password.

4. If this is 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**.



Create Synchronized Realm

Server LDAP Path: LDAP://

Sync Server Type: Windows LDAP

Configuration:

```
objFilter=(&(objectCategory=person)(objectClass=user));
authType=1;
attrUser=sAMAccountName;
attrDN=distinguishedName
```

User Name:

Password:

Sync Interval: Never

□ Run immediately

SAVE CANCEL

When 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 username. 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:

  o0 (None)

  o1 (Secure)

  o2 (Encryption/SecureSocketsLayer)

  o4 (ReadonlyServer)

  o16 (Anonymous)

  o32 (FastBind)

  o64 (Signing)

  o128 (Sealing)

  o256 (Delegation)

  o512 (ServerBind)

For more information on each authentication type see the official Microsoft documentation.

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:

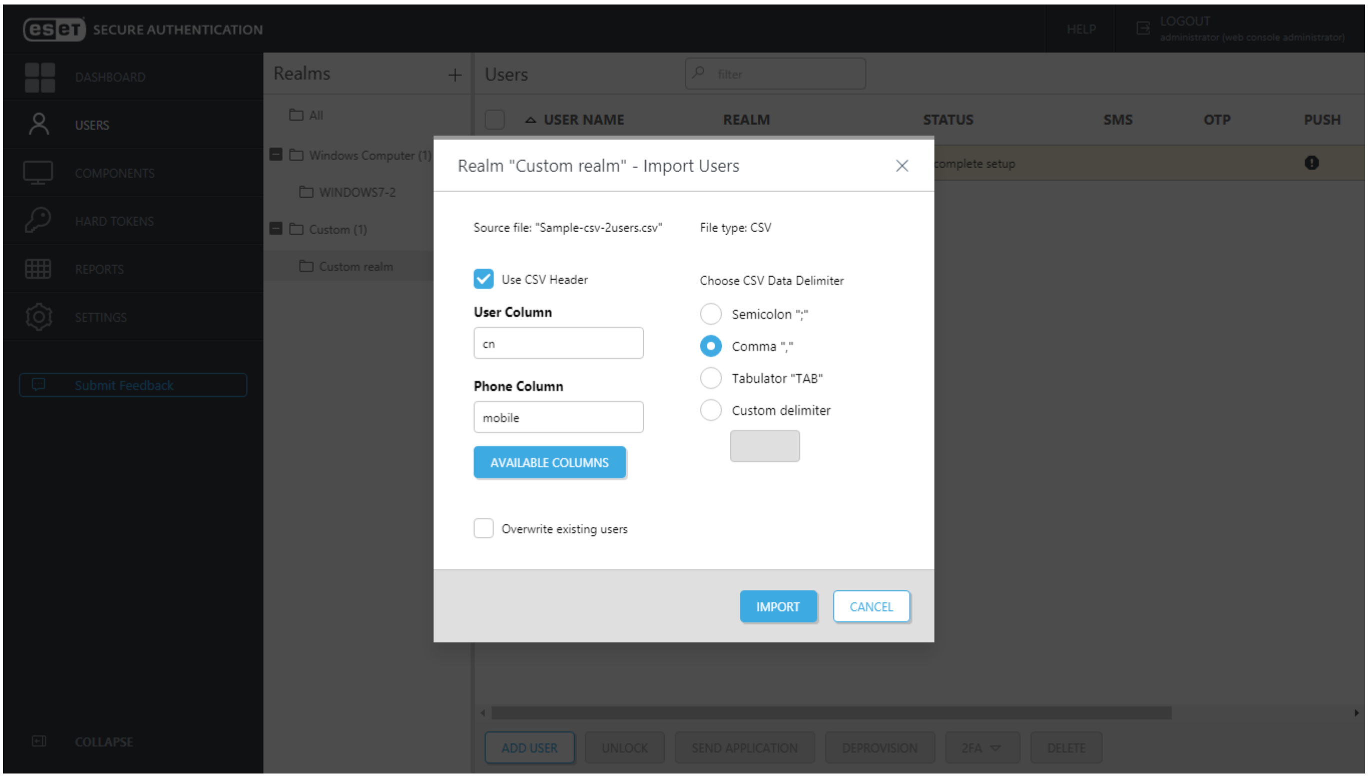
1. Select a custom realm.

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**.



Realm "Custom realm" - Import Users

Source file: "Sample-csv-2users.csv"

File type: CSV

☑ Use CSV Header

User Column: cn

Phone Column: mobile

AVAILABLE COLUMNS

□ Overwrite existing users

Choose CSV Data Delimiter

○ Semicolon ";"
● Comma ","
○ Tabulator "TAB"
○ Custom delimiter

IMPORT CANCEL

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,mobile,telephoneNumber,displayName,co"
```

- Export to LDF file:

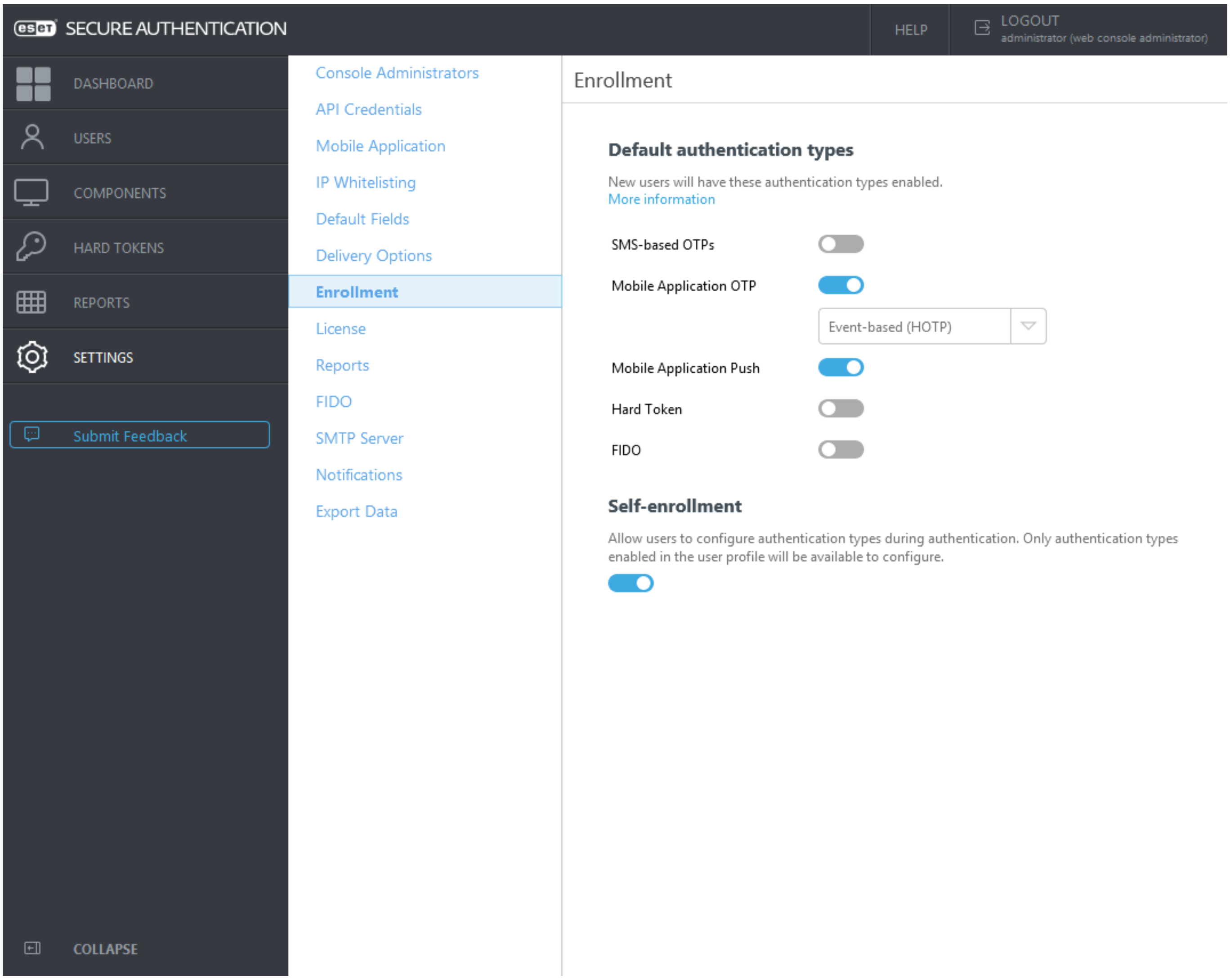
```
ldifde -f export.ldf -s mydomain.com -r "(objectclass=user)" -l "cn, memberOf, distinguishedName, mobile, pager, facsimileTelephoneNumber"
```

Self-enrollment

License seat consumption

Every user with an enabled authentication method (even if not functional) consumes a license seat.
If any default authentication type is enabled at **Settings** > **Enrollment** > **Default authentication types**, every new user will consume a license seat.

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 must contact the administrator to generate a Master Recovery Key (MRK) to authenticate.



Enrollment

Default authentication types

New users will have these authentication types enabled.
More information

SMS-based OTPs: off

Mobile Application OTP: on — Event-based (HOTP)

Mobile Application Push: on

Hard Token: off

FIDO: off

Self-enrollment

Allow users to configure authentication types during authentication. Only authentication types enabled in the user profile will be available to configure.

Self-enrollment: on

Enable self-enrollment

1. In the ESA Web Console, navigate to **Settings** > **Enrollment**.

2. Click the desired toggles under **Default authentication types** to automatically enable authentication options for new users.

3. Click the toggle in the **Self enrollment** section.

4. Click **Save**.

If self-enrollment is enabled, the user can authenticate using MRK. To enroll, click **Set up** and fill in missing information.

Default authentication types

To assign new users (either imported or created automatically after the 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**.

Supported ESA components

Self-enrollment works with the following ESA components:

- Windows Login plugin
- Remote Desktop plugin
- Web App plugin
- Identity Provider Connector
- AD FS
- ESA Web Console

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 type an OTP related to the Hard Token, click **Add another authentication method**.

3. Type an OTP related to the Hard Token.

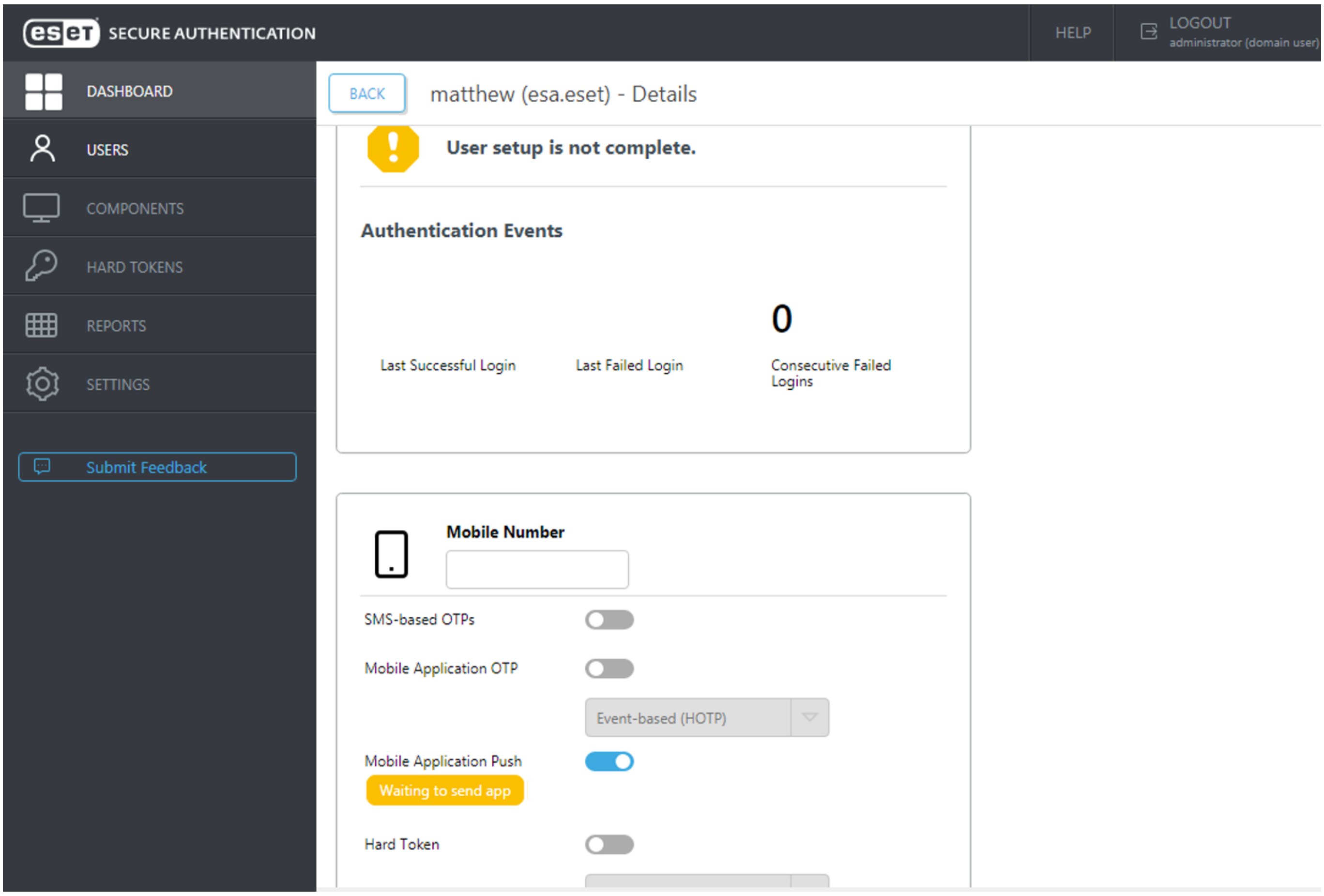
4. Click **Setup**.

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 requires the user to verify the successful registration of the new authentication method by approving the push notifications.

Self-enrollment example

1. A user has the **Mobile Application Push** authentication turned on as the default authentication type or the administrator has turned it on in the ESA Web Console.



matthew (esa.eset) - Details

User setup is not complete.

Authentication Events

Last Successful Login	Last Failed Login	Consecutive Failed Logins
		0

Mobile Number

SMS-based OTPs

Mobile Application OTP

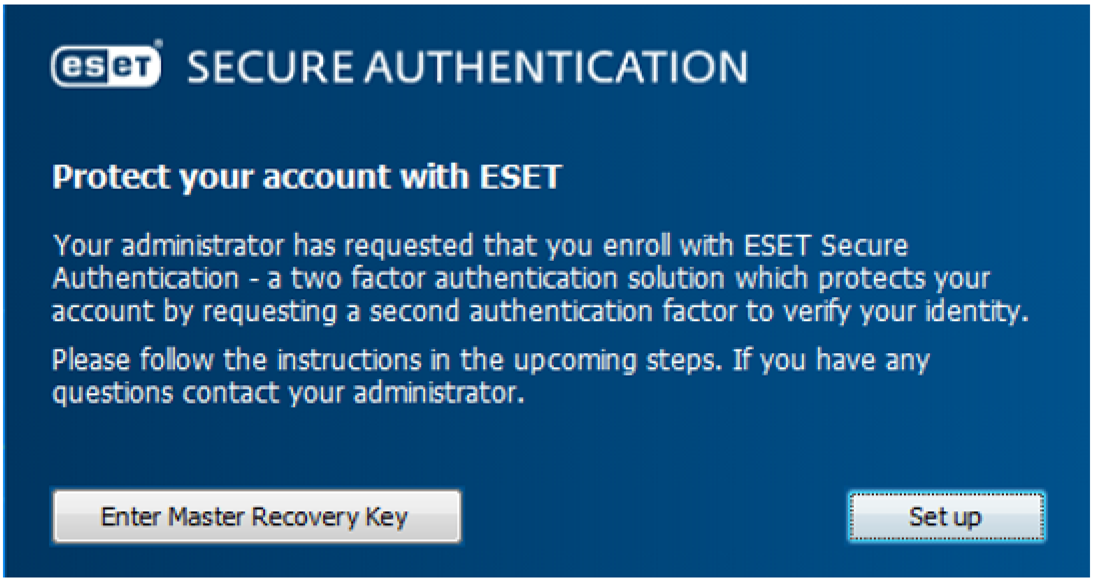
Event-based (HOTP)

Mobile Application Push

Waiting to send app

Hard Token

2. On the next log in to a computer protected by ESA Windows login protection, the user is requested to enroll with ESET Secure Authentication. Click **Setup**.



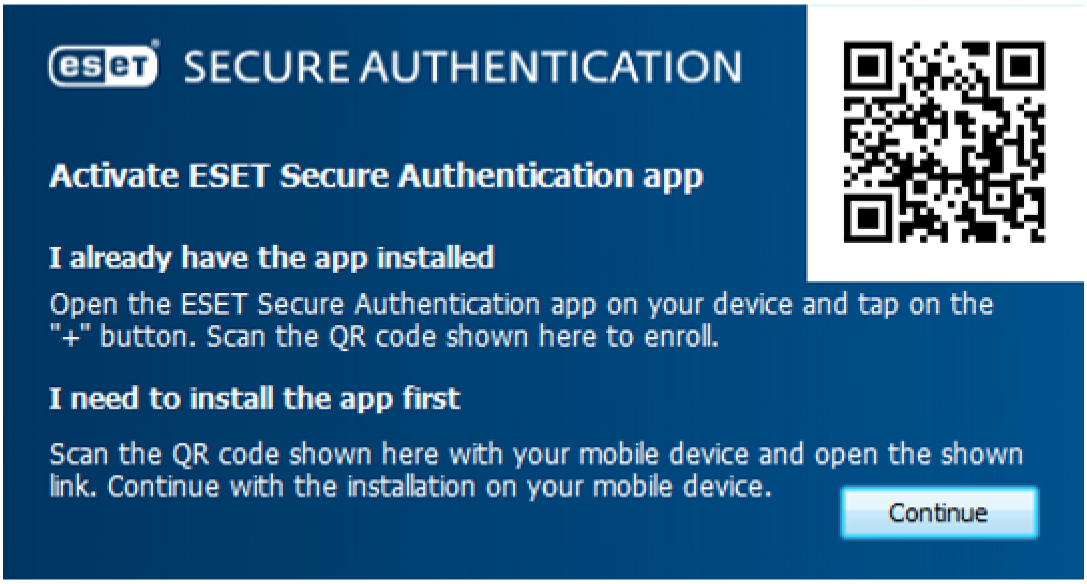
Protect your account with ESET

Your administrator has requested that you enroll with ESET Secure Authentication - a two factor authentication solution which protects your account by requesting a second authentication factor to verify your identity.

Please follow the instructions in the upcoming steps. If you have any questions contact your administrator.

3. If you have the ESA mobile app installed, open it, tap **+** and scan the QR code displayed in the dialog. Click

Continue. If you do not have the mobile app installed, scan the QR code to download and install the mobile app. Click **Continue**.



Activate ESET Secure Authentication app

I already have the app installed

Open the ESET Secure Authentication app on your device and tap on the "+" button. Scan the QR code shown here to enroll.

I need to install the app first

Scan the QR code shown here with your mobile device and open the shown link. Continue with the installation on your mobile device.

4. Confirm the push notification sent to your phone. The **Verify enrollment** window displays a number and the push notification appears on your phone (could take up to two minutes). Approve the push notification if the number on it matches the number shown in the **Verify enrollment** screen.

5. In the **Enrollment successful** screen, click **Finish**.

Groups Based User Management

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

There are several Active Directory groups are created at installation time:

- ESA Users

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

- ESA SMS Users

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

- ESA Mobile App Users

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

- ESA Hard Token Users

The ESA Hard Token Users group contains all users that have been enabled for Hard Token OTPs.

- ESA FIDO Users

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

- EsaCoreAuthServices, EsaServices and ESA Admins store no real users. They are related to internal security of ESET Secure Authentication.

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

1. Launch the ADUC

2. Right-click your domain node, and select **Find**

3. Type in "ESA SMS" and hit **Enter** - the group will be displayed in the **Search Result** section

4. Double click the group and select the **Members** tab to view all users in your domain that have been enabled for SMS OTPs.

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. Invitations can be used also in non-domain environment, but make sure ESA components and the Authentication Server will be able to see (ping) each other.

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.

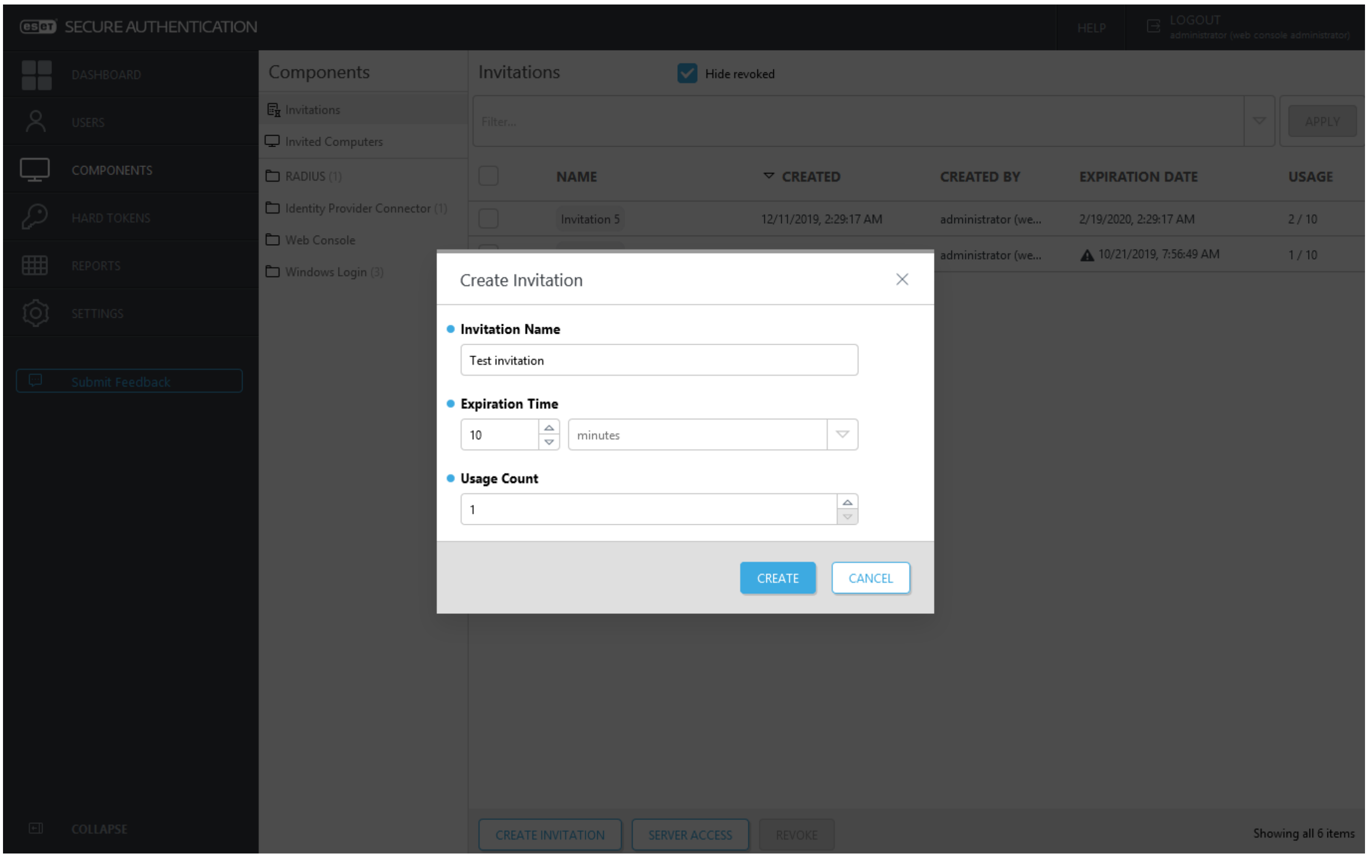
If you use ESET Secure Authentication in a domain established by Active Directory Domain Services, and you want to deploy 2FA on computers outside that domain, invitations make it possible.

Generate an invitation

1. In the ESA Web Console, click **Components** > **Invitations**.

2. Click **Create invitation**.

3. Type an invitation name, expiration time and usage count. Click **Create**.



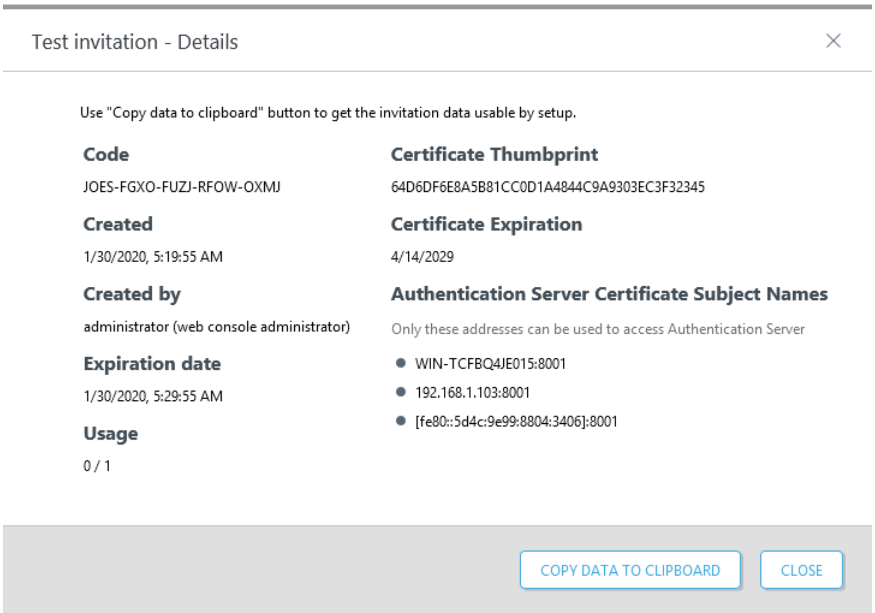
Create Invitation

Invitation Name: Test invitation

Expiration Time: 10 minutes

Usage Count: 1

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



Test invitation - Details

Use "Copy data to clipboard" button to get the invitation data usable by setup.

Code
JOES-FGXO-FUZJ-RFOW-OXMJ

Created
1/30/2020, 5:19:55 AM

Created by
administrator (web console administrator)

Expiration date
1/30/2020, 5:29:55 AM

Usage
0 / 1

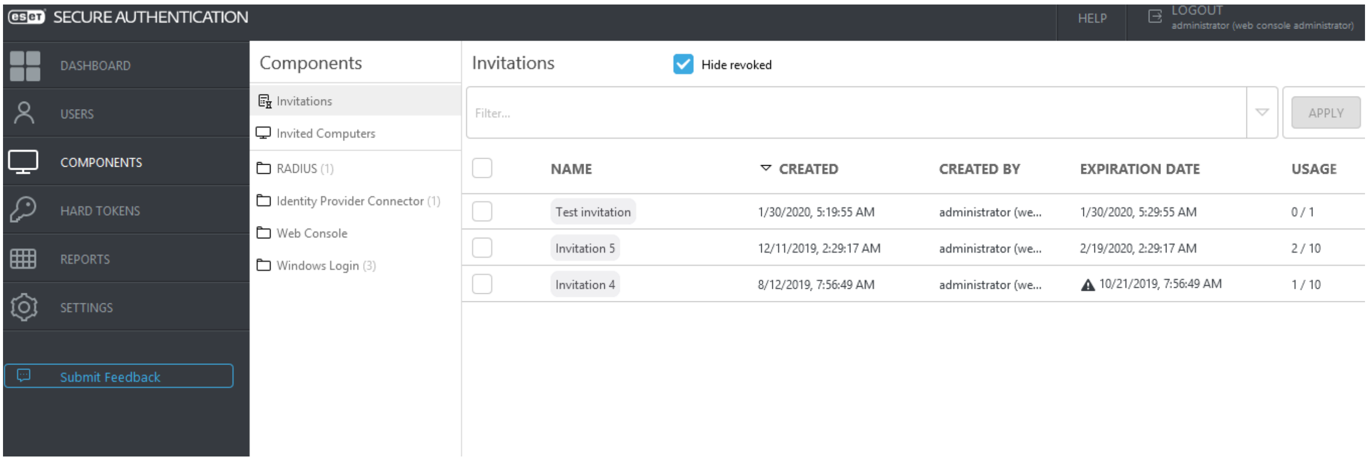
Certificate Thumbprint
64D6DF6E8A5B81CC0D1A4844C9A9303EC3F32345

Certificate Expiration
4/14/2029

Authentication Server Certificate Subject Names
Only these addresses can be used to access Authentication Server

- WIN-TCFBQ4JE015:8001
- 192.168.1.103:8001
- [fe80::5d4c:9e99:8804:3406]:8001

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



☑ Hide revoked

□	NAME	CREATED	CREATED BY	EXPIRATION DATE	USAGE
□	Test invitation	1/30/2020, 5:19:55 AM	administrator (we...	1/30/2020, 5:29:55 AM	0 / 1
□	Invitation 5	12/11/2019, 2:29:17 AM	administrator (we...	2/19/2020, 2:29:17 AM	2 / 10
□	Invitation 4	8/12/2019, 7:56:49 AM	administrator (we...	⚠ 10/21/2019, 7:56:49 AM	1 / 10

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

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 with a user who belongs to the same Active Directory domain, and also belongs to the "ESA Admins" group.

If you have a different NetBIOS name for the domain, using domain authentication might not work.

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

Add HTTP entries to servicePrincipalName of ESASrv_<computer name> account

> **Important**
> Applying this solution can create a `servicePrincipalName` conflict with another service, for example it can break the functionality of another web service hosted on the same computer. For example, Outlook Web Access. If this solution does not suit you, proceed to Workaround 1 or Workaround 2 below.

1. Open ADUC.
2. Click **View**, select **Advanced Features**.
3. Expand `<domain>`, click ESET Secure Authentication.
4. Right-click `ESASrv_<computer name>`, select Properties.
5. Switch to the **Attribute Editor** tab, double-click **servicePrincipalName**.
6. Type `HTTP/<hostname>`, click **Add**.
7. Type `HTTP/<hostname>.<domain>`, click **Add**.

8. Click **OK** to close both the editor and the **Properties** window.

Workaround 1

Open ESA Web Console on the computer where the Authentication Server is installed.

Workaround 2

When logging on remotely, use the IP address of the Authentication Server, not FQDN or hostname.

Adjust browser configuration

- 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. Type the domain name of ESA Web Console without protocol (`https://`), without port number and trailing slash.
  6. Press **Enter** key.

Notifications

This feature is intended for the administrator of ESET Secure Authentication (ESA).

What types of notifications are included?

- Server startup: Each time the Authentication Server is started (re-started).

- Error: If any error occurs that might affect the authentication process.
- Web Console Login: Each time a console administrator logs in to ESA Web Console
- User Locked: Each time a user has been locked due to failed authentication (did not provide correct second authentication factor)
- User Unlocked
- License: If the license state changes from OK to anything else

How does it work?

ESA uses an SMTP server defined by you to deliver email notifications regarding the selected types of actions.

1. Define the details of a working SMTP server:

   a.In the ESA Web Console navigate to **Settings** > **SMTP Server** and fill in the required details.

   b.Use the **Send test email** to test the configuration. If an email is delivered to the provided email address, the configuration is correct.

2. Enable the Notifications feature and select the type and frequency of notifications:

   a.In the ESA Web Console navigate to **Settings** > **Notifications**.

   b.Select **Enable notifications**.

   c.For **Recipient Email Address**, type the email address where the notifications will be delivered.

   d.Select the desired **Notification Types**.

   e.In the **Throttling** section, select the frequency of delivering notifications:

   - **Immediately:** As soon as a selected type of action occurs, a notification email is sent.
   - **10 minutes:** If in the past 10 minutes any of the selected type of actions occurred, an email summary will be sent.
   - **1 hour:** If in the past hour any of the selected type of actions occurred, an email summary will be sent.
   - **1 day:** Daily summary delivered via email about occurrence of selected types of actions.

   f.Click **Save**.

> **Multiple Authentication Servers**
>
> If you have multiple Authentication Servers, notifications are sent by each of them regardless of the selected **Throttling**.

Authentication options

ESET Secure Authentication (ESA) 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
- OTP delivered via email
- Push Authentication
- Hard tokens
- OTP received via custom delivery option
- FIDO—only one FIDO authenticator can be registered per user

> **Security of authentication options**
> ESA offers a wide range of 2FA methods that fit the varying preferences of our customers.
> The most secure and highly usable is Mobile Application Push (Push authentication).
> Still highly reliable, but in some situations, less convenient are: Mobile Application OTP, Hard Token, and FIDO.
> SMS-based OTPs, thus still available, are not considered the most secure mainly due to the underlying security used in the SMS delivery systems.
> When choosing the delivery of OTP by email, there might be usage schemas having weaker security.

> **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.

Authentication options available offline

> **Before offline use**
> 1. ESA must be activated using a license key or ESET Business Account credentials.
> 2. To enroll and provision users, ESA core must be able to access `esa.eset.com`.

When the Authentication Server cannot connect to the internet, the following options are available to authenticate a login attempt:

- Hard tokens
- FIDO

- SMS OTP utilizing custom delivery within your internal network not connecting to the internet

- OTP generated via ESA mobile application (activate (provision) the mobile app online)

Windows Login protection in offline mode

When using the Windows Login protection in offline mode, the following options are available to authenticate a login attempt:

- Hard tokens (event-based OTP only)

- OTP generated via ESA mobile application (event-based OTP only)

- FIDO

> **Offline OTPs**
>
> In offline mode, only 20 OTPs are cached by default. Cache renewal occurs in the following ways:
>
> - Automatically after successful login in online mode
> - 10 minutes after successful offline login, the ESA component attempts to download new OTPs. The next attempts are every 60 minutes
> - If a new network is connected (for example, the network adapter is restarted), the ESA component attempts to download new OTPs immediately

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.

The mobile application version 3.0+ supports Google Authenticator tokens. Instead of installing the Google Authenticator app, click the **+** button in the mobile application of ESET Secure Authentication to scan the QR code when setting up 2-step Verification with Google Authenticator. Then you will be able to generate OTPs with ESA Mobile App instead of Google Authenticator App when signing in to a Google service protected by 2-step verification.

For instructions on installing and using the mobile application, click the desired mobile OS to be redirected to the corresponding article:

- Android

- iPhone

See a list of IP addresses and ports used for communication with ESET Secure Authentication Provisioning Server.

You can protect the mobile app from unauthorized access by setting a PIN code. To access the mobile app faster, allow the use of Fingerprint scanner (Android, iOS) or Face recognition (iOS) if biometric authentication is configured on your mobile device.

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

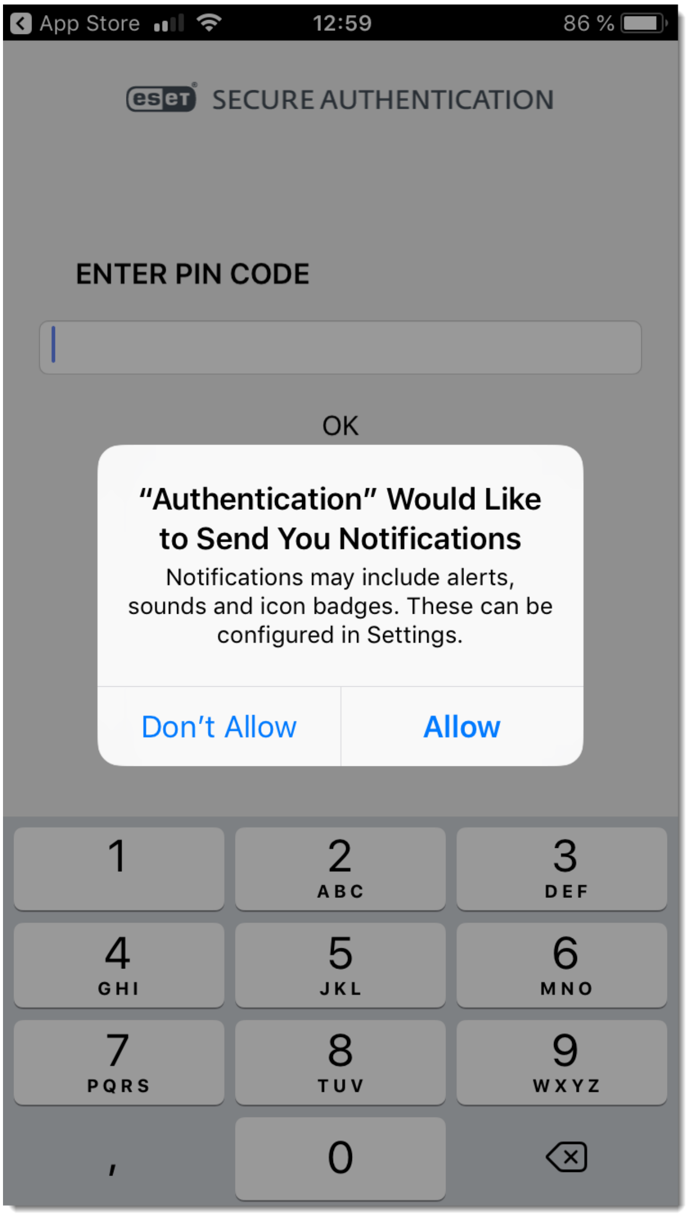
OTPs are displayed in the mobile application with a space between the 3rd and 4th digits to improve readability. All authentication methods except MS-CHAPv2 strip whitespace from the provided credentials, so a user may include or exclude whitespace without affecting authentication.

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 extended 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.



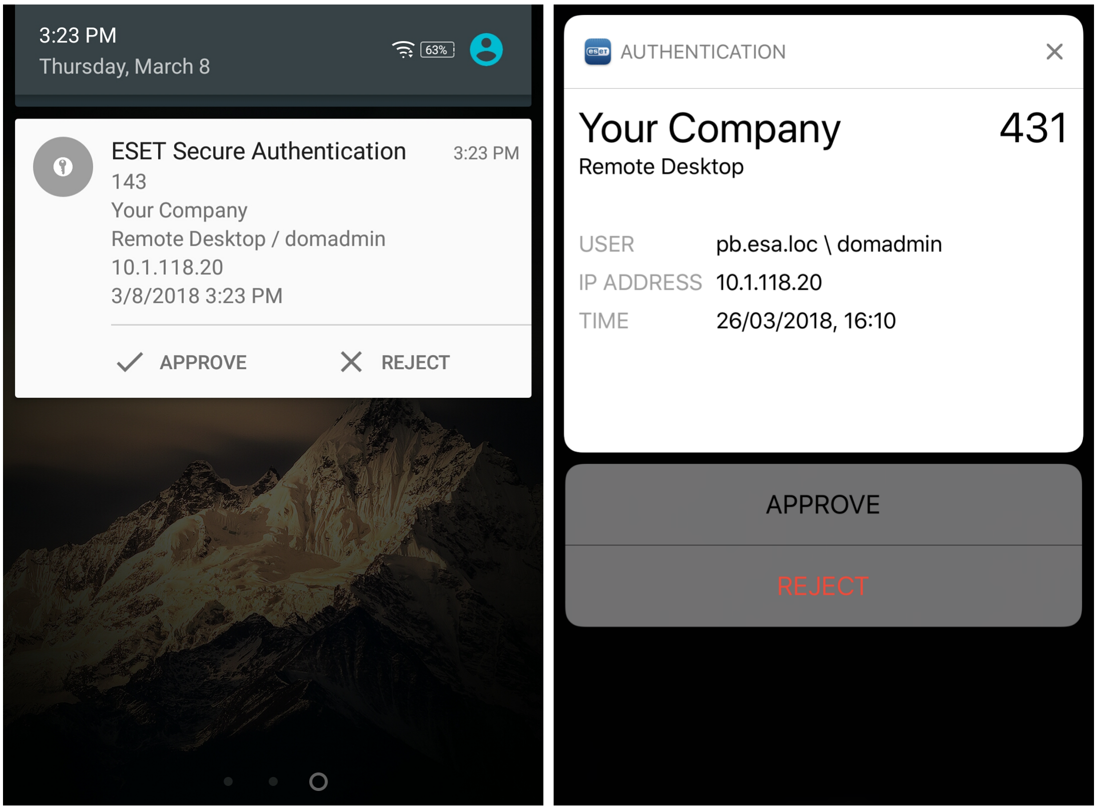
“Authentication” Would Like to Send You Notifications

Notifications may include alerts, sounds and icon badges. These can be configured in Settings.

Note

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.



3:23 PM
Thursday, March 8

ESET Secure Authentication 3:23 PM
143
Your Company
Remote Desktop / domadmin
10.1.118.20
3/8/2018 3:23 PM

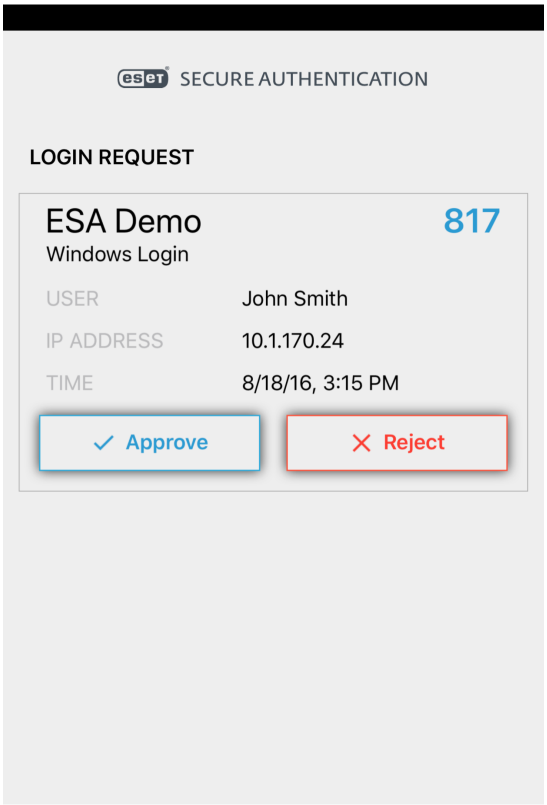
AUTHENTICATION

Your Company 431
Remote Desktop

USER pb.esa.loc \ domadmin
IP ADDRESS 10.1.118.20
TIME 26/03/2018, 16:10

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.



SECURE AUTHENTICATION

LOGIN REQUEST

ESA Demo 817
Windows Login

USER John Smith
IP ADDRESS 10.1.170.24
TIME 8/18/16, 3:15 PM

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.

What if I reject the push notification?

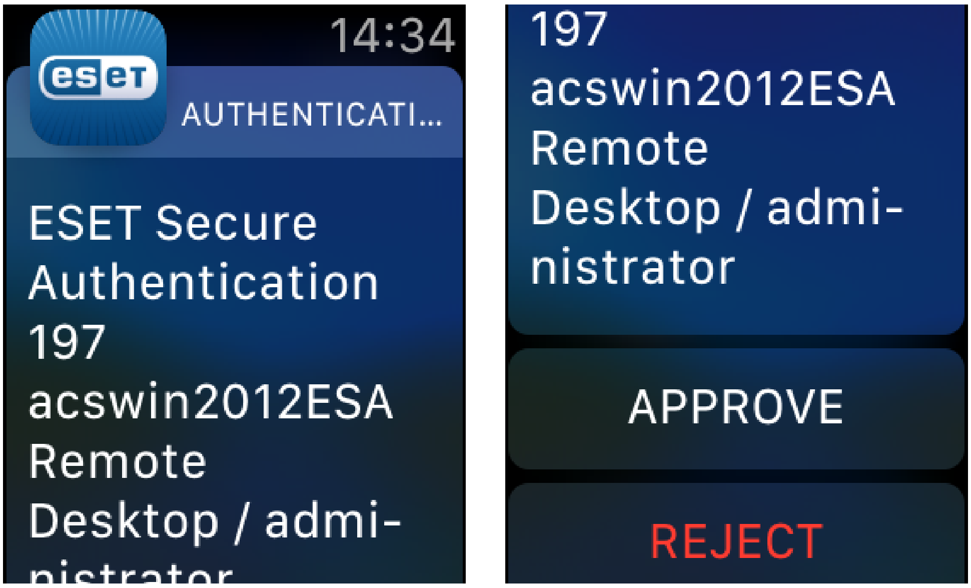
Rejection of push notification does not send any feedback to the Authentication Server (AS), but closes the notification bubble/window. If the AS does not receive approval in 150 seconds, the user is not granted access to the service/computer protected by 2FA.

Android smart watch

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

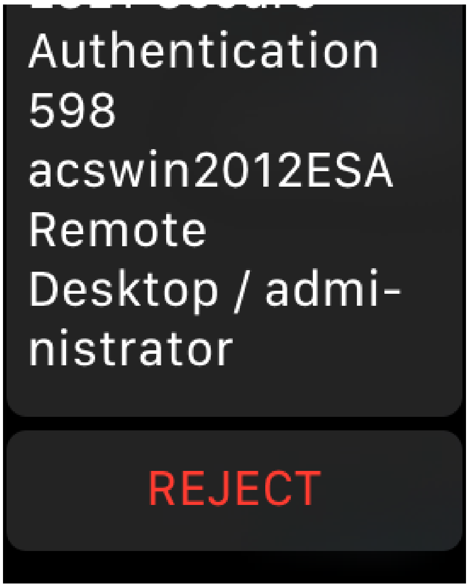


ESET Secure Authentication
197
acswin2012ESA
Remote
Desktop / administrator

197
acswin2012ESA
Remote
Desktop / administrator

Notification arrived; Scroll down to action buttons

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


Authentication
598
acswin2012ESA
Remote
Desktop / administrator

Hard Tokens

A hard token (also known as hardware 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.

- HOTP stands for "HMAC-based One-time Password", which is an event-based OTP
- TOTP stands for "Time-based One-time Password"

Both HOTP and TOTP can be generated by a hardware (hard tokens) or software (for example, ESA Mobile App).

ESA supports all OATH compliant hard tokens, but ESET does not supply them. The hard token HOTPs can be used in the same way as the HOTPs 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.

The token data can be imported into ESET Secure Authentication using an XML file in the PSKC format. Most hard token vendors supply you with a PSKC file when you purchase your hard tokens.

We recommend verifying with the vendor the hard token you are about to use is OATH-compliant.

To use and manage hard tokens, see instructions below.

Enable and Import Hard Tokens

1. In the ESA Web Console, click **Hard Tokens**.

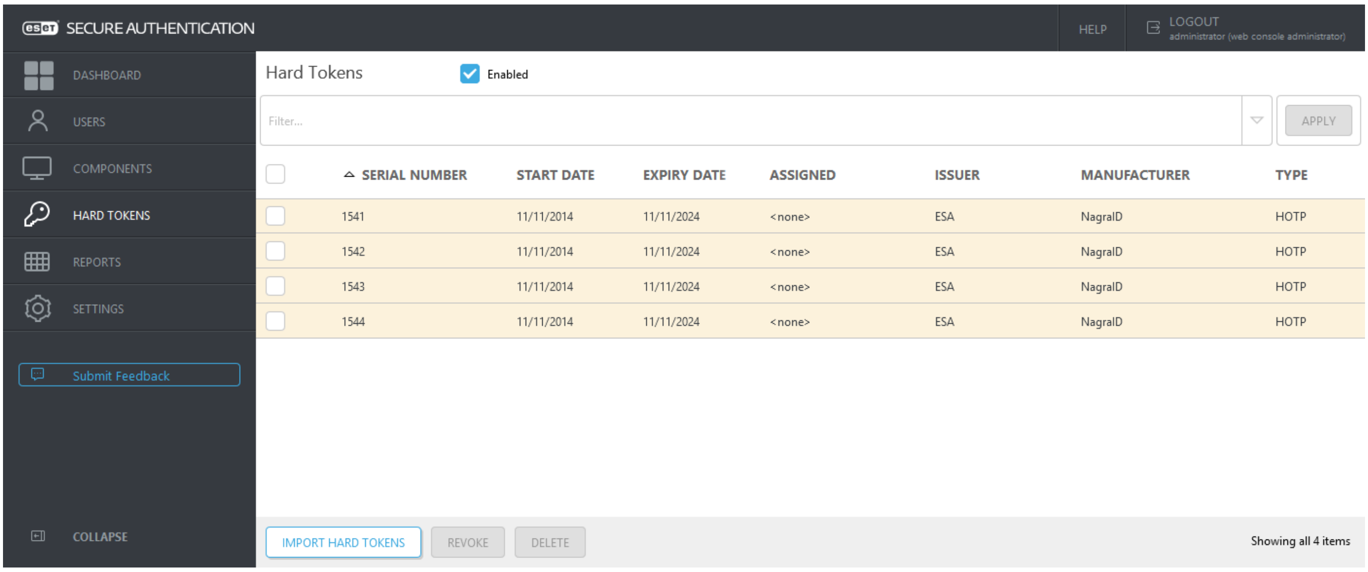
2. Select the **Enabled** check box if it has not been selected by default.

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.



□	SERIAL NUMBER	START DATE	EXPIRY DATE	ASSIGNED	ISSUER	MANUFACTURER	TYPE
□	1541	11/11/2014	11/11/2024	<none>	ESA	NagraID	HOTP
□	1542	11/11/2014	11/11/2024	<none>	ESA	NagraID	HOTP
□	1543	11/11/2014	11/11/2024	<none>	ESA	NagraID	HOTP
□	1544	11/11/2014	11/11/2024	<none>	ESA	NagraID	HOTP

Showing all 4 items

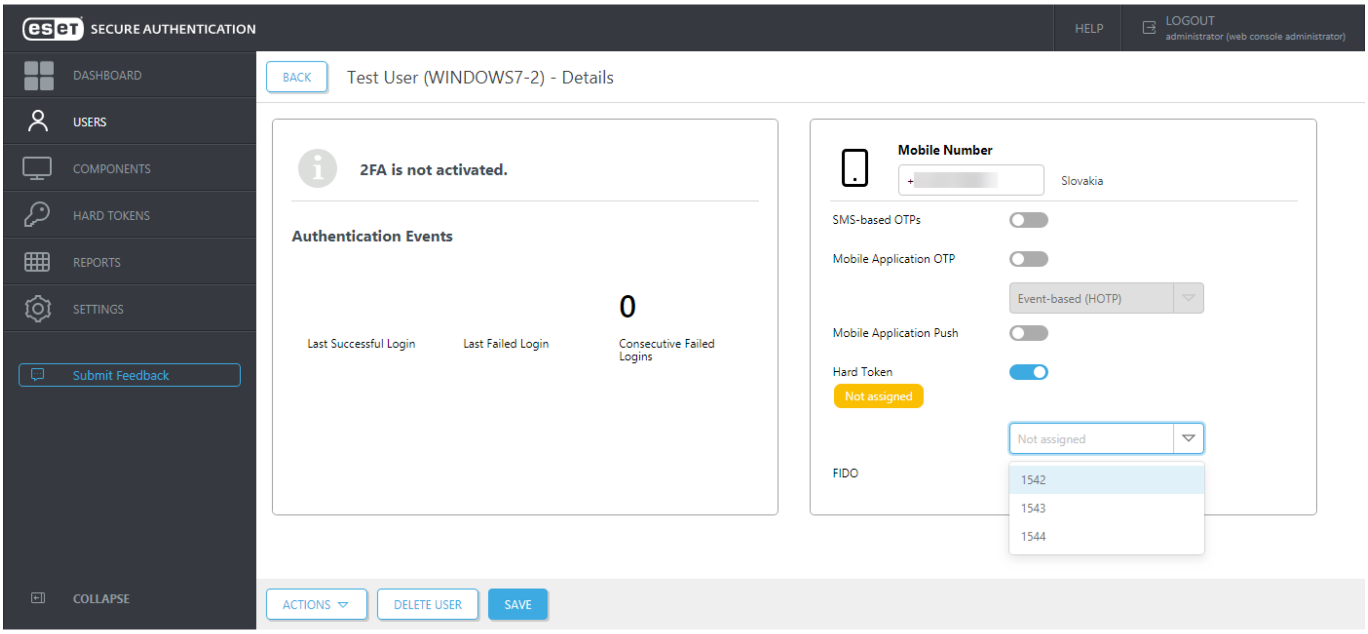
Assign Hard Token to a user

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**.



Test User (WINDOWS7-2) - Details

2FA is not activated.

Authentication Events

Last Successful Login

Last Failed Login

0 Consecutive Failed Logins

Mobile Number: +[redacted] Slovakia

SMS-based OTPs: off

Mobile Application OTP: off, Event-based (HOTP)

Mobile Application Push: off

Hard Token: on, Not assigned

Not assigned: 1542, 1543, 1544

FIDO

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

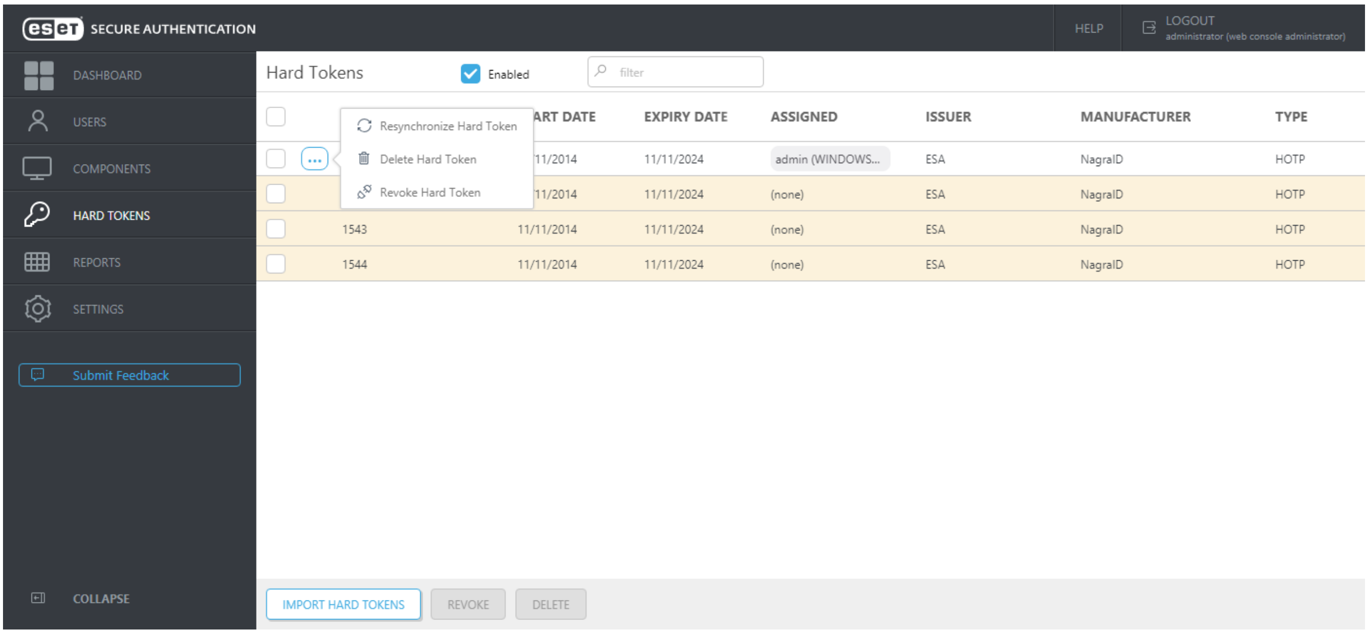
There is a possibility that a hard token becomes out of sync with the system. This can happen if:

- a user generates many new OTPs for an event-based hard token without using them
- the internal time of a time-based hard token is out of sync

In these scenarios, a resynchronization will be required.

A token can be resynchronized as follows:

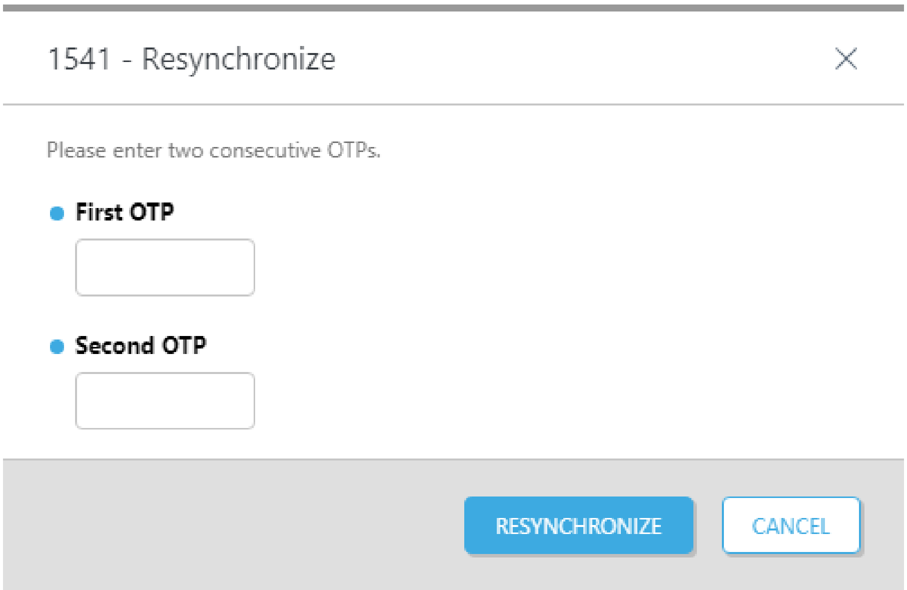
1. In the ESA Web Console, click **Hard Tokens**.
2. In the appropriate row, click ⋯, and select **Resynchronize Hard Token**.



Hard Tokens

		ART DATE	EXPIRY DATE	ASSIGNED	ISSUER	MANUFACTURER	TYPE
□	...	11/2014	11/11/2024	admin (WINDOWS...	ESA	NagraID	HOTP
□		11/2014	11/11/2024	(none)	ESA	NagraID	HOTP
□	1543	11/11/2014	11/11/2024	(none)	ESA	NagraID	HOTP
□	1544	11/11/2014	11/11/2024	(none)	ESA	NagraID	HOTP

3. Generate and type two consecutive OTPs using the selected hard token.



1541 - Resynchronize

Please enter two consecutive OTPs.

First OTP

Second OTP

4. Click the **Resynchronize** button.

5. 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**.

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.

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
  - Identity Provider Connector
- Windows Login Protection

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.

oDiscouraged—It does not matter if the FIDO-compatible authenticator supports user verification or not.

- Authenticator Type

oPlatform (On bound)—The FIDO authenticator is a built-in solution (software, hardware) of the device where it is used as a second authentication factor.

oCross-platform (Roaming)—The FIDO authenticator is detachable and can be used with several devices.

oNot specified—Does not matter if the FIDO authenticator is detachable or not.

Register FIDO origin

If you want to use 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. Type the ESA Web Console URL in the **FIDO Origin** window. In our example, https://my-web-console.com:8001.

4. Click **Apply** > **Save**.

> FIDO origin
>
> Every ESA component where FIDO will be used as a second authentication factor, has to be registered as the origin.
> To use FIDO for other ESA component than ESA Web Console, self-enrollment for FIDO must be enabled, so that FIDO origin can be automatically set.

Activate FIDO for a Web Console administrator

In our example, we activate 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.

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 are typed.

Activate FIDO for a user

1. Navigate to **Settings** > **Enrollment**.

2. Enable **FIDO**, click **Save**.

3. Navigate to **Users**, select the applicable user.

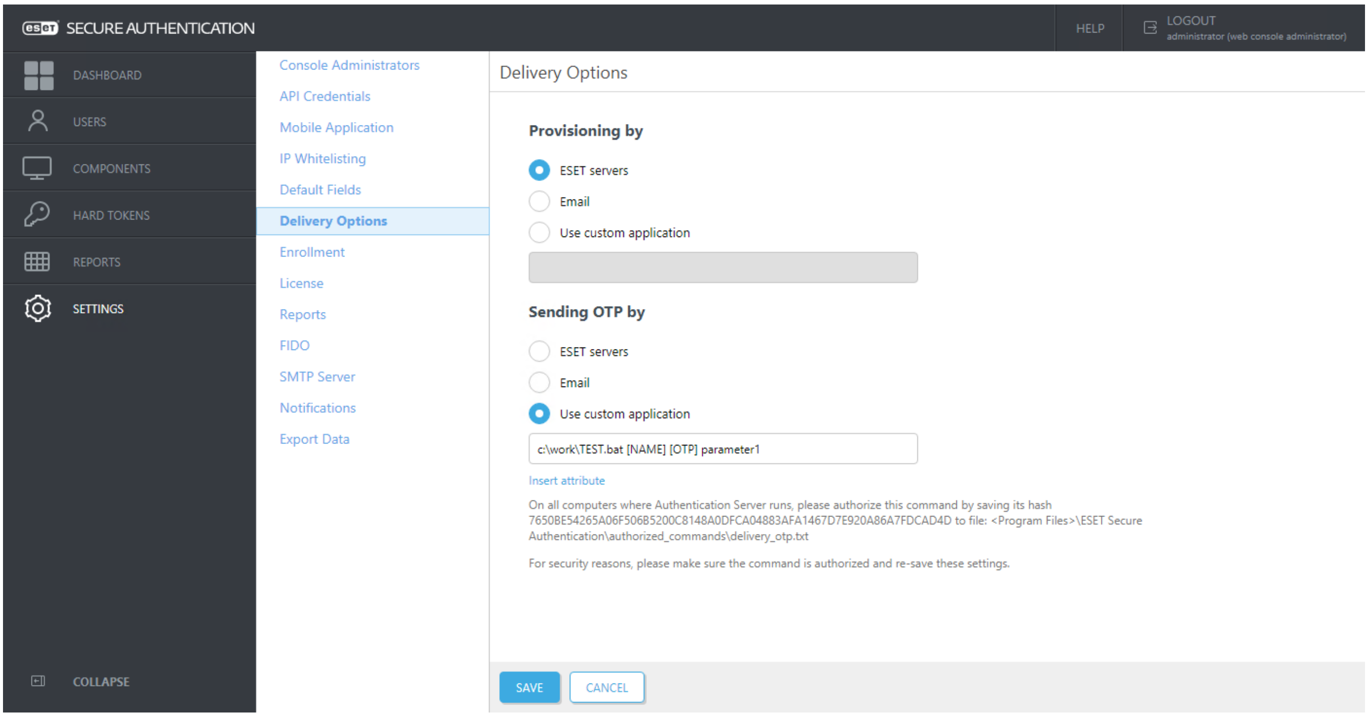
4. Turn on **FIDO**, click **Save**.

5. The user will have to finish setup during self-enrollment.

Delivery options

OTP (SMS, mobile app) default delivery options work perfectly for most users; ESA can also accommodate custom delivery options.

In ESA Web Console, click **Settings** ⚙ > **Delivery Options**.



Provisioning by

● ESET servers
○ Email
○ Use custom application

Sending OTP by

○ ESET servers
○ Email
● Use custom application

c:\work\TEST.bat [NAME] [OTP] parameter1

On all computers where Authentication Server runs, please authorize this command by saving its hash 7650BE54265A06F506B5200C8148A0DFCA04883AFA1467D7E920A86A7FDCAD4D to file: <Program Files>\ESET Secure Authentication\authorized_commands\delivery_otp.txt

For security reasons, please make sure the command is authorized and re-save these settings.

Select **Email**, or specify the path to your custom script by which you want to handle provisioning or delivery of OTP. Click **Insert attribute** to view a list of available parameters you can pass to your custom script. For example, 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).

Authorize commands

In ESET Secure Authentication version 3.0.21 and later, the **Use custom application** option requires command authorization.

1. Create an "`authorized_command`" folder in the folder displayed under the command field. In our example, `C:\Program Files\ESET Secure Authentication\`.

2. Based on the instructions under the command line field, create "`delivery_provisioning.txt`" or "`delivery_opt.txt`" in the "`authorized_command`" folder and save the provided hash in the folder.

3. Click **Save**.

Use email as the default delivery/provisioning option

To deliver OTP and/or provisioning information via email, define the details of a working SMTP server first:

1. In the ESA Web Console, click **Settings** > **SMTP Server** and fill in the required details.

    a.If SSL/TLS is used, the SMTP's SSL certificate must be trusted by the server hosting the Authentication Server.

2. Use the **Send test email** to test the configuration. If an email is delivered to the provided email address, the configuration is correct.

3. In **Settings** ⚙ > **Delivery Options**, select **Email**, click **Save**.

4. Enable **SMS-based OTPs** per user:

    a.Click **Users**.

    b.Click a user, enable **SMS-based OTPs**, click **Save**.

5. If self-enrollment is enabled, ensure **SMS-based OTPs** is enabled at **Settings** > **Enrollment** > **Default authentication types**.

> Security of authentication options
>
> ESA offers a wide range of 2FA methods that fit the varying preferences of our customers.
> The most secure and highly usable is Mobile Application Push (Push authentication).
> Still highly reliable, but in some situations, less convenient are: Mobile Application OTP, Hard Token, and FIDO.
> SMS-based OTPs, thus still available, are not considered the most secure mainly due to the underlying security used in the SMS delivery systems.
> When choosing the delivery of OTP by email, there might be usage schemas having weaker security.

Sample scenario available in Active Directory Integration deployment type - Delivering OTP via custom email solution (application)

Prerequisite

- Know the SMTP details of the email gateway you want to use for sending the email message containing the OTP

- Have a custom script for sending email messages

- Have a custom .BAT script you define the path to it in the ESA Web Console as shown in the screenshot above, while this .BAT script is going to call your custom script that is supposed to send the email message

- Every 2FA-enabled user who receives OTP passwords via email must have their email address defined in the **General** tab's **Email** field when viewing their details through the Active Directory Users and Computers management interface.

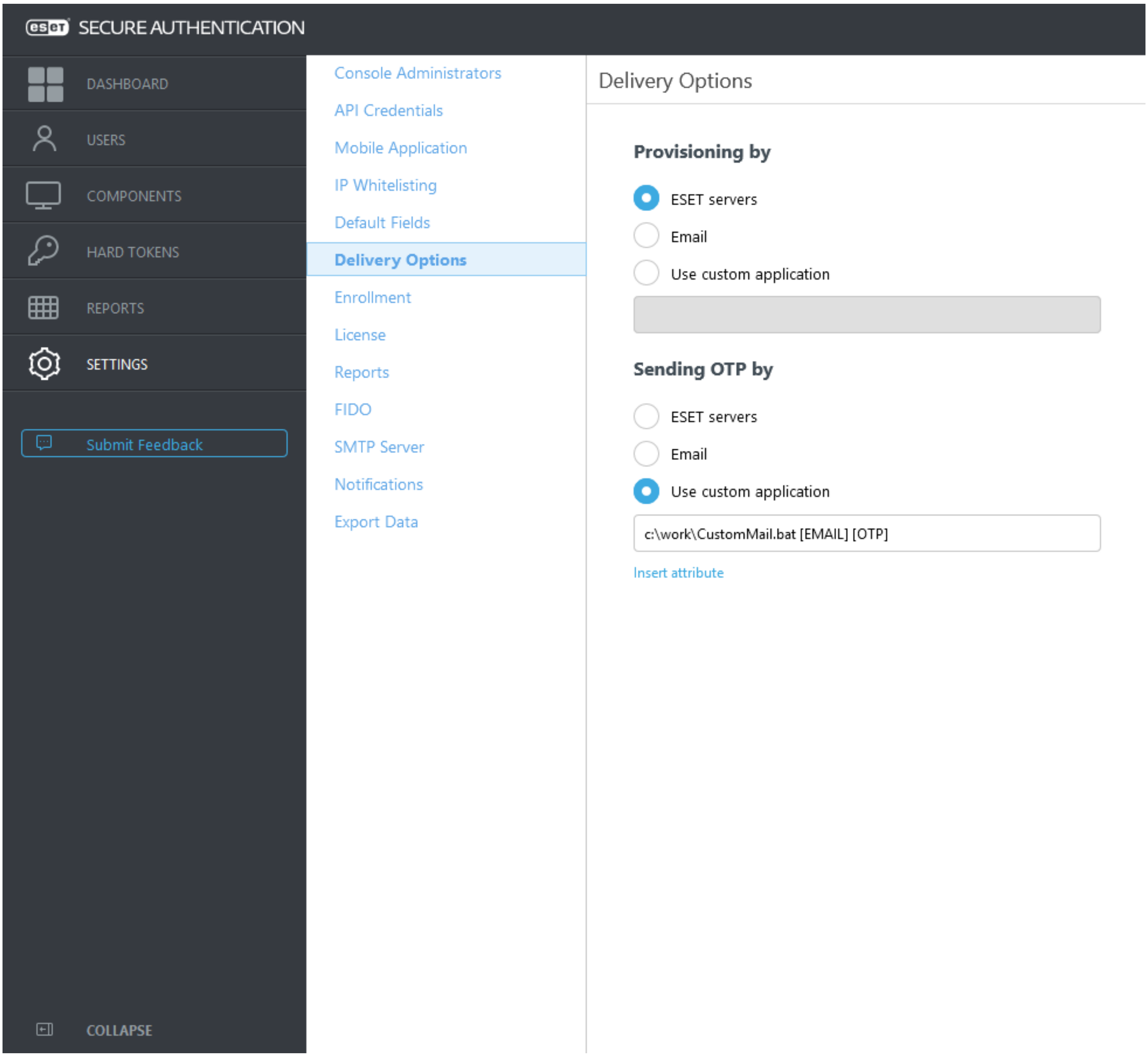
> ℹ SMTP details
>
> In the sample python script above the `smtpserver:port`, `username` and `password` are supposed to be replaced with the corresponding SMTP details.

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
```

> ℹ Prerequisite
>
> 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, define the path leading to **CustomMail.bat** script, select the essential parameters such as [E-mail-Addresses] and [OTP] and then click **Save**



Delivery Options

Provisioning by

● ESET servers
○ Email
○ Use custom application

Sending OTP by

○ ESET servers
○ Email
● Use custom application

c:\work\CustomMail.bat [EMAIL] [OTP]

Insert attribute

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

> **Email vs SMS delivery**
> Compared to SMS delivery (or usage of provisioned mobile application), email as the means of OTP distribution is slightly less secure because the email can be read on any device the user possesses. This method does not confirm that the intended recipient owns the registered phone (phone number).

Sample PowerShell scripts

Below are two sample PowerShell scripts to be used for delivering OTP via custom email solution (application).

PowerShell script using Send-MailMessage - we name the file as

sendmail.ps1

```
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 -Force
$credential = New-Object System.Management.Automation.PSCredential ($smtpUsername, $smtpPassword_sec)

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

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

```
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)
```

Replace the placeholders

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 `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]
```

Credential providers supported by ESA

Windows Login

Windows Login Protection by ESA provides two-factor authentication (2FA) only to password-protected Windows accounts (domain or local accounts). In this case, the original "password credential provider" is protected by 2FA.

If a Windows account can be accessed by Windows Hello, PIN, or a Microsoft account, ESA cannot provide 2FA protection for those login types.

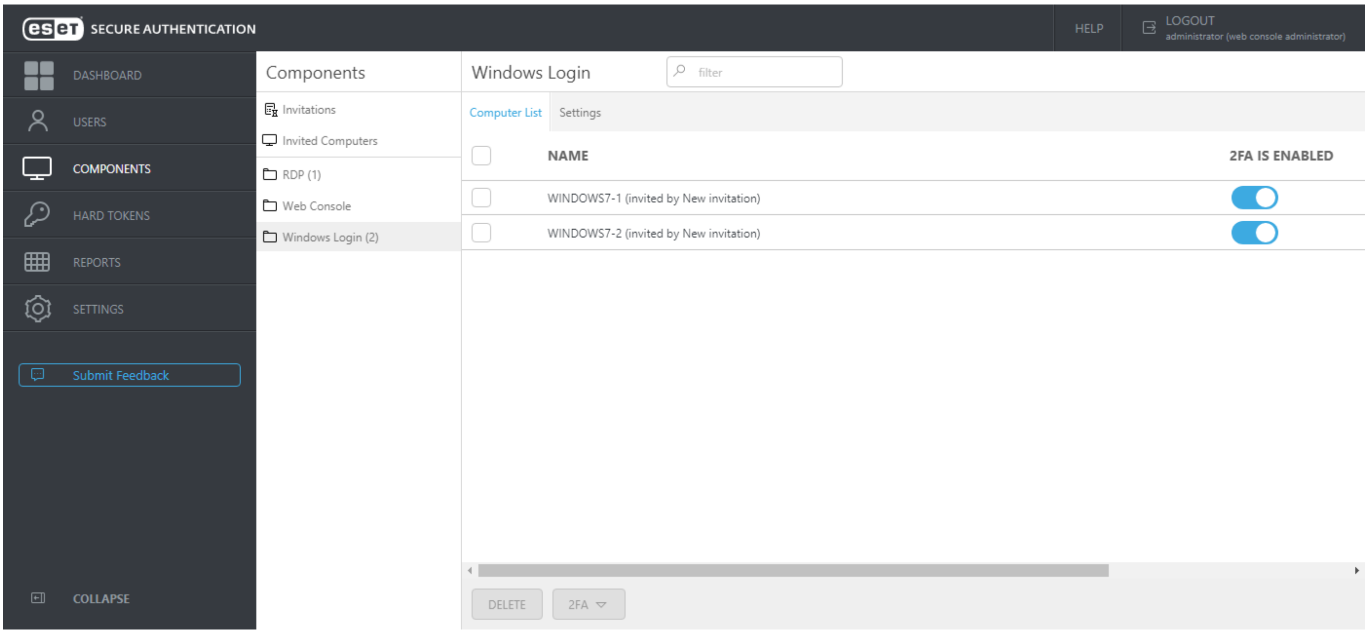
Remote Desktop Protocol (RDP)

ESA provides two-factor authentication only if the RDP client requires the first factor (username & password) before creating the remote session. Windows RDP works this way.

ESA RDP protection disables other credential providers.

Windows Login Protection

ESA features local login protection for Windows in a domain or LAN environment. To utilize this feature, select the **Windows Login** component during ESA installation. When the installation is complete, access the ESA Web Console, click **Components** > **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.

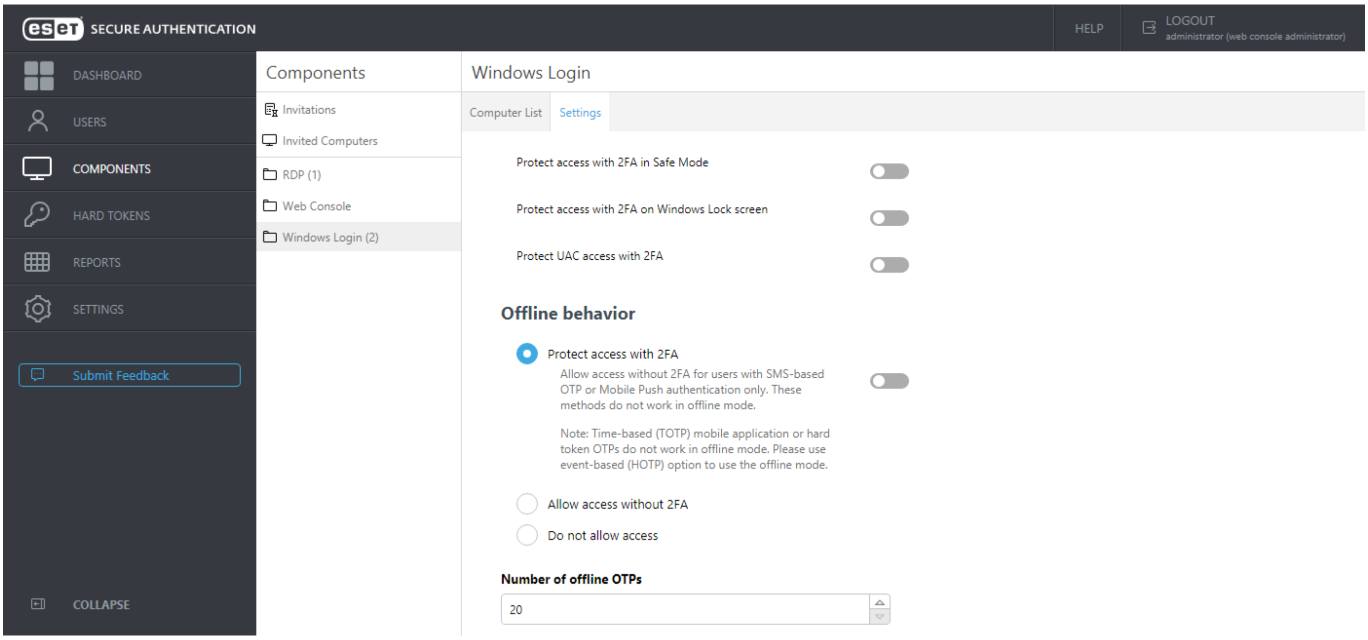


NAME	2FA IS ENABLED
WINDOWS7-1 (invited by New invitation)	●
WINDOWS7-2 (invited by New invitation)	●

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 specific computer, the computer will be automatically removed from the Computer List of ESA Web Console. 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. Suppose a computer entry is removed from the Computer List, but the **Windows Login** component is not removed from the specific computer. In that case, the computer will show up again in the Web Console with default settings.

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



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.

Note: Time-based (TOTP) mobile application or hard token OTPs do not work in offline mode. Please use event-based (HOTP) option to use the offline mode.

○ Allow access without 2FA

○ Do not allow access

Number of offline OTPs

20

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).

Suppose 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. In that case, 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, type their username and password again to receive a new OTP.

2FA protection cannot be bypassed by an attacker even if the attacker knows 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 drive's content is encrypted.

We recommend combining 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 first time while the PC is online. By 'online',we mean that the main computer where the Authentication Server is installed and the ESET Secure Authentication Service service is running and can be pinged from the 2FA-secured computer.

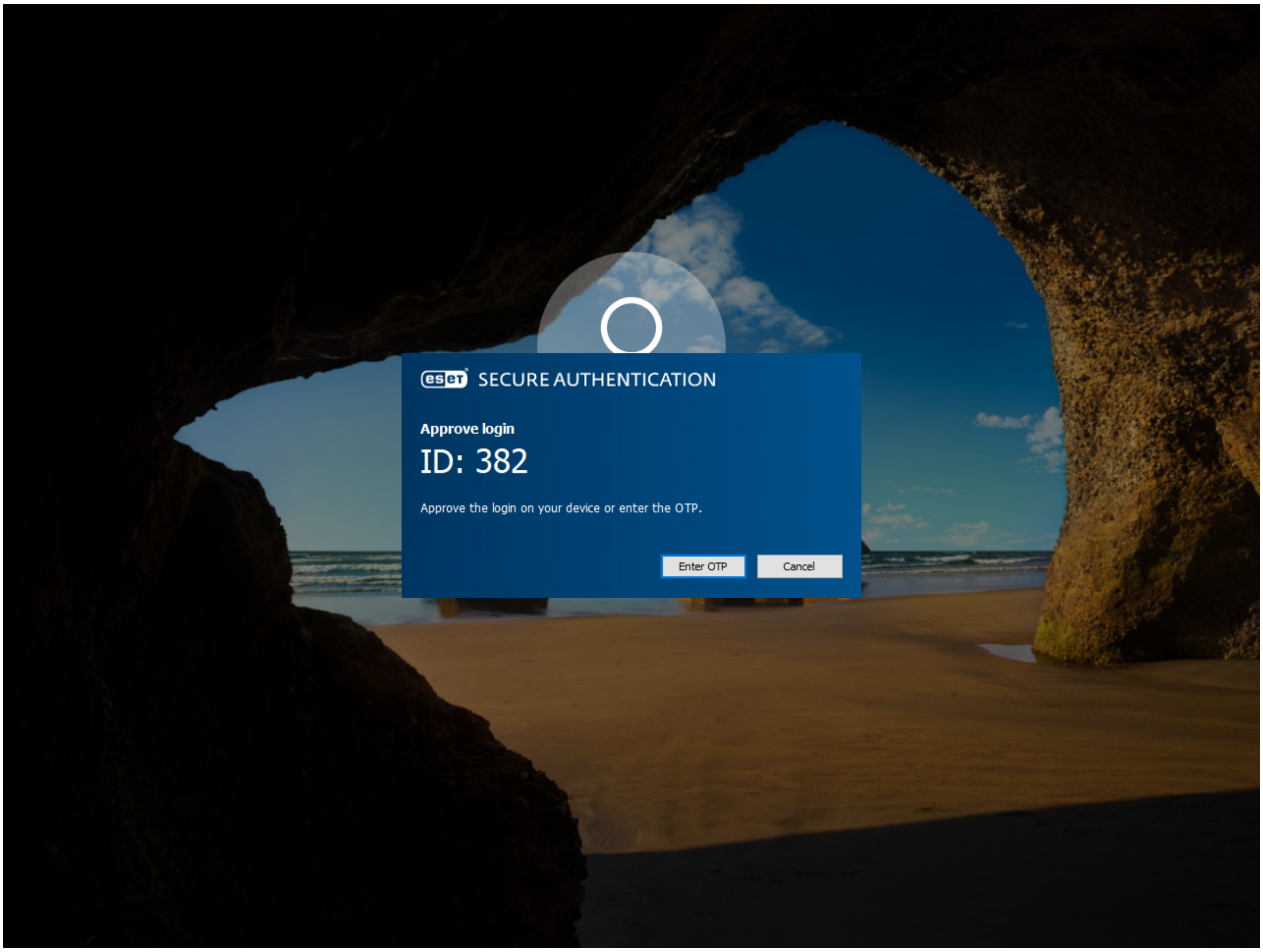
Suppose the Windows Login component is installed on the same computer where the Authentication Server is installed, and 2FA protection for Safe Mode is enabled. Simultaneously, the offline mode is disabled (**Do not allow access** is selected in **Offline behavior** section). In that case, the user will 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. You can increase the number of offline login limit in the Web Console at **Components > Windows Login > Settings > Number of offline OTPs**.

Time-based OTPs are not cached

OTPs generated by a time-based hard token or time-based OTPs generated by the mobile application are not stored in the offline cache of Windows Login plugin.

Suppose Windows 10 login is secured by ESA. After typing a valid username and password, users will be prompted to approve login on their Android/iOS mobile device, or Android/Apple watch, or to type an OTP.



SECURE AUTHENTICATION

Approve login

ID: 382

Approve the login on your device or enter the OTP.

Identity Provider Connector (IdP Connector)

Some online services (also known as "service providers") allow you to log in using third-party online services (also known as "identity providers").

Identity Provider Connector (IdP Connector) of ESA enables adding two-factor authentication between any cloud service (service provider) and identity providers, which use SAML standard.

Service and Identity Provider using SAML standard

1. There is always a Service Provider (SP) and an Identity Provider (IdP), and they need to know about each other. For example, the SP needs to know the metadata URL of the IdP and vice versa.

2. The user goes to the SP to log in but is redirected to the IdP.

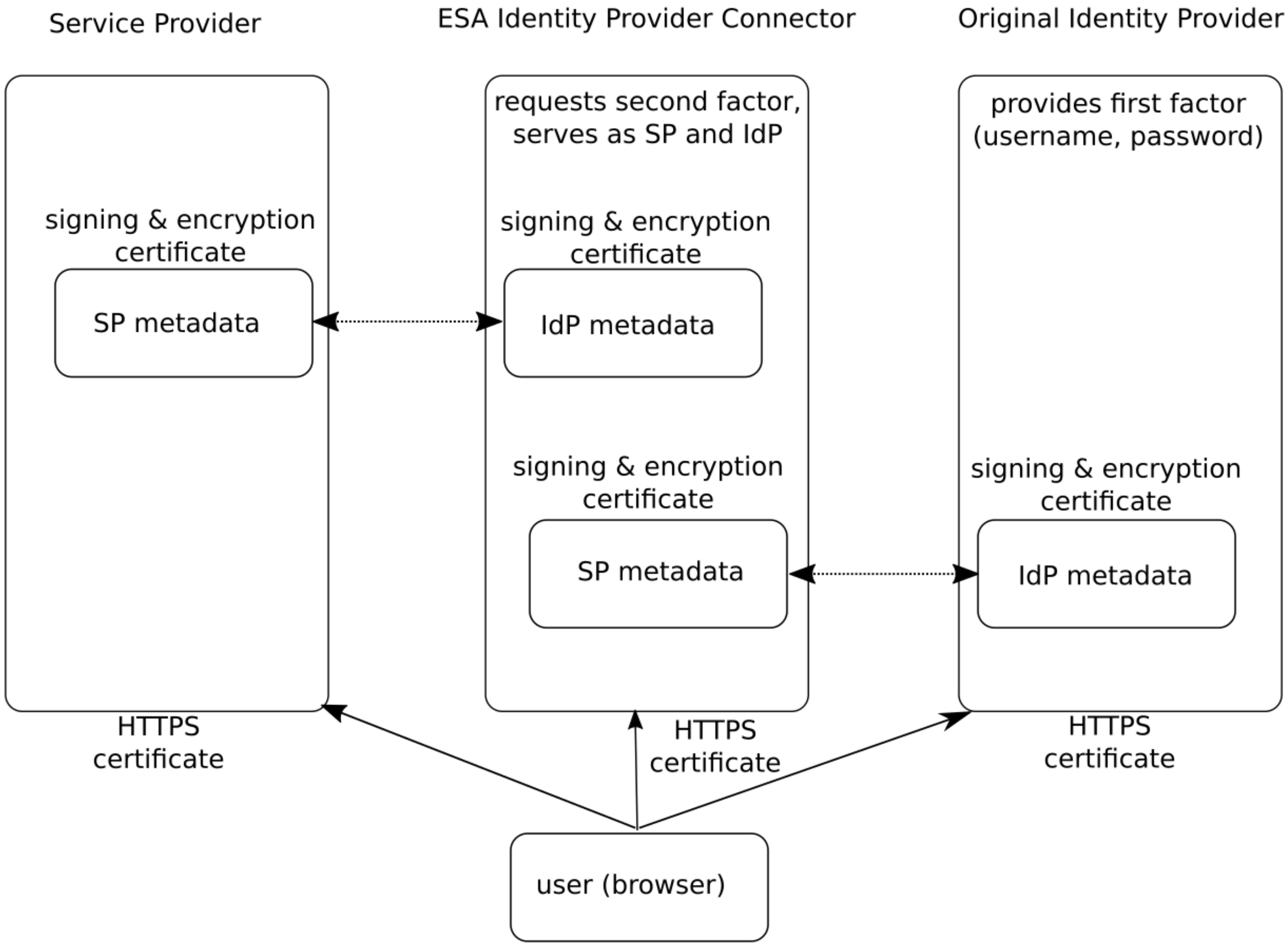
3. After successful login to the IdP, the user is redirected back to the SP with signed information about their identity.

4. The SP verifies the signature and then reads the user information, also called "claims".

Some services (SP, IdP) provide their configuration (URLs, certificate details) as SAML metadata file.

When ESA IdP Connector is implemented between a service provider and identity provider (later called "original identity provider"), the communication roles are as follows:

- The Service Provider (SP) uses ESA IdP Connector as the identity provider (IdP)
- The original IdP uses ESA IdP Connector as the SP
- ESA IdP Connector handles the request from the SP and contacts the original IdP to verify the first factor
- ESA IdP Connector provides 2FA interface to verify the second factor


Service Provider
ESA Identity Provider Connector
Original Identity Provider
requests second factor, serves as SP and IdP
provides first factor (username, password)
signing & encryption certificate
SP metadata
signing & encryption certificate
IdP metadata
signing & encryption certificate
SP metadata
signing & encryption certificate
IdP metadata
HTTPS certificate
HTTPS certificate
HTTPS certificate
user (browser)

Requirements

- ESA Identity Provider Connector (ESA IdP Connector) installed
- Identity provider (IdP) and Service provider (SP), both using SAML standard
- All certificates involved in the communication (singing certificate, decryption certificate, SSL certificate) must be valid

Identity providers tested with ESET Secure Authentication

- OpenAM
- Okta
- Azure AD
- AD FS
- Shibboleth
- Keycloak

Service providers tested with ESET Secure Authentication

- Dropbox
- Confluence

> ℹ **Custom logo**
>
> If you want a custom logo to be displayed on the screen waiting to type 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, AD FS protection, Identity Provider Connector) 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*".

Proceed to the configuration of Identity Provider Connector in ESA, or see our configuration examples.

Instructions to replace ESA IdProvider Connector certificate

Configure Identity Provider Connector (IdP Connector) in ESA Web Console

The configuration involves details of both Identity Provider (IdP) and Service Provider (SP).

1. In ESA Web Console, navigate to **Components** > **Identity Provider Connector**.

2. Click **Create New Identity Provider Configuration**.

3. In **Basic settings**:

    oType a desired **Configuration Name**. It will be used in the list of IdP Connector configurations.

    oType a desired **Path Name** which will be used as part of **Configuration URL** used in further configuration.

4. In **2FA settings**:

    oLeave **2FA enabled** selected to require second authentication factor from users who have any 2FA configured.

    oTo allow users not configured for any 2FA to log in through this IdP Connector configuration, leave **Allow non-2FA** selected.

5. In **Original Identity Provider**:

    o**Configuration from the Original Identity Provider**

    - **Use metadata**—use this option if the configuration metadata of the IdP is available through secure connection (HTTPS) or as a local file. Type that secure URL (starting with https:// or file://) to the **Metadata URL** field.

    - **Configure manually**—if you use this option, you have to retrieve and type manually the following details of the of the IdP:

        o**Single Sign-on Destination** where the authenticated user is redirected to log in. Some identity providers refer to it as Login URL.

        o**Single Logout Destination** where the user is redirected to log out. Some identity providers refer to it as Logout URL.

        o**Signature Validation Certificate**—signing certificate of the IdP.

    o**Configuration to the Original Identity provider**

    This section provides all essential information and data to configure the original identity provider to work with ESA IdP Connector.

    i. If the identity provider can read configuration from metadata, provide it the URL displayed in **Metadata URL**. Otherwise, use the information from the other fields (**Identifier**, **Sign-on response URL**, **Logout response URL**, **Logout URL**), and export the **Singing Certificate** and **Decryption Certificate** if your identity provider requires it .

ii. Configure the identity provider to issue Name ID claim in the format `<username>@<domain>` (the common options are email address or UPN). ESA IdP Connector will then register the user identified by `<username>` at the ESA Authentication Server in the `<domain>` realm.

6. Adjust **Advanced Security Settings** to meet your preferences, or if your IdP requires it.

oSign Requests to the original Identity Provider—if selected, **Singing Certificate** of ESA has to be configured as trusted on the machine hosting the IdP.

o**Validate original Identity Provider certificate**—if selected, the signing certificate of IdP must be configured trusted on the machine hosting ESA.

o**Check original Identity Provider certificate revocation**—if selected, ESA checks if the signing certificate of IdP is still valid.

7. Click **Add Service Provider**, and type a desired **Display Name**. It will be used in the list of configured service providers within the being configured IdP Connector.

o**Configuration from the Service Provider**

i. **Use metadata**—use this option if the configuration metadata of the identity provider is available through secure connection (HTTPS). Type that secure URL (starting with https://) to the **Service Provider Metadata URL** field.

ii. **Configure manually**—if you use this option, you have to retrieve and type manually the following details of the of the service provider:

o**Issuer**. Some SPs refer to it as Audience URL or Entity ID.

o**Single Sign-on Destination** where the authenticated user is redirected. Some SPs refer to it as Assertion Consumer Service URL.

o**Single Logout Destination** where the user is redirected after logout.

o**Signature Validation Certificate**—signing certificate of the SP.

b.**Configuration to the Service Provider**:

This section provides all essential information and data to configure the original identity provider to work with ESA IdP Connector

i. If the SP can read configuration from metadata, provide it the URL displayed in **Metadata URL**. Otherwise, use the information from the other fields (**Identifier**, **Sign-on URL**, **Logout URL**), and export the **Singing Certificate** and **Decryption Certificate** if your SP requires it .

ii. To remove, add or update collected identity information (claim) before forwarding it to the SP, create desired rules in the **Claims Translation** section. See claim translation examples below.

8. Adjust **Advanced Security Settings** to meet your preferences, or if your SP requires it.

o**Check signature of requests from the Service Provider**—if selected, the certificate of the SP has to be configured in ESA.

- oValidate Service Provider certificate—if selected, the certificate of SP must be configured trusted on the machine hosting ESA.

- oCheck Service Provider certificate revocation—if selected, ESA checks if the certificate of SP is still valid.

9. Click **Save**.

Claim translation examples

In the examples below we assume that we logged in through an IdP and the following claims were received by ESA IdP Connector:

```
http://original_identity_provider/claim/nameid: sample@user.com

http://original_identity_provider/claim/displayname: SU

http://original_identity_provider/claim/name: Sample User

http://original_identity_provider/claim/nameid: sample@user.com

http://original_identity_provider/claim/saml2nameid: sample@user.com

http://original_identity_provider/claim/samle2nameidformat: urn:oasis:names:tc:SAML:
1.1:nameid-format:emailAddress
```

Remove a certain claim

To remove "`http://original_identity_provider/claim/displayname: SU`" from the set of claims above, configure the following rule in ESA IdP Connector:

1. Click **Add**.

2. Select **Remove** from the list-box.

3. For **Type**, type "`http://original_identity_provider/claim/displayname`" without quotation marks.

4. Click **Save**.

To create a new claim with a custom value or update an existing claim (replace its value)

To replace "SU" with "sampleuser" in "`http://original_identity_provider/claim/displayname: SU`", configure the following rule in ESA IdP Connector:

1. Click **Add**.

2. Select **Add** from the list-box.

3. For **Type**, type "`http://original_identity_provider/claim/displayname`" without quotation marks.

4. For **Constant value**, type "sampleuser".

5. Click **Save**.

If "`http://original_identity_provider/claim/displayname`" did not exist in the received set of claims, it would be created with the value defined in **Constant value**:

"`http://original_identity_provider/claim/displayname: sampleuser`"

To create a new claim with the value of an existing claim

To create "`http://original_identity_provider/claim/profilename`" claim with the value of "`http://original_identity_provider/claim/displayname`" claim, configure the following rule in ESA IdP Connector:

1. Click Add.

2. Select **Copy** from the list-box.

3. For **From type**, type "`http://original_identity_provider/claim/displayname`" without quotation marks.

4. For **To type**, type "`http://original_identity_provider/claim/profilename`" without quotation marks.

5. Click **Save**.

IdP Connector Configuration Examples

In the configuration examples below we assume the following settings:

- ESA installation URL: `https://esa.test.local:44322/`
- **Path Name** configured in the ESA Identity Provider Connector (ESA IdP Connector>): *test*

Links to configuration examples below: Open AM, Okta, Azure AD, AD FS, Shibboleth, Dropbox, Confluence

Identity Providers

OpenAM

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. In section **Original Identity Provider** > **Configuration from the original Identity Provider**, set the **Metadata URL** to

```
https://<OpenAM_FQDN>/openam/saml2/jsp/exportmetadata.jsp?entityid=https://<OpenAM
_FQDN>/openam&realm=/
```

<OpenAM_FQDN> must be replaced with the domain name you specified when creating the hosted IdP in the OpenAM console.

3. If in the Advanced Settings of ESA IdP Connector configuration, the **Validate original Identity Provider certificate** and **Check original Identity Provider Certificate revocation** options are selected, the OpenAM signing certificate must be configured trusted on the machine where ESA IdP Connector is installed (for example, by adding them to Trusted People).

Configure OpenAM

1. Log in to OpenAM.

2. In **Realms**, select a realm, then select **Create SAML v2 Providers**.

3. Click **Register Remote Service Provider**.

4. Type the metadata URL gained from ESA:

   a.In ESA Web Console navigate to **Components** > **Identity Provider Connector** > select the configured IdP Connector > **Original Identity Provider** > **Configuration to the original Identity Provider** > **Metadata URL**. In our example: `https://esa.test.local:44322/test/metadata/ToIdentityProvider`

5. In **Circle of Trust**:

   a.Select **Add to existing**.

   b.Select the **Existing Circle of Trust** where your Hosted Identity Provider belongs.

6. Navigate to **Federation** > **Entity Providers** > select the identity provider being used > **Name ID Format**.

7. Assign a value to **Name ID Value Map** if there is none.

8. Import ESA IdP Connector sertificates to OpenAM using the Command Line tool.

```
keytool -importcert -alias esa_signing -keystore <openam_keystore.jks> -
file <esa_signing_certificate>

keytool -importcert -alias esa_decryption -keystore <openam_keystore.jks> -
file <esa_decryption_certificate>
```

In the code above the `<openam_keystore.jks>`, `<esa_signing_ceritificate>` and `<esa_decryption_ceritificate>` have to be replaced with the corresponding path leading to their location.

Okta

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. In section **Original Identity Provider** > **Configuration from the original Identity Provider**, set the **Metadata URL** to the URL you will retrieve from Okta when its configuration is complete:

  a.Log in to the created Okta application as an administrator.

  b.Select the **Sign On** tab, right-click the **Identity Provider metadata** in the **Settings** section and copy its link address (link location).

3. If in the Advanced Settings of ESA IdP Connector configuration, the **Validate original Identity Provider certificate** and **Check original Identity Provider Certificate revocation** options are selected, Okta signing certificate has to be configured trusted on the machine where ESA IdP Connector is installed (for example by adding them to Trusted People).

Configure Okta

1. Log in to Okta Admin account.

2. Navigate to **Applications** > **Applications**.

3. Click **Add Application**, then click **Create New App**.

4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**.

5. Click **Create**.

6. When configuring the App:

  a. **Single sing on URL**—retrieve the URL from ESA Web Console when configuring ESA IdP Connector:

    i. **Original Identity Provider** > **Configuration to the Original Identity Provider** > **Sign-on URL**. In our example:
    `https://esa.test.local:44322/test/Auth/LoginResponse`

  b.**Audience URI (SP Entity ID)**—retreive the corresponding value from ESA Web Console when configuring ESA IdP Connector:

    i. **Original Identity Provider** > **Configuration to the Original Identity Provider** > **Identifier**. In our example:
    `https://esa.test.local:44322/test/`

  c.In **SAML Settings**, select **Email** for **Application username**.

Azure AD

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. In section **Original Identity Provider** > **Configuration from the original Identity Provider**, set the **Metadata**

URL to the URL you will retrieve from Azure when its configuration is complete:

a.In the Azure portal, navigate to **Azure Active Directory** > **Enterprise applications** and select the application from the list.

b.Click **Single sing-on**, and copy the URL from the **App Federation Metadat Url** field in the **SAML Singing Certificate** section.

3. If in the Advanced Settings of ESA IdP Connector configuration, the **Validate original Identity Provider certificate** and**Check original Identity Provider Certificate revocation** options are selected, Azure signing certificate has to be configured trusted on the machine where ESA IdP Connector is installed (for example by adding it to Trusted People). You can download the Azure signing certificate from the Azure portal:

a.Navigate to **Azure Active Directory** > **Enterprise applications** > select the application you configured for single sign-on > **Single sing-on**.

b.In the **SAMLE Signing Certificate** section, click **Download** next to **Certificate (Raw)**.

Configure Azure AD

1. Log in to Azure portal.

2. Navigate to **Azure Active Directory** > **Enterprise applications** > **New Application**.

3. Click **Non-gallery application**.

4. In the **Single sing-on** section configure the following fields based on information retrieved from ESA IdP Connector configuration:

a.**Identifier (Entity ID)**—use the value from **Original Identity Provider** > **Configuration to the Original Identity Provider** > **Identifier**. In our example:
`https://esa.test.local:44322/test`

b.**Reply URL (Assertion Consumer Service URL)**, **Sign on URL**—use the value from **Original Identity Provider** > **Configuration to the Original Identity Provider** > **Sign-on URL**. In our example:
`https://esa.test.local:44322/test/Auth/LoginResponse`

c.**Logout Url**—use the value from **Original Identity Provider** > **Configuration to the Original Identity Provider** > **Logout URL**. In our example:
`https://esa.test.local:44322/test/Auth/LogoutResponse`

AD FS

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. In section **Original Identity Provider** > **Configuration from the original Identity Provider**, set the **Metadata URL** to

```
https://AD FS_FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
```

where *<AD FS_FQDN>* has to be replaced with the domain name of your AD FS server.

3. If in the Advanced Settings of ESA IdP Connector configuration, the **Validate original Identity Provider certificate** and **Check original Identity Provider Certificate revocation** options are selected, AD FS signing certificate has to be configured trusted on the machine where ESA IdP Connector is installed (for example by adding it to Trusted People).

Configure AD FS

1. Open AD FS Management.

2. Click **Trust Relationships** > **Relying Party Trusts** > **Add relying Party Trust**.

3. Select **Claims Aware**, click Start.

4. Select **Import data about the relying party published online or on a local network**, and type into the **Federation metadata address (host name URL)** field the metadata URL provided in ESA IdP Connector:

   a.**Original Identity Provider** > **Configuration to the Original Identity Provider** > **Metadata URL**

5. Complete the configuration.

6. When you click **Close** in the **Finish** page, the **Edit Claim Rules** dialog box opens automatically.

7. Select **Issuance Transform Rules** tab, click **Add Rule**.

8. From **Claim rule template**, select **Send LDAP Attributes as Claims**, click **Next**.

9. From **Attribute store**, select **Active Directory**.

10. Select **User-Principal-Name** for **LDAP Attribute**, and **Name ID** for **Outgoing Claim**.

11. Click **Finish**, then click **OK** in the **Edit Claim Rules** dialog box.

12. Apply the following configuration through PowerShell:

```
Set-ADFSRelyingPartyTrust -Targetname "<relying_party_name>" -
SigningCertificateRevocationCheck "none"

Set-ADFSRelyingPartyTrust -Targetname "<relying_party_name>" -
EncryptionCertificateRevocationCheck "none"
```

In the code above replace `<relying_party_name>` with the name of Relying Party Trust you configured in previous steps.

13. Download certificates from ESA IdP Connector, section **Original Identity Provider** > **Configuration from the original Identity Provider**, and import them to the Windows certificate store to make them trusted.

Shibboleth

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. In section **Original Identity Provider** > **Configuration from the original Identity Provider**, set the **Metadata URL** to

```
file://C:\Program Files (x86)\Shibboleth\IdP\metadata\idp-metadata.xml
```

if ESA IdP Connector is installed on the same machine as Shibboleth. Otherwise, copy the *idp-metadata.xml* file of Shibboleth to the computer where ESA IdP Connector is installed and refer to that path.

3. If in the Advanced Settings of ESA IdP Connector configuration, the **Validate original Identity Provider certificate** and **Check original Identity Provider Certificate revocation** options are selected, Shibboleth signing certificate (located at *C:\Program Files (x86)\Shibboleth\IdP\credentials\idp-signing.crt* by default) has to be configured trusted on the machine where ESA IdP Connector is installed (for example by adding it to Trusted People).

Configure Shibboleth

1. Download the ESA IdP Connector metadata file from the URL provided in ESA IdP Connector:

a.**Original Identity Provider** > **Configuration to the Original Identity Provider** > **Metadata URL**

b.Save it on the computer where Shibboleth is installed and refer to its location in "*C:\Program Files (x86)\Shibboleth\IdP\conf\metadata-providers.xml*":

```
<MetadataProvider id="sp-
metadata" xsi:type="FilesystemMetadataProvider" metadataFile="<metadata_xml_fil
e_from_esa>"/>
```

In the code above `<metadata_xml_file_from_esa>` refers to the path of downloaded ESA IdP Connector metadata file.

2. Make Shibboleth to send some data, that identifies the user, in email format as the value of NameID parameter. For example, mail LDAP attribute:

a.Define for `shibboleth.SAML2NameIDGenerators` in "C:\Program Files (x86)\Shibboleth\IdP\conf\saml-nameid.xml":

```
<bean parent="shibboleth.SAML2AttributeSourcedGenerator" p:omitQualifiers="true
" p:format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress" p:attributeSourceIds="#{ {'mail'} }" />
```

b.Add to "*C:\Program Files (x86)\Shibboleth\IdP\conf\saml-nameid.properties*":

```
idp.nameid.saml2.default = urn:oasis:names:tc:SAML:1.1:nameid-
```

```
format:emailAddress
```

Keycloak

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. In section **Original Identity Provider** > **Configuration from the original Identity Provider**, set the **Metadata URL** to

```
https://<keycloak>/auth/realms/<realm>/protocol/saml/descriptor
```

while in the URL above replace `<keycloak>` with the domain name (and port) of your Keycloak instance, and `<realm>` with the corresponding realm name.

3. If in the Advanced Settings of ESA IdP Connector configuration, the **Validate original Identity Provider certificate** and **Check original Identity Provider Certificate revocation** options are selected, Keycloak signing certificate has to be configured trusted on the machine where ESA IdP Connector is installed (for example by adding it to Trusted People).

Configure Keycloak

1. Download the ESA IdP Connector metadata as an XML file from ESA Web Console:

   a.Open the metadata URL found at **Components** > **Identity Provider Connector** > select the configured IdP Connector > **Original Identity Provider** > **Configuration to the Original Identity Provider** > **Metadata URL** in a browser.

   b.Press **CTRL + S**, select "XML" for **Save as type** if available, click **Save**.

2. Log in to Keycloak admin console.

3. Click **Clients** > **Create**.

4. Next to **Import**, click **Select file**, browse for the metadata *.xml* file downloaded in step 1.

5. From **Client Protocol**, select **SAML**.

6. Complete the rest of the fields and click **Save**.

7. In the **Settings** tab of the created client, turn off **Sign Assertions**.

8. From **Name ID Format**, select **email**.

Service Providers

Dropbox

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. When you add a service provider, select **Configure manually** in the **Configuration from the Service Provider** section.

3. For **Issuer**, type `http://Dropbox`.

4. Set the **Single Sign-on Destination** to `https://www.dropbox.com/saml_login`.

5. Copy the **Sign-on URL**, **Logout URL** to a text file, and export the **Singing Certificate** for a later use when configuring your Service Provider.

6. In **Advanced Security Settings**, deselect **Check signature of requests from the Service Provider**.

Configure Dropbox

1. Log in to Dropbox as administrator.

2. Navigate to **Settings** > **Single sing-on**.

3. Type into the **Sing-in URL** field the **Sign-on URL** you copied from the configured ESA IdP Connector.

4. Type into the **Sign-out URL** field the **Logout URL** you copied from the configured ESA IdP Connector.

5. For **X.509 Certificate**, import the Signing Certificate you exported previously from the configured ESA IdP Connector.

Confluence

Configure ESA IdP Connector

1. Follow the generic instruction on configuring IdP Connector in ESA Web Console.

2. When you add a service provider, select **Configure manually** in the **Configuration from the Service Provider** section.

3. For **Issuer**, copy and paste the URL address found in Confluence admin console at **SAML Authentication** > **Audience URL (Entity ID)**.

4. For **Single Sign-on Destination**, copy and paste the URL address found in Confluence admin console at **SAML Authentication** > **Assertion Consumer Service URL**.

5. Copy the **Identifier**, **Sign-on URL** to a text file, and export the **Singing Certificate** for a later use when

configuring your Service Provider.

6. In **Advanced Security Settings**, deselect **Check signature of requests from the Service Provider**.

Configure Confluence

1. Log in to Confluence as administrator.

2. Click **SAML Authentication**.

3. In the **SAML SSO 2.0 settings** section:

   a.Type into the **Single sing-on Issuer** field the **Identifier** you copied from the ESA IdP Connector.

   b.Type into the **Identity provider single sign-on URL** field the **Sign-on URL** you copied from ESA IdP Connector.

   c.Copy and paste into **X.509 Certificate** field the content of Signing Certificate you exported from ESA IdP Connector.

Master recovery key

A master recovery key (MRK) is an alternative OTP that can be used to log in to a computer or service protected by 2FA in situations where the user cannot type 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 ESA component, meaning, User1 and User2 would have a different MRK for PC1. Access via MRK is available even in online and offline mode for Windows Login Protection. 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.

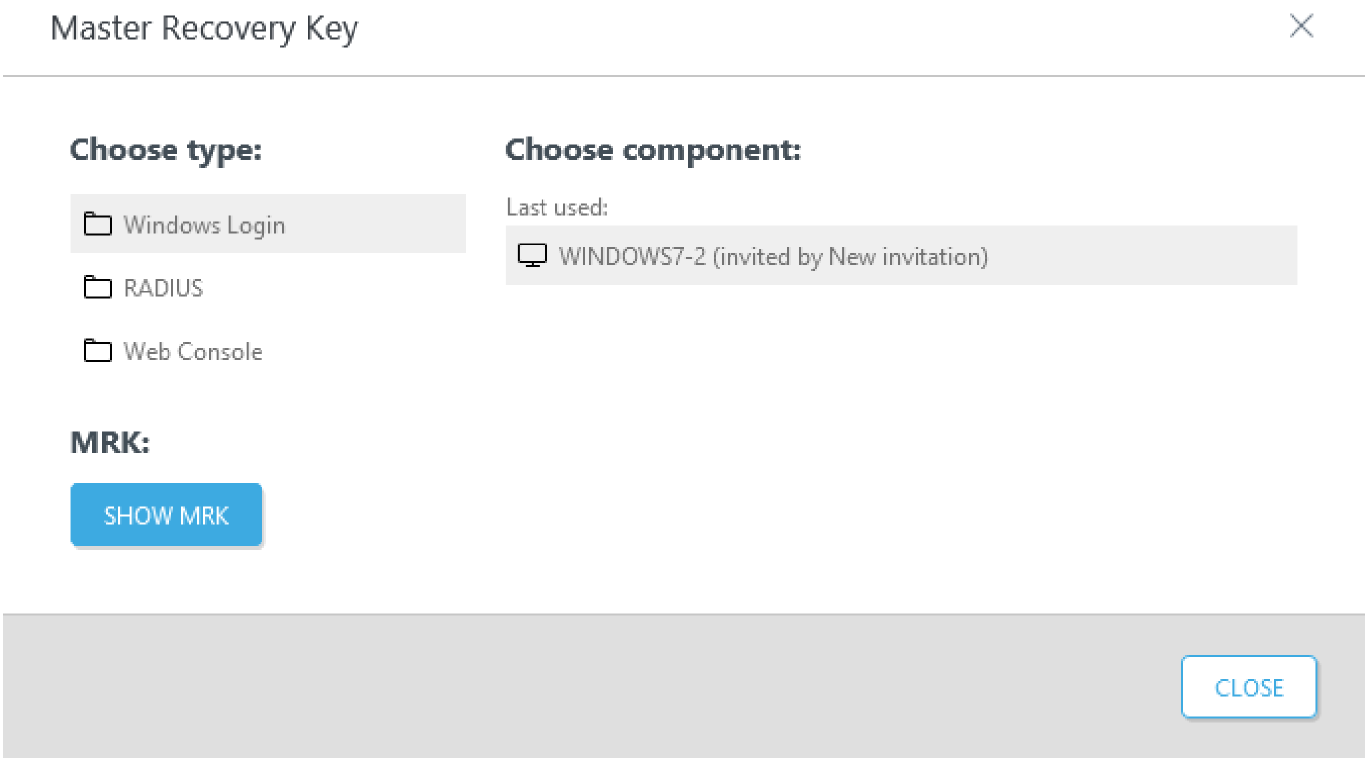
In ESA version 2.6 and later, you can use MRK also for other components than Windows Login.

To use MRK for authentication

The example below uses MRK for Windows Login.

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 specific user > clicks **Actions** > selects **Show MRK** > selects the protection module type in **Choose type** section, then selects the specific computer from the **Choose component** list, and clicks **Show MRK**. At this point a **MRK** is generated.



Master Recovery Key

Choose type:

Choose component:

Last used:

WINDOWS7-2 (invited by New invitation)

MRK:

Multiple ESA components

If the user had multiple ESA components listed within a specific protection module (for example, multiple computers within Windows Login protection module), the actual component for which the user is requesting MRK would be listed at the top of the list as **Last used**.

3. The administrator provides the obtained MRK to the user, who can log in by typing the MRK instead of OTP.

While the computer is in offline mode, an MRK may be used to log in to the specific 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 a successful login using MRK or other authentication option.

Reset ESA Web Console administrator credentials

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, type the original administrator username and a new password when prompted. To create a different account, type a new username and password.

4. Close the installer when complete.

5. Restart the ESET Secure Authentication Core service for the change to take effect.

RADIUS server and 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.

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.

RADIUS Configuration

To configure 2FA for your VPN, add your VPN appliance as a RADIUS client:

1. In the ESA Web Console, navigate to **Components** > **RADIUS**, select a RADIUS server, and click **Create new RADIUS client**.

2. In the **Basic Settings** section:

   a.Give the RADIUS client a memorable name for easy reference.

   b.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).

   c.The shared secret is the RADIUS shared secret for the external authenticator you will configure on your appliance.

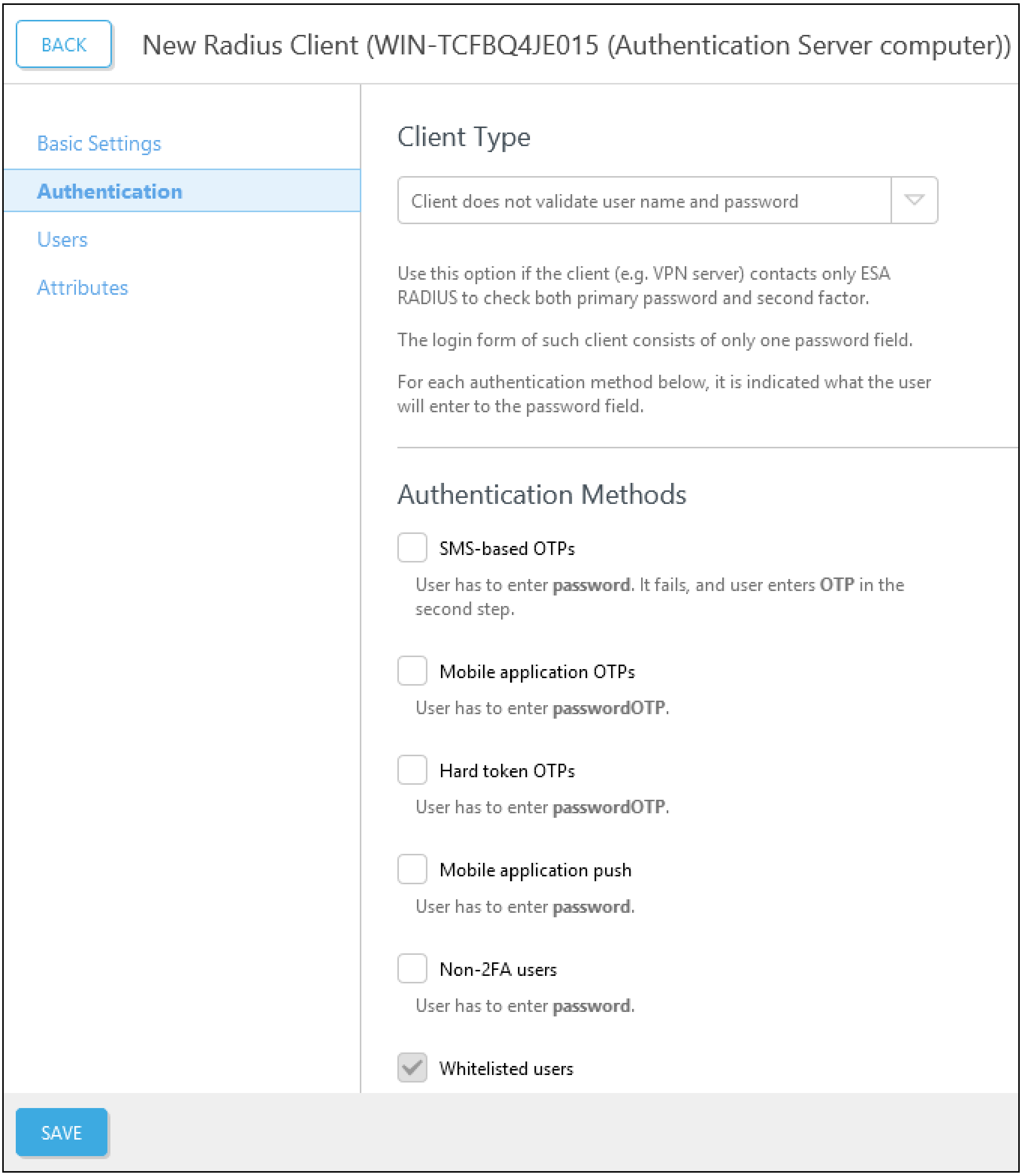
3. In the **Authentication** section:

   a.Select the Client Type.

   b.Select the desired authentication method. The optimal authentication method depends on your VPN appliance make and model. See ESA VPN integration guidelines for more details in the ESET Knowledgebase.

   c.Optionally, you can allow any non-2FA users to use the VPN.

> i
>
> ### Non-2FA users
>
> 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.
> Suppose an ESA RADIUS client is configured to allow Non-2FA users to log in using their generic credentials. If self-enrollment with any default authentication type is enabled, all users will be requested to provide 2FA or MRK to authenticate.



New Radius Client (WIN-TCFBQ4JE015 (Authentication Server computer))

Client Type

Client does not validate user name and password

Use this option if the client (e.g. VPN server) contacts only ESA RADIUS to check both primary password and second factor.

The login form of such client consists of only one password field.

For each authentication method below, it is indicated what the user will enter to the password field.

Authentication Methods

☐ SMS-based OTPs

User has to enter **password**. It fails, and user enters **OTP** in the second step.

☐ Mobile application OTPs

User has to enter **passwordOTP**.

☐ Hard token OTPs

User has to enter **passwordOTP**.

☐ Mobile application push

User has to enter **password**.

☐ Non-2FA users

User has to enter **password**.

☑ Whitelisted users

4. In the **Users** section, from the **Realm** selection box, select **Current AD domain** or **Current AD domain and domains in trust** 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.

5. If your VPN client requires additional RADIUS attributes to be sent by ESA RADIUS, in the **Attributes** section, click **Add** to configure them.

6. When you are finished making changes, click **Save**.

7. Restart 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.

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

Client Type options

- **Client does not validate user name and password**
- **Client validates user name and password**
- **Use Access-Challenge feature of RADIUS**
- **Client does not validate user name and password - avoid compound**

More information on Client Type options

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

- Pulse Connect Secure (formerly Junos Pulse (VPN))
- Linux PAM module

The Microsoft RRAS RADIUS client should not be used with the Access-Challenge feature.

RADIUS Usage

When 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.

VPN Authentication Options

This section reviews available configuration options for a RADIUS client using the ESA Web Console in an AD environment.

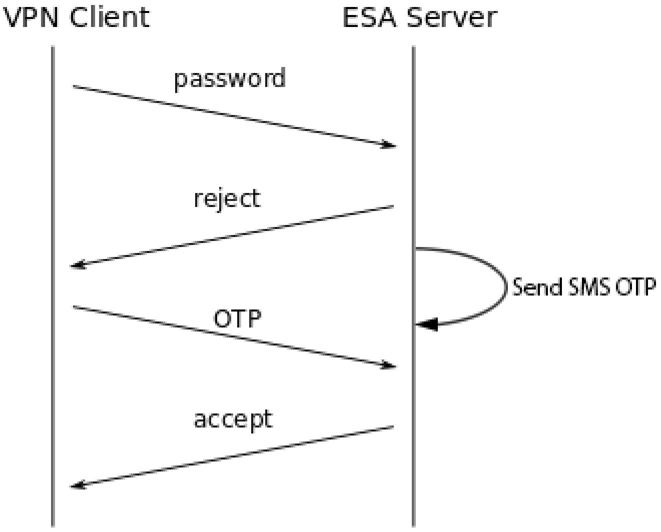
SMS-based OTPs

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 type 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

On-demand SMS-based OTP

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.

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 types '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 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.

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 typing 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 types 'password123456' in the password field of their VPN client.

Supported authentication protocols: PAP.

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.

Non-2FA Pass-through

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

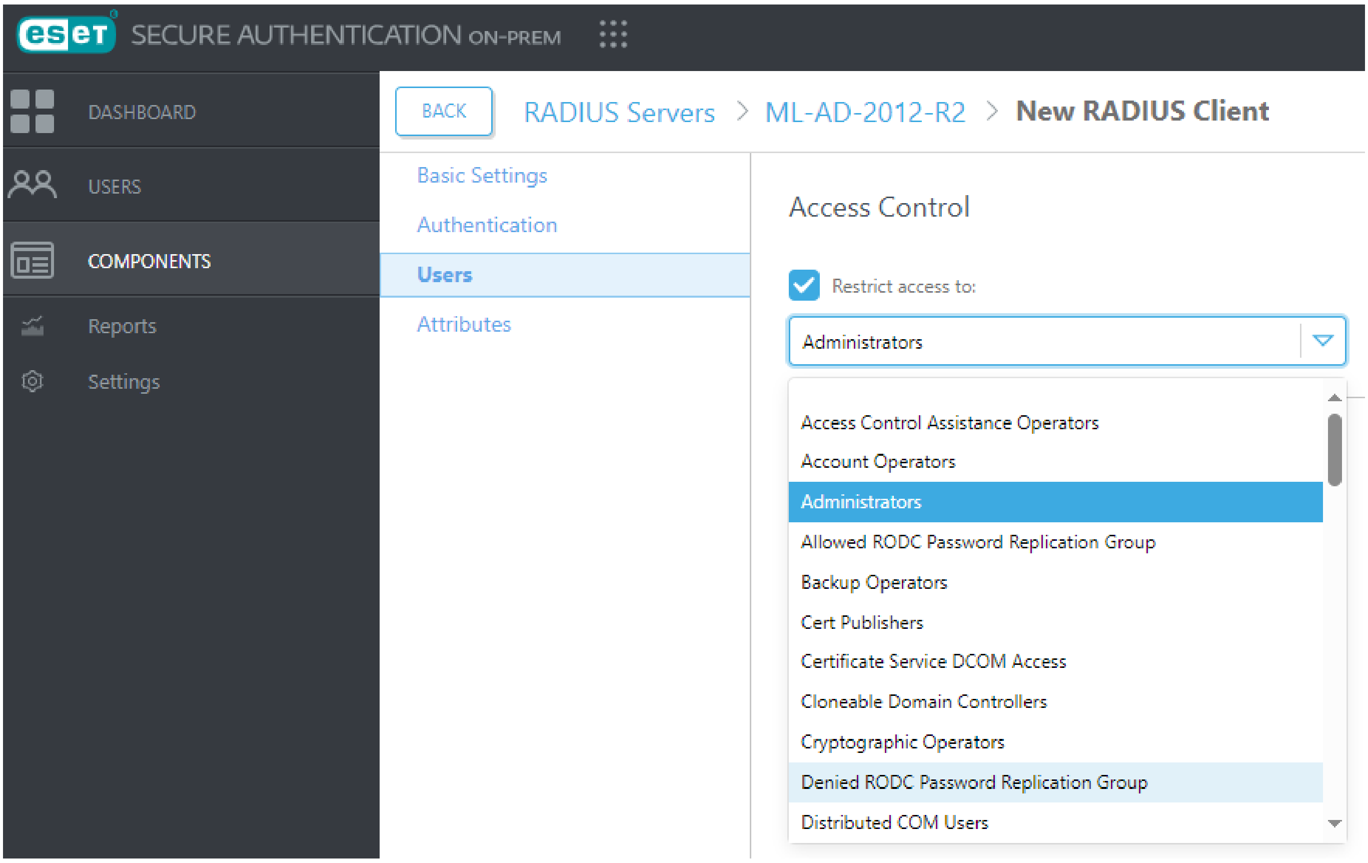
In this configuration, the user logs in with their Active Directory password.

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.

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.



Access Control

☑ Restrict access to:

Administrators

Access Control Assistance Operators
Account Operators
Administrators
Allowed RODC Password Replication Group
Backup Operators
Cert Publishers
Certificate Service DCOM Access
Cloneable Domain Controllers
Cryptographic Operators
Denied RODC Password Replication Group
Distributed COM Users

ESA Authentication Methods and PPP Compatibility

The VPN server must be configured to allow all protocols 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

Verifying ESA RADIUS functionality

This following articles describe the necessary steps for verifying the connectivity of your ESA RADIUS server. Each client connecting to the RADIUS server has to be explicitly configured in ESA Web Console as a RADIUS Client.

Troubleshooting a RADIUS server consists of the following steps:

- Verifying that your RADIUS server is listening for incoming requests
- Testing connectivity to the RADIUS server from your localhost
- Testing connectivity to the RADIUS server over the network

The last two steps require the NTRadPing utility.

To complete the tests in this guide, you will need an Active Directory (AD) user account for testing purposes. The user **Alice** is referred to throughout this guide as the AD user account used for testing. The static AD password `Esa132` is used as the password for this testing account for the purposes of this guide.

> Notes
>
> Make sure that **Alice** has no 2FA methods enabled in the ESA Web Console before you begin.
> This guide wsas written for a deployment scenario where the ESA RADIUS Server is running on the same server as the ESA Authentication Server.

Make sure your ESA RADIUS Service is running

1. Open your Windows Services console, and verify that the **ESET Secure Authentication RADIUS Service** is in the Running state, as shown in **Figure 1**.

2. In this step we verify that ESA RADIUS Server process is listening on the port selected during installation of **RADIUS Server for VPN Protection** component, by default UDP 1812. If you defined a different **RADIUS Port**, look for that port in the output of the command below.

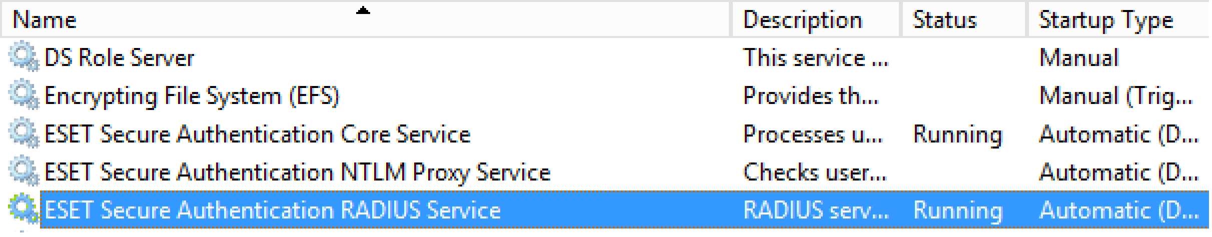
   a.Open a command prompt and type the following command:

```
C:\>netstat –a –p udp –b | more
```

b.Verify that EIP Radius.WindowsService.EXE is the only service listening on UDP1812

Active Connections

```
Proto  Local Address                         Foreign Address
 State

UDP    0.0.0.0:1812                          *:*

[EIP.Radius.WindowsService.EXE]
```



Name	Description	Status	Startup Type
DS Role Server	This service ...		Manual
Encrypting File System (EFS)	Provides th...		Manual (Trig...
ESET Secure Authentication Core Service	Processes u...	Running	Automatic (D...
ESET Secure Authentication NTLM Proxy Service	Checks user...		Automatic (D...
ESET Secure Authentication RADIUS Service	RADIUS serv...	Running	Automatic (D...

Figure 1: Verify that the ESET Secure Authentication RADIUS Service is Running

Configure your RADIUS Server

Follow the steps below to configure a dummy RADIUS client:

1. Log in to ESA Web Console and ensure that an active ESA license is being used by the installation (the status of the license may be viewed in the **Dashboard**).

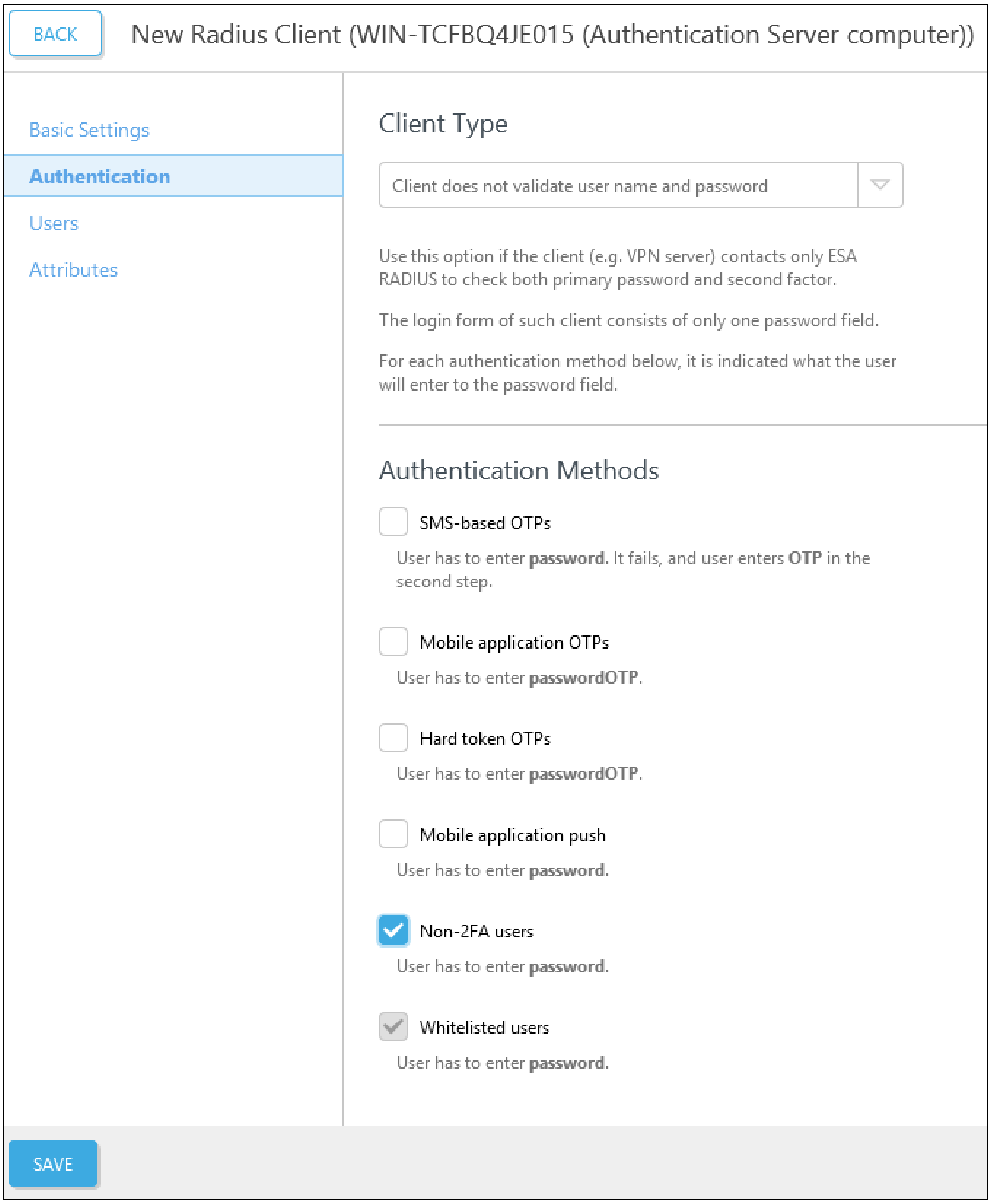
2. Navigate to **Components** > **RADIUS** and click your RADIUS server name. Click **Create new RADIUS client**.

3. In **Basic Settings**:

a.give the RADIUS client a memorable name for easy reference.

b.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. In **Authentication**, fill out the details as shown in the screenshot below:



New Radius Client (WIN-TCFBQ4JE015 (Authentication Server computer))

Client Type

Client does not validate user name and password

Use this option if the client (e.g. VPN server) contacts only ESA RADIUS to check both primary password and second factor.

The login form of such client consists of only one password field.

For each authentication method below, it is indicated what the user will enter to the password field.

Authentication Methods

□ SMS-based OTPs

User has to enter **password**. It fails, and user enters **OTP** in the second step.

□ Mobile application OTPs

User has to enter **passwordOTP**.

□ Hard token OTPs

User has to enter **passwordOTP**.

□ Mobile application push

User has to enter **password**.

☑ Non-2FA users

User has to enter **password**.

☑ Whitelisted users

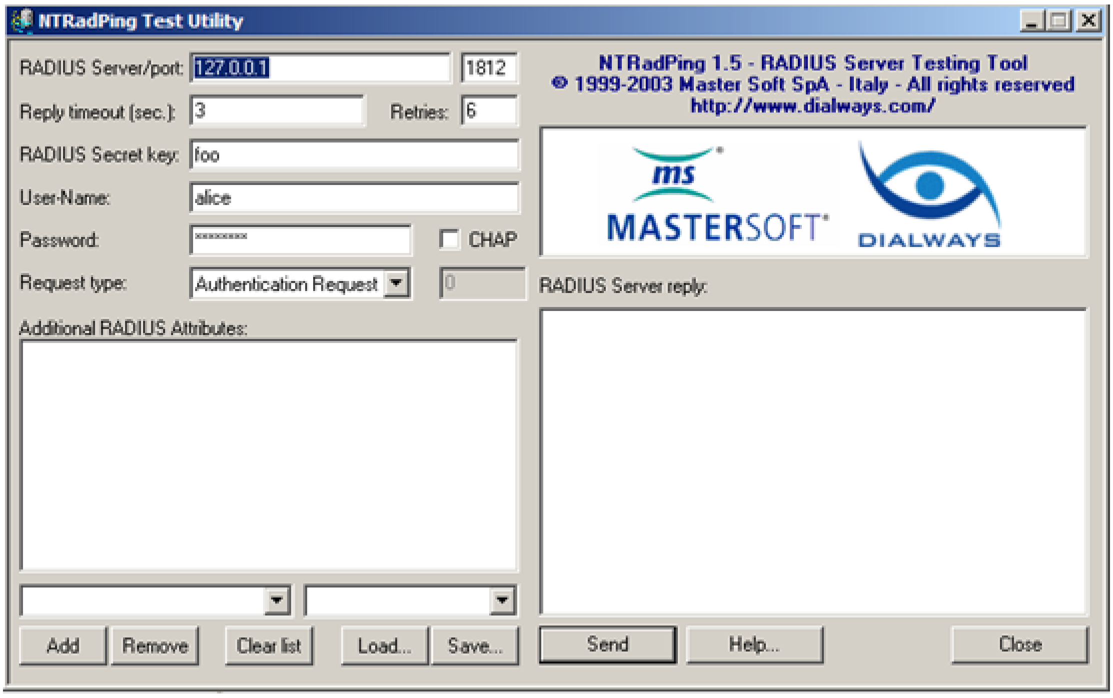
User has to enter **password**.

5. In **Users** > **Realm**, select **Current AD domian**.

6. Click **Save**.

Verify functionality (localhost)

1. Launch NTRadPing and fill out the values as shown in the following screenshot:



NTRadPing Test Utility

RADIUS Server/port: 127.0.0.1 1812

Reply timeout (sec.): 3 Retries: 6

RADIUS Secret key: foo

User-Name: alice

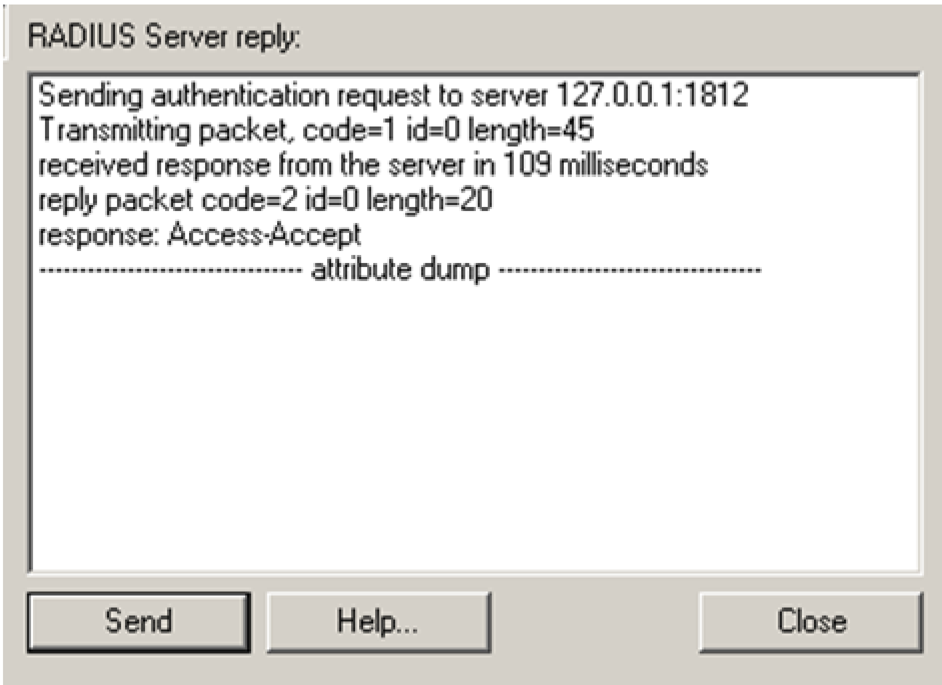
Password: xxxxxxxx □ CHAP

Request type: Authentication Request 0

Additional RADIUS Attributes:

2. Click **Send**.

3. Verify that you received an **Access-Accept** response:



RADIUS Server reply:

```
Sending authentication request to server 127.0.0.1:1812
Transmitting packet, code=1 id=0 length=45
received response from the server in 109 milliseconds
reply packet code=2 id=0 length=20
response: Access-Accept
-------------------------------- attribute dump --------------------------------
```

4. If you received a response other than **Access-Accept**, proceed to the troubleshooting section.

Verify network connectivity from another machine (optional)

This step is useful to make sure that there are no networking issues between your machines.

1. If you received an **Access Accept** response during the first test and you are using Microsoft RRAS/NPS as

your VPN server, repeat the steps for localhost testing but launch NTRadPing on your RRAS server and follow steps a and b below:

a.Change the NTRadPing IP address to point to your ESA RADIUS server.

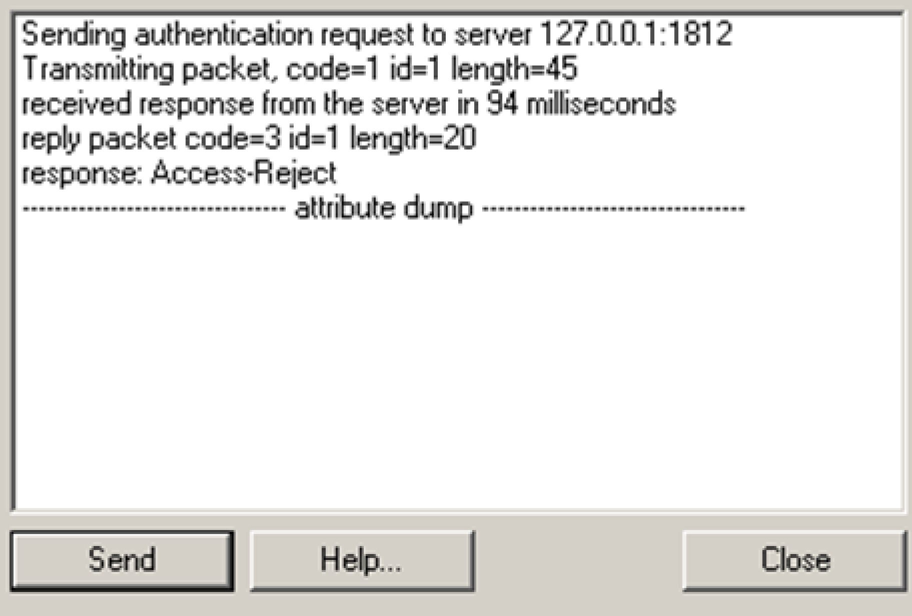
b.Change the IP address of your **Dummy Client** to match your RRAS server.

2. If you are using a dedicated VPN appliance, perform the steps detailed above using another machine on the same network segment as your VPN appliance.

I received an Access-Reject

Symptom

You receive the following response:



```
Sending authentication request to server 127.0.0.1:1812
Transmitting packet, code=1 id=1 length=45
received response from the server in 94 milliseconds
reply packet code=3 id=1 length=20
response: Access-Reject
--------------------------------- attribute dump ---------------------------------
```

Steps to resolve

Verify the following:

1. Ensure you have typed Alice’s password into the **Password** field correctly. Retry by clicking the **Send** button again.

2. Ensure that Alice’s AD password is indeed what you are typing in. Reset the password if necessary.

3. Verify that in the WEB Console, Alice does not have any 2FA methods enabled, ensure that Mobile Application and SMS OTPs are NOT selected.

4. Ensure that Alice is not locked out, and unlock the account if neccesary.

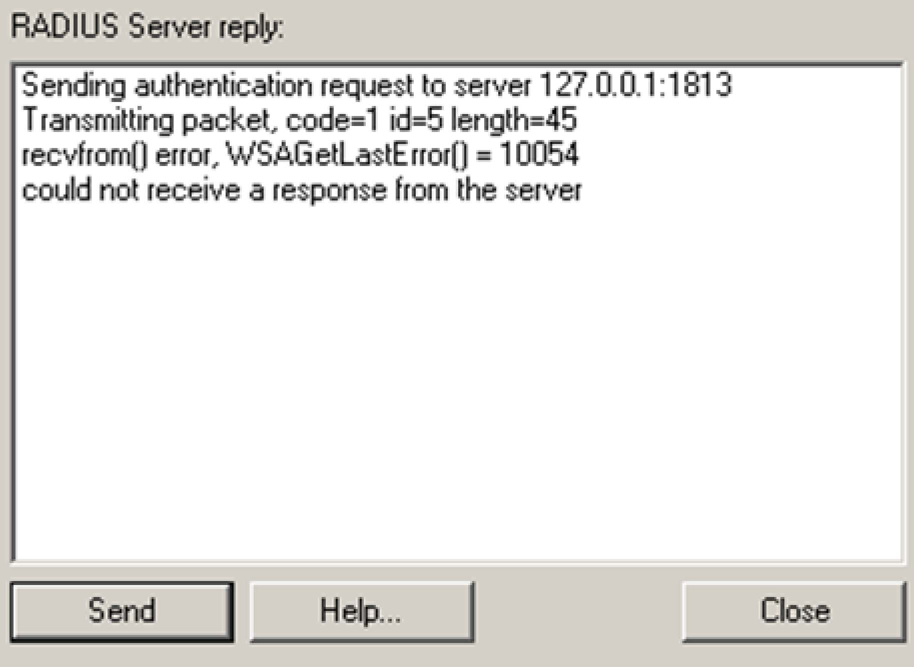
5. Double check your RADIUS configuration and your NTRadPing configuration.

6. If after completing the steps above you issue is still not resolved, contact ESET Customer Care and provide them with your RADIUS logfile, located in *C:\ProgramData\ESET Secure Authentication\logs*.

I received a connection error

Symptom

Instead of Access-Accept, you experience the following:



```
Sending authentication request to server 127.0.0.1:1813
Transmitting packet, code=1 id=5 length=45
recvfrom() error, WSAGetLastError() = 10054
could not receive a response from the server
```

Steps to resolve

1. Ensure that you have created the dummy RADIUS client with the correct IP address, as per the instructions in the section Configure your RADIUS Server. Verify that your ESA RADIUS Service is in the **Started** state.

2. Ensure that you have typed the correct details into NTRadPing, as per the screenshot in section Verify functionality (localhost).

3. Verify that your RADIUS server is listening on the correct port. Launch a command prompt and run the following command:

```
netstat –a –p UDP –b  C:\temp.txt
```

4. Open the file C:\temp.txt and verify that the following entries exist for your RADIUS server:

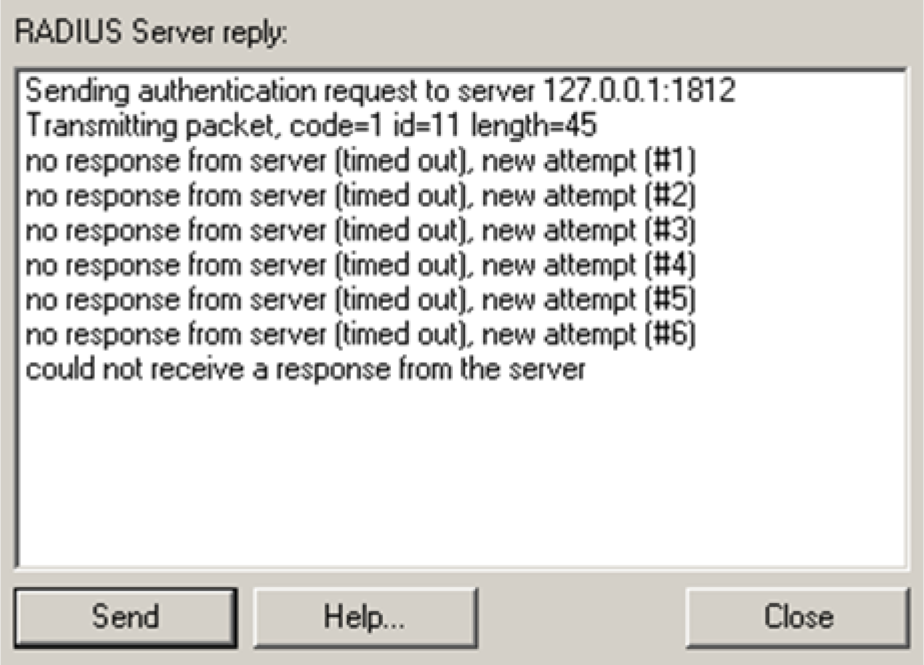
```
 Proto  Local Address                    Foreign Address                State

 UDP 0.0.0.0:1812                             *:*

[EIP.Radius.WindowsService.EXE]
```

5. If none of the above solve the issue, contact ESET Customer Care and provide them with your RADIUS logfile, located in *C:\ProgramData\ESET Secure Authentication\logs*.

I experienced timeouts

Symptom

Instead of Access-Accept, you receive the following:



RADIUS Server reply:

```
Sending authentication request to server 127.0.0.1:1812
Transmitting packet, code=1 id=11 length=45
no response from server (timed out), new attempt (#1)
no response from server (timed out), new attempt (#2)
no response from server (timed out), new attempt (#3)
no response from server (timed out), new attempt (#4)
no response from server (timed out), new attempt (#5)
no response from server (timed out), new attempt (#6)
could not receive a response from the server
```

Steps to resolve

1. Ensure that you have created the dummy RADIUS client with the correct IP address, as per the instructions in the section Configure your RADIUS Server.

2. Ensure that you have typed the correct details into NTRadPing, as per the screenshot in section Verify functionality (localhost).

3. Verify that your RADIUS server is listening on the correct port. Launch a command prompt and run the following command:

```
netstat –a –p UDP –b  C:\temp.txt
```

4. Open the file C:\temp.txt and verify that there is an entry for your RADIUS server which looks like this:

```
Proto  Local Address                    Foreign Address                State

UDP 0.0.0.0:1812                            *:*

[EIP.Radius.WindowsService.EXE]
```

5. If after performing the steps above your issue is still not resolved, contact ESET Customer Care and provide them with your RADIUS logfile, located in *C:\ProgramData\ESET Secure Authentication\logs*.

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.

> Important
>
> First, configure the Linux/Mac RADIUS client in ESA Web Console. Type the IP address of your Linux/Mac computer in the **IP Address** field. Select **Client does not validate user name and password - use Access-Challenge** from the **Client Type** drop-down menu.

When you complete these steps, configure your Linux or Mac computer based on the instructions in the following sub-chapters.

Create ESA RADIUS clients via API

If you have integrated ESA protection for many Linux/Mac desktop logins via PAM modules, and you need to configure many RADIUS clients in ESA, the following PowerShell script will ease your work.

Prerequisites

1. Configure a RADIUS client in ESA Web Console.

   - **Basic Settings** > **IP address**: Type in the IP address of the computer hosting the PAM module by which the ESA RADIUS server can reach it

   - **Basic Settings** > **Shared Secret**: Type in the same shared secret as you set in your VPN appliance

   - **Authentication** > **Client Type** > **Client validates user name and password - use Access-Challenge**

2. Enable ESA API and add API credentials for **Management API** in ESA Web Console.

3. List the IP address and **Shared Secret** of each VPN appliance in a `.csv` file as `<IP address>;<Shared Secret>` pairs.

For example:

```
192.168.0.11;test1

192.168.0.12;test2

192.168.0.13;test3
```

If executing the script on a different machine then the one hosting the Authentication Server:

1. Make sure ESA certificate is trusted on that computer.

2. Make sure the certificate includes the FQDN of the Authentication Server in the list of alternative DNS names.

How does the script work?

The script reads each row of the `.csv` file and creates as many RADIUS clients as many rows of IP address and Shared Secret pairs are found. The **Authentication** section of each RADIUS client will be configured based on the pre-configured RADIUS client.

Sample PowerShell script to create new ESA RADIUS clients via ESA API - we name the file create_radius_clients.ps1

```
# configuration


# Management API credentials - username:password

$credentials = "kjssgmarkm:dapweburnx"


# IP address or FQDN of the Authentication Server

$esaAuthenticationServer = "127.0.0.1:8001"


# Name of ESA RADIUS Server foudn in ESA Web Console at Componets > RADIUS

$radiusServerName = "BTSH00049D (Authentication Server computer)"


# Name of the pre-configured ESA RADIUS client

$baseRadiusClientName = "Base Client"


# List of IP Address and Shared Secret of each VPN appliance is saved in the clients
.csv file.

# The clients.csv file is in the same directory where the this PowerShell script res
ides
```

```
$csvImportFilePath = $PSScriptRoot + "\\clients.csv"

# headers preparation

$ErrorActionPreference = "Stop"

$encodedCredentials = [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($credentials))
$basicAuthHeader = "Basic $encodedCredentials"
$headers = @{Authorization = $basicAuthHeader}

# find RADIUS server

$body = @{
  componentType = "radius"
}
$bodyStr = $body | ConvertTo-Json
$response = Invoke-WebRequest -Uri https://$esaAuthenticationServer/manage/v2/GetComponentSettings -Method POST -Body $bodyStr -ContentType "application/json" -Headers $headers

$components = $response.Content | ConvertFrom-Json

$radiusServerKey = $null
foreach ($component in $components)
{
  if ($component.Info.Name -ceq $radiusServerName) {
    $radiusServerKey = $component.Info.Key
  }
}

if ($radiusServerKey -ceq $null) {
  Throw "RADIUS server not found: " + $radiusServerName

}


# base RADIUS client


$body = @{

  componentKey = $radiusServerKey

}

$bodyStr = $body | ConvertTo-Json

$response = Invoke-WebRequest -
Uri https://$esaAuthenticationServer/manage/v2/GetRadiusClients -Method POST -Body $
bodyStr -ContentType "application/json" -Headers $headers


$clients = $response.Content | ConvertFrom-Json


$baseRadiusClientSettings = $null

foreach ($client in $clients)

{

  if ($client.ClientName -ceq $baseRadiusClientName) {

    $baseRadiusClientSettings = $client

  }

}


if ($baseRadiusClientSettings -ceq $null) {

    Throw "RADIUS client not found: " + $baseRadiusClientName

}


# create clients


foreach($line in [System.IO.File]::ReadLines($csvImportFilePath))

{

  $fields = $line.Split(';')
  if ($fields.Count -cne 2) {
    Throw "Invalid fields count: " + $line
  }

  $ip = $fields[0]
  $sharedSecret = $fields[1]

  $newClientSettings = $baseRadiusClientSettings | ConvertTo-Json | ConvertFrom-Json
  $newClientSettings.Id = [guid]::NewGuid().ToString("d")
  $newClientSettings.ClientName = "Generated - " + $ip
  $newClientSettings.ClientIp = $ip
  $newClientSettings.SharedSecret = $sharedSecret

  $body = @{
    componentKey = $radiusServerKey;
    client = $newClientSettings
  }
  $bodyStr = $body | ConvertTo-Json
  $response = Invoke-WebRequest -
Uri https://$esaAuthenticationServer/manage/v2/CreateRadiusClient -Method POST -Body
 $bodyStr -ContentType "application/json" -Headers $headers
}

echo "success"
```

PAM configuration

Configure a custom realm

1. Create a custom realm for users logging in through a PAM module.

2. When configuring the RADIUS client, select the custom realm in the **Users** section.

i

Custom realm versus Current AD domain

If a custom realm is selected and the PAM module sends "domain\username" to the ESA RADIUS server, then a user with the username "domain\username" is created in the custom realm.
If you select **Current AD domain** or **Current AD domain and domains in trust** instead of a custom realm and the PAM module sends "domain\username" to the ESA RADIUS server, a user with the username "username" will be created in the "domain" realm.

PAM Authentication Module

1. Download PAM RADIUS tar.gz from https://freeradius.org/sub_projects/

2. Extract the downloaded package by executing the following command in a terminal window:

```
tar xzvf pam_radius-release_2_0_0.tar.gz
```

3. Build the .so library by executing the following commands in a terminal window:

```
cd pam_radius-release_2_0_0
./configure
make
```

On Linux, for example OpenSuse, depending on the output of the `configure` command, dependencies might have to be installed.

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

4. Copy the built library to the default location of PAM modules

Linux:
```
cp pam_radius_auth.so /lib/security
```
or
```
cp pam_radius_auth.so /lib64/security
```

Mac:
```
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.

5. Create a server configuration file named *server* at */etc/raddb/.* In it, type 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 60

where:

- `1.1.1.1` represents the IP address of ESA RADIUS server

- `test` is the shared secret of a RADIUS client configured in ESA Web Console

- `60` is the time in seconds how long to wait for the approval of push notification

6. Apply appropriate security permissions to the configuration file

```
chown root /etc/raddb

chown root /etc/raddb/server

chmod 600 /etc/raddb

chmod 600 /etc/raddb/server
```

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/* .

- **sshd** - Remote login using SSH

> Make sure to set **ChallengeResponseAuthentication** to **yes** in */etc/ssh/sshd_config*.

- **sudo**
- **su**
- **common-auth** - OpenSUSE (all authentications)
- **login** - OpenSUSE (console login)
- **authorization** - macOS logon screen

To enable two-factor authentication for any of the services above, add the following line to the corresponding configuration file in */etc/pam.d*:

```
auth required pam_radius_auth.so use_first_pass
```

In the command above, `pam_radius_auth.so` represents the path to an earlier configured PAM module, or it will be "*pam_radius_auth.so*". `use_first_pass` ensures the PAM module does not require an additional password (OTP) in vain, unless ESA RADIUS requires the second factor. For example, if a user with 2FA protection has Push Authentication enabled, then the PAM module waits only for the approval of the Push notification without requesting to type an OTP.

To ensure 2FA is not requested when the first factor failed, change `auth required pam_unix.so` to `auth requisite pam_unix.so`.

Some login interfaces, including the macOS login screen, cannot display a separate field for 2FA. In such cases, only users using Push authentication (Mobile application push), or Non-2FA users or users from a whitelisted IP address can log in. To ensure that only the Mobile application push is used without prompting for OTP even if the user had additional 2FA options enabled, add `client_id=challenge_never` to the configuration line:

```
auth required pam_radius_auth.so use_first_pass client_id=challenge_never
```

Available values for `client_id`:

- `challenge_if_possible` - The default option always prompts for OTP if the user has any OTP type enabled, even if sending "Mobile application push" succeeded.
- `challenge_always` - Always prompt for OTP, even if sending "Mobile application push" succeeded and the user does not have any type of OTP enabled. It always allows you to type in MRK if something goes wrong. (this is recommended for critical scenarios, for example, SSH login to a remote server that cannot be easily accessed otherwise)
- `challenge_if_needed` - Never prompt for OTP if sending "Mobile application push" succeeded", thus avoiding additional OTP request/field and allowing faster login.
- `challenge_never` - Never prompt for OTP.

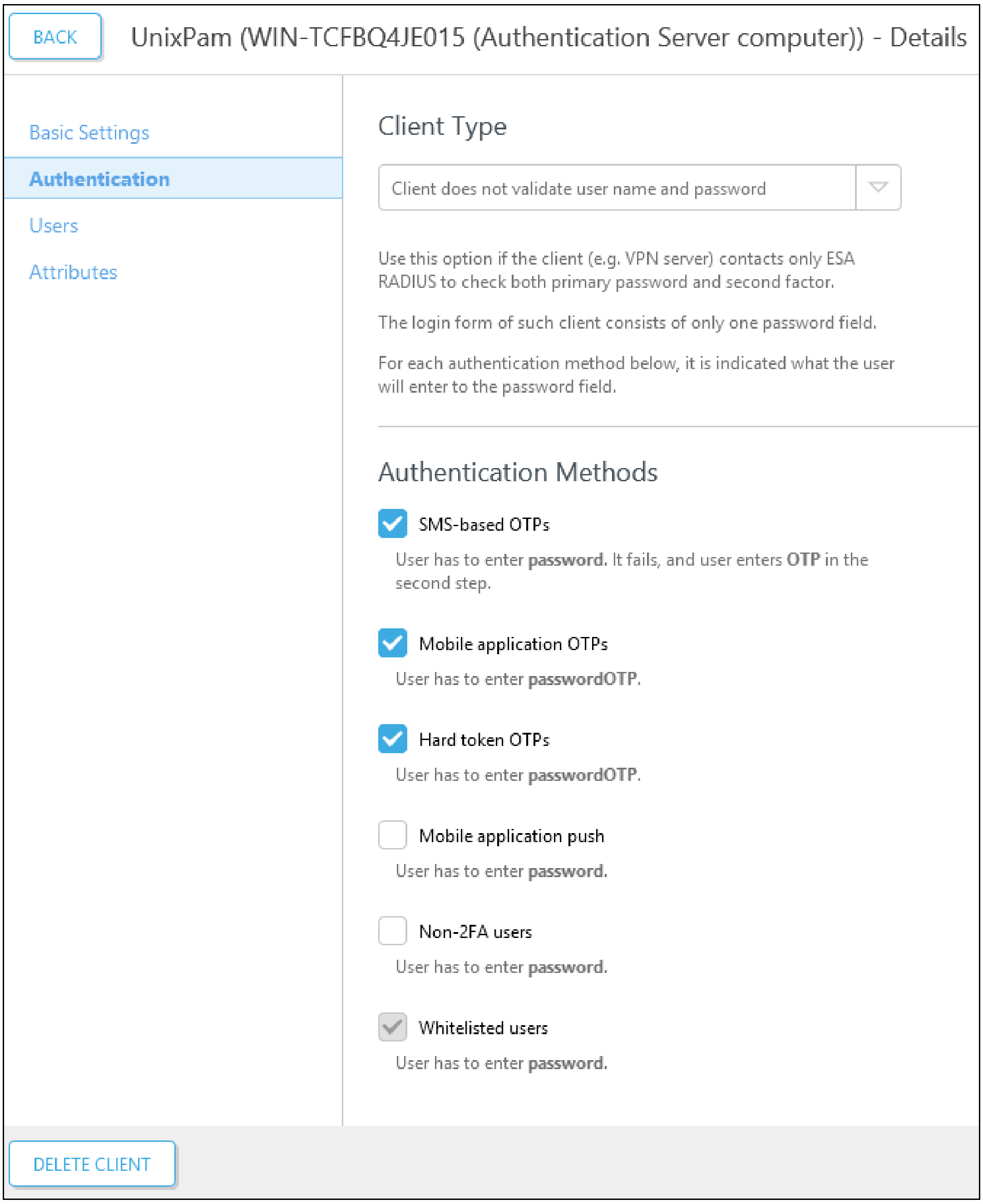
On some Linux distributions it is easily possible to change the login manager. For example, gdm supports prompting for additional information.

Other RADIUS configurations

In the examples below we used an Active Directory domain environment.

Client Type - Client does not validate username and password

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


BACK
UnixPam (WIN-TCFBQ4JE015 (Authentication Server computer)) - Details
Basic Settings
Authentication
Users
Attributes
DELETE CLIENT

Client Type

Client does not validate user name and password

Use this option if the client (e.g. VPN server) contacts only ESA RADIUS to check both primary password and second factor.

The login form of such client consists of only one password field.

For each authentication method below, it is indicated what the user will enter to the password field.

Authentication Methods

☑ SMS-based OTPs

User has to enter **password**. It fails, and user enters **OTP** in the second step.

☑ Mobile application OTPs

User has to enter **passwordOTP**.

☑ Hard token OTPs

User has to enter **passwordOTP**.

□ Mobile application push

User has to enter **password**.

□ Non-2FA users

User has to enter **password**.

☑ Whitelisted users

User has to enter **password**.

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

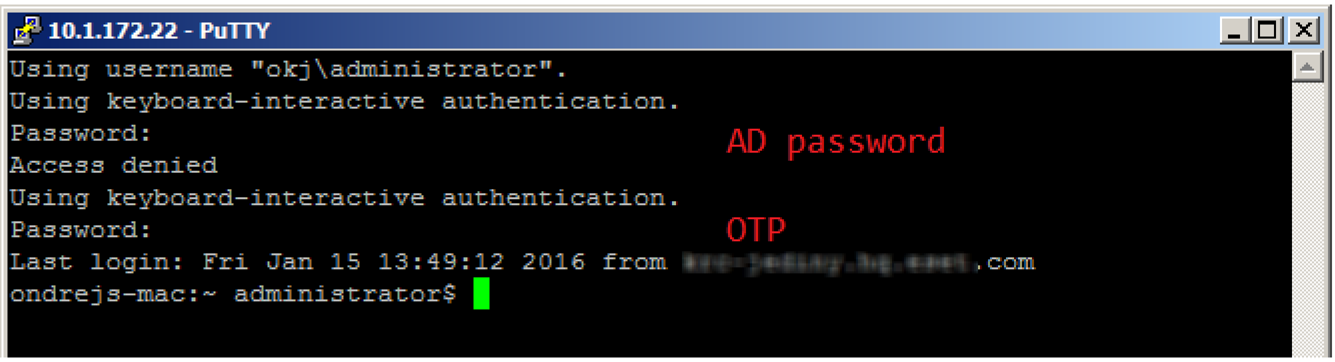
```
auth required /usr/lib/pam/pam_radius_auth.so
```

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

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

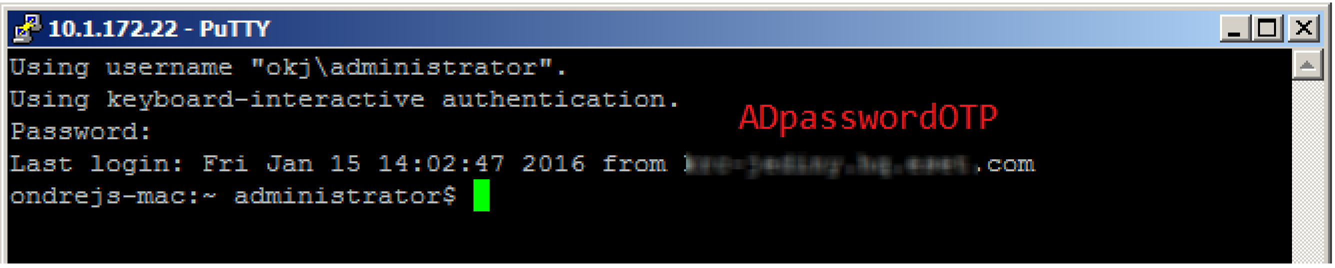
In this case a SSH login process would look like this:

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



```
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Last login: Fri Jan 15 13:49:12 2016 from [redacted].com
ondrejs-mac:~ administrator$
```

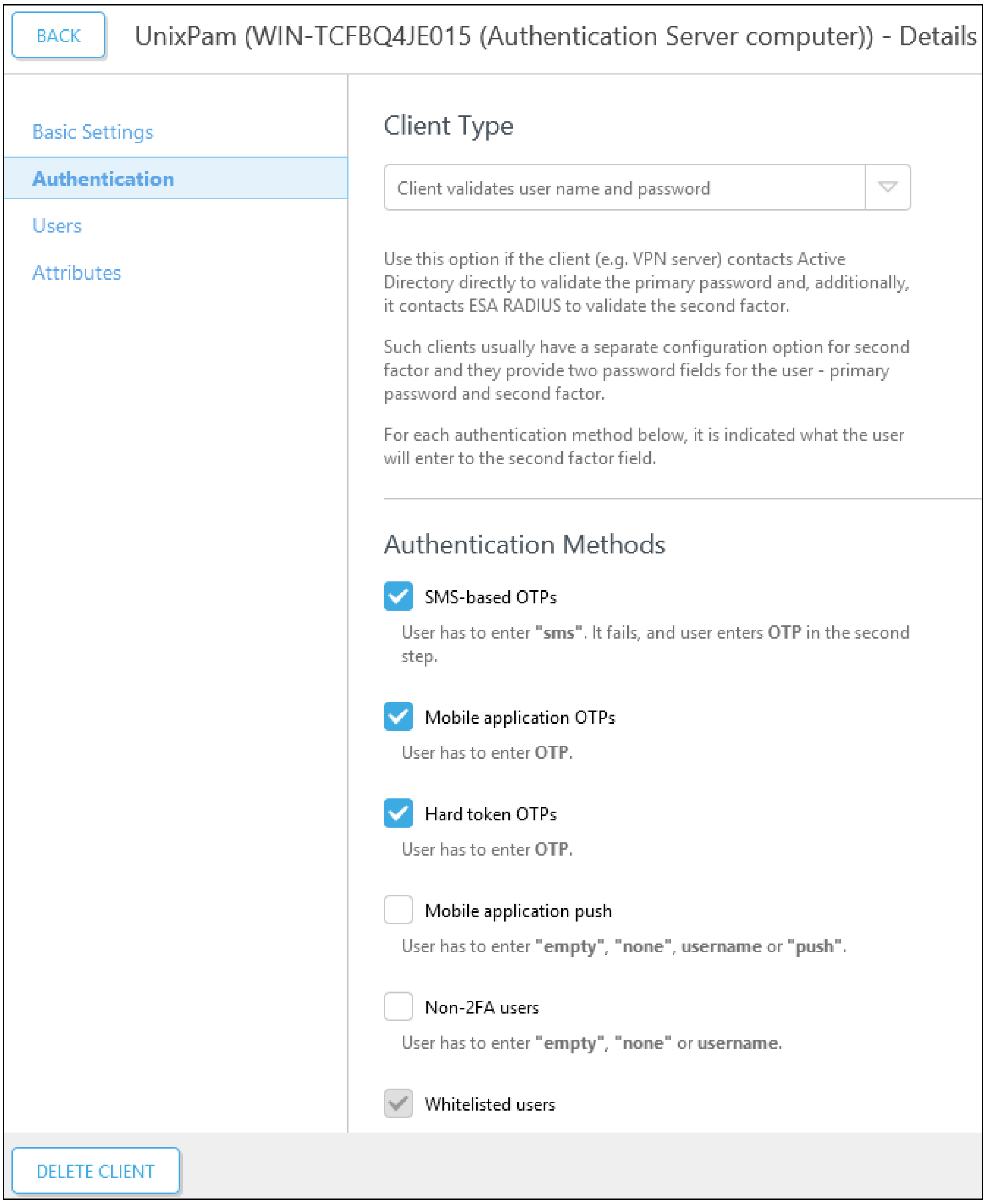
- Other type of OTP (compound authentication) - the user must type both the AD password and OTP at the same time as ADpasswordOTP. For example if your AD password is Test and the received OTP is 123456, you would type Test123456.



```
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password:
Last login: Fri Jan 15 14:02:47 2016 from [redacted].com
ondrejs-mac:~ administrator$
```

Client Type - Client validates username and password

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



UnixPam (WIN-TCFBQ4JE015 (Authentication Server computer)) - Details

Client Type

Client validates user name and password

Use this option if the client (e.g. VPN server) contacts Active Directory directly to validate the primary password and, additionally, it contacts ESA RADIUS to validate the second factor.

Such clients usually have a separate configuration option for second factor and they provide two password fields for the user - primary password and second factor.

For each authentication method below, it is indicated what the user will enter to the second factor field.

Authentication Methods

☑ SMS-based OTPs

User has to enter **"sms"**. It fails, and user enters **OTP** in the second step.

☑ Mobile application OTPs

User has to enter **OTP**.

☑ Hard token OTPs

User has to enter **OTP**.

☐ Mobile application push

User has to enter **"empty"**, **"none"**, **username** or **"push"**.

☐ Non-2FA users

User has to enter **"empty"**, **"none"** or **username**.

☑ Whitelisted users

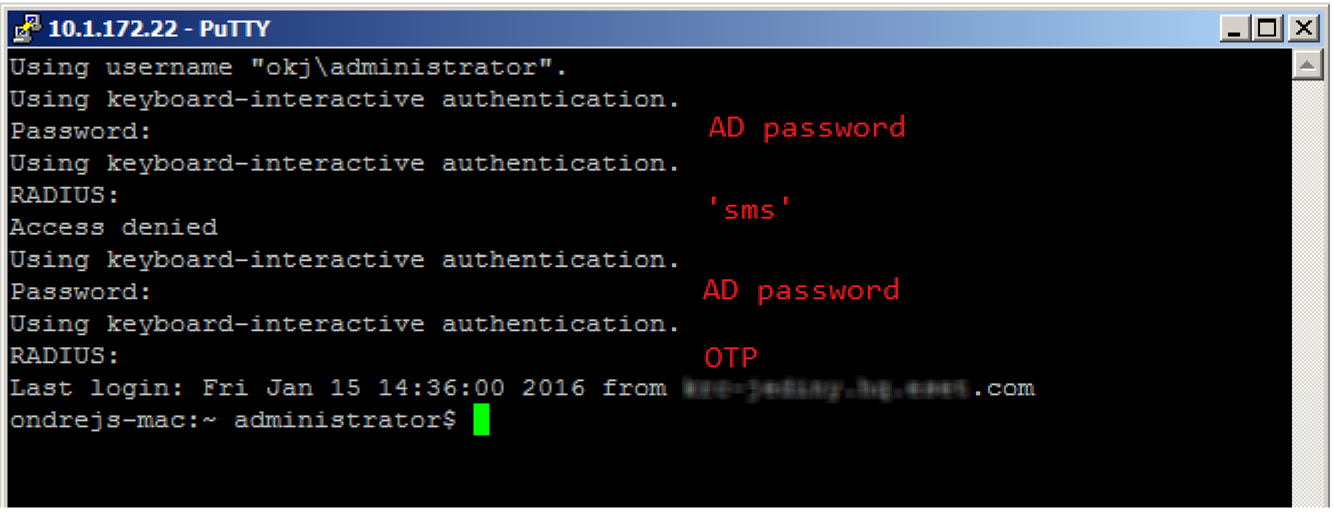
When configuring RADIUS in this manner, add the following line in **/etc/pam.d/sshd** (or the appropriate integration):

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

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

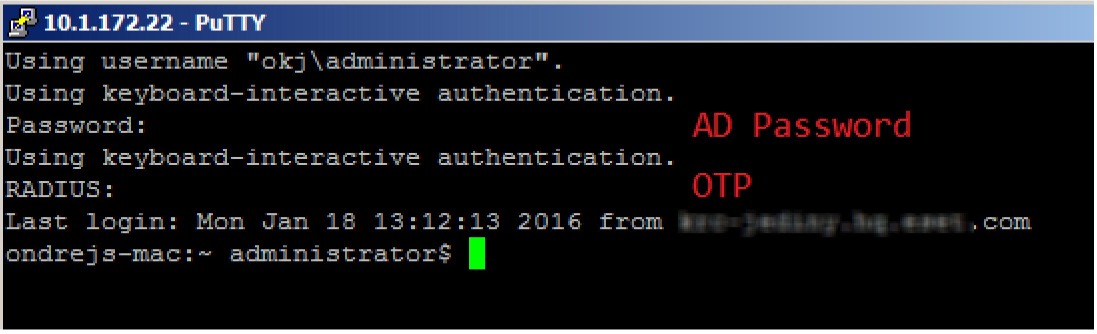
- prompts that start with the string **Password:** are handled by other PAM modules. Prompts that begin with the string **RADIUS:** are handled by our PAM module. See the argument '**prompt=RADIUS**' in the sample code above

- SMS - at the first prompt, a user must type their AD password. At the second prompt, they must type the text '**sms**' (without apostrophes). At the third prompt, they must type their AD password. At the fourth prompt, they must type the received OTP



```
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
RADIUS:
Access denied
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
RADIUS:
Last login: Fri Jan 15 14:36:00 2016 from [redacted].com
ondrejs-mac:~ administrator$
```

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



```
Using username "okj\administrator".
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
RADIUS:
Last login: Mon Jan 18 13:12:13 2016 from [redacted].com
ondrejs-mac:~ administrator$
```

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 or prompted to authenticate using FIDO. The user will only be allowed access to the Web Application if a valid OTP is typed or the push notification is approved or FIDO authentication is successful.

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

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 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 not configured for any authentication method 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.

Multiple OWA/ECP instances handled as one

Suppose you have multiple OWA/ECP instances for the same Microsoft Exchange installation.

By default, if a 2FA-enabled user logs in and authenticates using 2FA to one instance, when logging in to another instance, the user is required to use 2FA again.

To prevent requiring 2FA when logging in to the other instance:

1. In ESA Web Console, click **Components** > **Outlook Web App** or **Exchange Control Panel**.
2. Click the three dots icon next to an OWA/ECP instance and select **Change Solution**.
3. In the **Solution Identifier**, type a memorable string.
4. Click **Save**.
5. Repeat steps 2–4 for each corresponding instance.
6. Restart the components by restarting Internet Information Services (IIS):
    1. Click **Start**.
    2. In the search box, type `cmd`.
    3. In the results, right-click **Command Prompt** and select **Run as administrator**.
    4. At the command prompt, type `iisreset`, and press **Enter**.
    5. When "Internet services successfully restarted" displays, exit the command prompt.

Usage

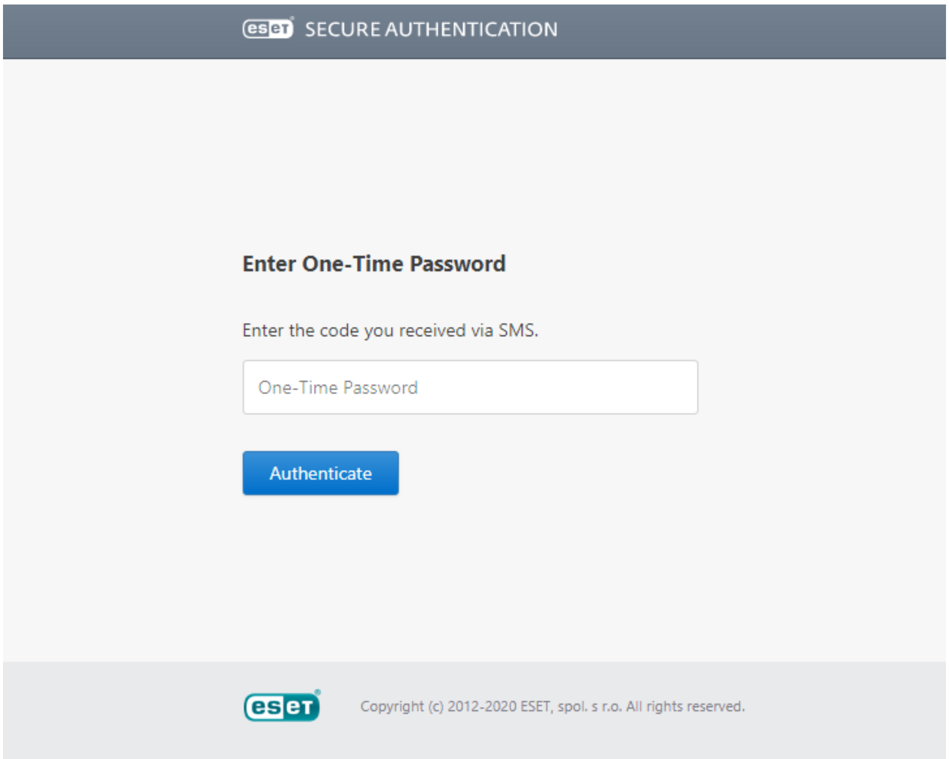
The same 2FA process is followed for all supported Web Apps.

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

1. A user that has ESA 2FA enabled in the ESA Web Console 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 using the Active Directory credentials of the test user.

3. The ESA authentication page should now appear, as per the figure below.



eset SECURE AUTHENTICATION
Enter One-Time Password
Enter the code you received via SMS.
One-Time Password
Authenticate
eset
Copyright (c) 2012-2020 ESET, spol. s r.o. All rights reserved.

a.If the user is enabled for SMS OTPs, an SMS will be sent containing an OTP that may be typed 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 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.

4. If a push notification is approved or a valid OTP is typed or FIDO is used to authenticate, the user will be redirected to the page they originally requested. The user will then be able to interact with the Web App.

5. 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 typed, then an error message will be displayed and the user will not be allowed access to the web application.

Custom logo

If you want a custom logo to be displayed on the screen waiting to type 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, AD FS protection, Identity Provider Connector) 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*".

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 where the Remote Desktop plugin of ESA has been installed.

Users will log in using the standard authentication process of Remote Desktop. After being authenticated by Remote Desktop, users will be prompted for an OTP or prompted to approve the push notification or prompted to authenticate using FIDO. Users will only be allowed access to their computer if a valid OTP is typed or the push notification is approved, or FIDO authentication is successful.

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

RDP client without username and password

ESA cannot protect RDP clients that do not provide username and password; if an RDP client does not have the username and password configured and it does not request a username and password, then no OTP is going to be requested either.

Configuration

To configure Remote Desktop 2FA for the desired user(s), enable 2FA in their profile(s). They also must be authorized Remote Desktop users.

To use Remote Desktop protection, RD Session Host must be configured to use an available *SSL (TLS)* option or *Negotiate*. Usually, the Security Layer is configured correctly. If you run into issues, check and adjust the settings as described below.

RDP without Remote Desktop Services

Use Group Policy to adjust the settings. For example, to modify the Local Computer Policy:

1. Press the **Windows key** ⊞ and **R** simultaneously.

2. Type `gpedit.msc` and press **Enter**.

3. In the left pane, click **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Security**.

4. In the right pane, double-click **Require use of specific security layer for remote (RDP) connections**.

5. Select **Enabled**.

6. From **Security Layer**, select an available SSL (TLS) option or *Negotiate*.

RDP using RD Services

To modify the settings on Windows Server 2008:

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 configured to use an available SSL (TLS) option or **Negotiate**.

To modify the settings on Windows Server 2012 and later, 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 configured to use an available SSL (TLS) option or **Negotiate**.

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 not configured for any authentication method 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 **Components**, click **RDP** and the **Computer list** window will appear listing all computers where Remote Desktop Protection of ESA is installed.

Usage

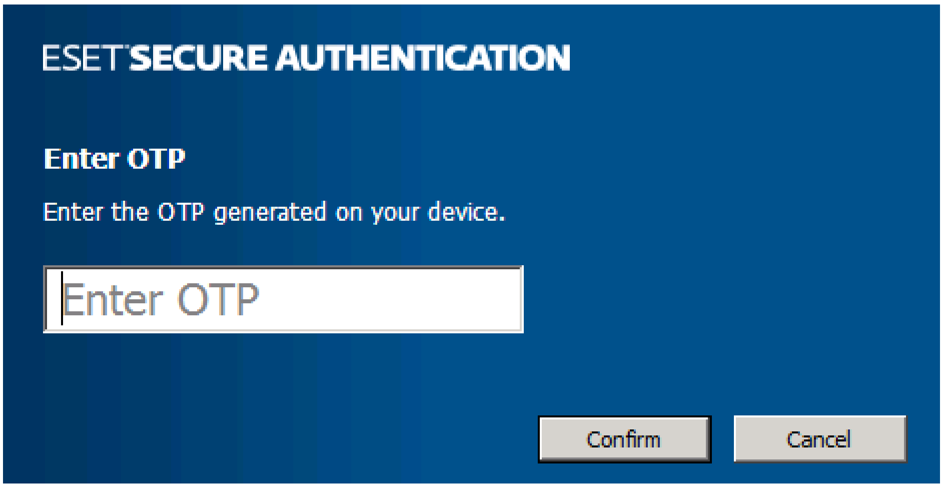
The operation of the Remote Desktop Protection module can be verified as follows:

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 using the login credentials of the test user.

2. The OTP prompt screen should now appear, as per the figure below.



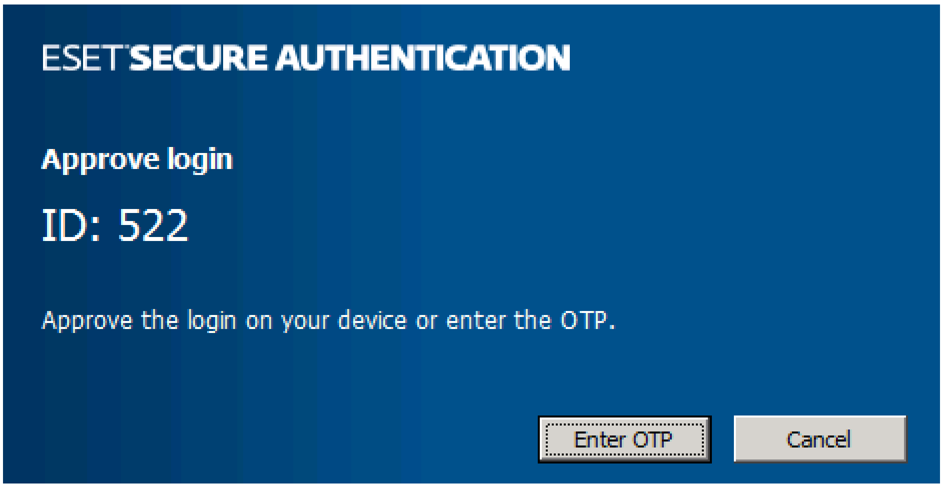
Enter OTP

Enter the OTP generated on your device.

a.If the user is enabled for SMS OTPs, an SMS will be sent containing an OTP that may be typed 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 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**.



Approve login

ID: 522

Approve the login on your device or enter the OTP.

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

4. If an invalid OTP is typed, then an error message will be displayed, and the user will not be allowed access to the remote computer.

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. After 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 access 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. Type the localhost IP address: 127.0.0.1,::1 in the text box.

4. Select the check-box next to **RDP**.

5. Click **Save**

> RDWA and ESA Authentication Server on different hosts
>
> 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 *EsaCore.log* log file located at *C:\ProgramData\ESET Secure Authentication\EsaCore.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.

Remote Desktop Web Access HTML5

There are currently two ways to access the HTML5 version of Remote Desktop Web Access (RD Web Access).

A user with **SMS OTPs** or **Mobile Application OTP** enabled:

1. Log in to the classic RD Web Access (`hostname.domain/rdweb`) while authenticating with an OTP.

2. In the same browser, log in to the HTML5 version of RD Web Access (`hostname.domain/rdweb/webclient`).

A user who has **Mobile Application Push** enabled can directly access the HTML5 version of RD Web Access. Approve the push notification when prompted to authenticate.

Remote Desktop Gateway and ESA RADIUS

A Remote Desktop Gateway Server enables users to connect to remote computers on a corporate network from any external computer.

Use ESA RADIUS to secure the authentication through Remote Desktop Gateway (RD Gateway) with a second factor - approval of push notification.

Prerequisites

- Authentication Server and RADIUS installed
- Functional Remote Desktop Gateway (RD Gateway)

Integration of ESA RADIUS with RD Gateway

The integration consists of two parts, RD Gateway configuration and ESA configuration.

RD Gateway configuration - Use NPS (recommended)

1. Open the **Remote Desktop Manager Gateway** application.

    a.In the navigation tree, right-click the computer name and click **Properties**.

    b.Click **RD CAP Store** and select **Central server running NPS**.

    c.Type the IP address of the NPS server, click **Add** > **OK**.

2. Open the **Network Policy Server** application.

    a.In the navigation tree, expand **RADIUS Clients and Servers**, right-click **Remote RADIUS Server Groups** > **New**.

    b.Define the desired **Group name**.

    c.Click **Add**.

        i. In the **Address** tab, type the IP address of ESA RADIUS in the **Server** field.

        ii. In the **Authentication/Accounting** tab:

            A.Leave the default value of 1812 in the **Authentication port** field.

            B.Define a desired **Shared secret**, type it also to **Confirm shared secret**.

            C.Select the check box next to **Request must contain the message authenticator attribute**.

        iii. In the **Load balancing** tab, set a reasonably high number (e.g., 120) for both the **Number of seconds**

without response before request is considered dropped and **Number of seconds between requests when server is identified as unavailable** fields. This is to avoid NPS retrying the authentication while the push request is being handled (it can take some time).

iv. Click **OK**.

d.Click **OK**.

e.In the navigation tree, expand **Policies**, select **Connection Request Policies**, double-click **TS GATEWAY AUTHORIZATION POLICY**.

i. In the **Settings** tab, select **Authentication** > **Forward requests to the following remote RADIUS server group for authentication**, select the ESA group created in the previous steps.

ii. Click **OK**.

RD Gateway configuration - Direct integration (not recommended)

When this type of integration is applied, there can be a problem with a very short RADIUS communication timeout. Meaning, more push notifications would be received for the same authentication request.

1. Open **Remote Desktop Manager Gateway** application.

2. In the navigation tree, right-click the computer name, click **Properties**.

3. Click **RD CAP Store**, select **Central server running NPS**.

4. Type the ESA RADIUS IP address, which is the IP address of the host computer where the ESA RADIUS component is installed, including the port number. Click **Add**.

5. Define a desired **Shared secret**, click **OK**.

6. Click **OK**.

ESA Configuration

1. Log in to the ESA Web Console.

2. Navigate to **Components** > **RADIUS**, click the RADIUS server you use.

3. Click **Create new RADIUS client**.

4. Type a desired **Name**.

5. Type the **IP address** of the the client (NSP or RD Gateway depending on the chosen integration method) as the RADIUS server sees it.

a.The IP address of the client can be found in: *C:\ProgramData\ESET Secure Authentication\logs\Radius.log*

b.Search for the following string in that log file: "Invalid Auth. packet received from : `<IP address>`:`<port>`"
The `<IP address>` and `<port>` will represent the real IP address and port number.

6. In the **Shared secret** field, type the same shared secret you configured in the Remote Desktop Manager Gateway.

7. In the **Client Type** drop-down menu, select **Client validates user name and password**.

8. Select the check box next to **Mobile Application Push**.

9. For **Realm**, select **Current AD domain** or **Current AD domain and domains in trust**.

> **Non-2FA users**
>
> If you want to allow users not configured for any 2FA type to be able to log in, select **Non-2FA users** too.

10. Click **Save**.

How it works

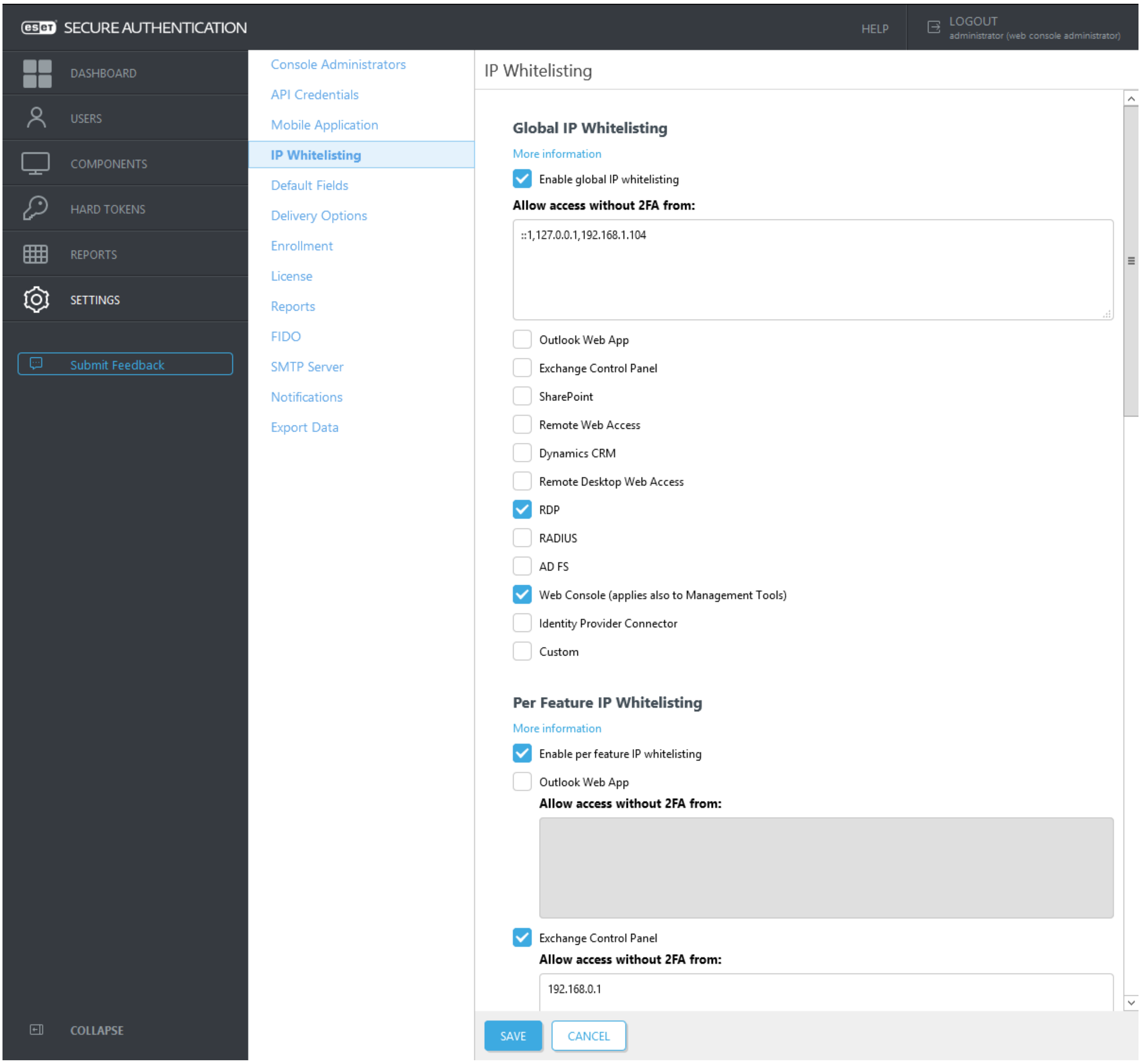
1. The user types their domain login credentials (first factor) in the RD Gateway log in dialog.

2. The user receives and approves the push notification (second factor) on their mobile phone.

3. In the subsequent log in dialog, the user types their login credentials for the target computer.

IP address whitelisting

If there are certain places, for example some branch offices, from where you want to grant access to Remote Desktop or Supported Web Applications secured by 2FA without the need to provide OTP, you can whitelist their IP addresses. To do so, open the ESA Web Console and navigate to **Settings** > **IP Whitelisting**.



IP Whitelisting

Global IP Whitelisting

More information

☑ Enable global IP whitelisting

Allow access without 2FA from:

::1,127.0.0.1,192.168.1.104

□ 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)
□ Identity Provider Connector
□ Custom

Per Feature IP Whitelisting

More information

☑ Enable per feature IP whitelisting

□ Outlook Web App

Allow access without 2FA from:

☑ Exchange Control Panel

Allow access without 2FA from:

192.168.0.1

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**.

Do not confuse Remote Web Access with Remote Desktop Web Access.

RADIUS

ESA RADIUS server reads the user's IP address from the first non-empty RADIUS attribute, namely:

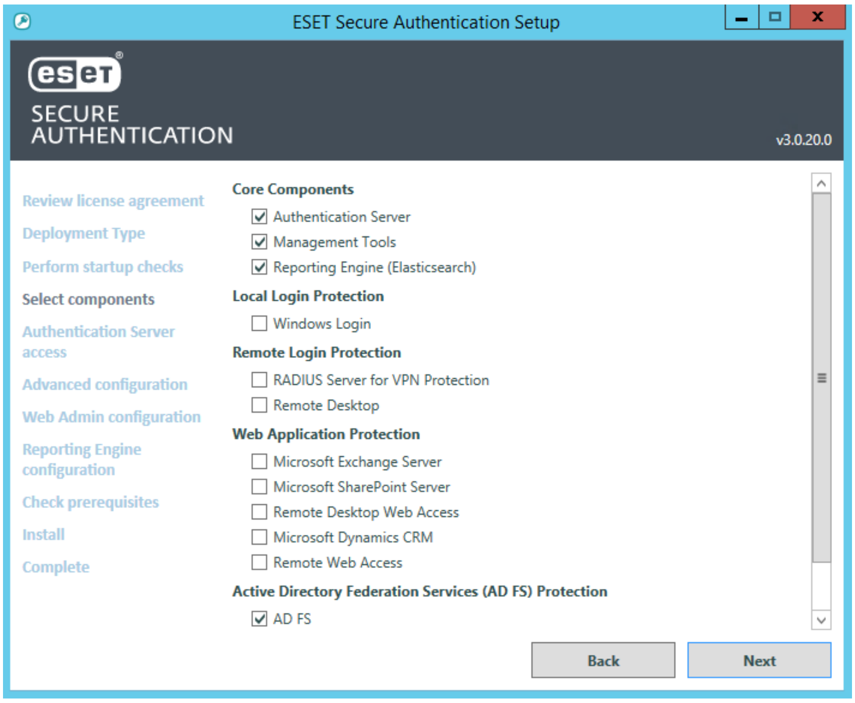
- `66 Tunnel-Client-Endpoint`
- `31 Calling-Station-Id`

The intent is to get the IP address read by the closest component; it is the VPN server in most cases.

AD FS

ESA is a great choice for security if you are using Active Directory Federation Services (AD FS) 3 or later 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.



Core Components

☑ Authentication Server
☑ Management Tools
☑ Reporting Engine (Elasticsearch)

Local Login Protection

□ Windows Login

Remote Login Protection

□ RADIUS Server for VPN Protection
□ Remote Desktop

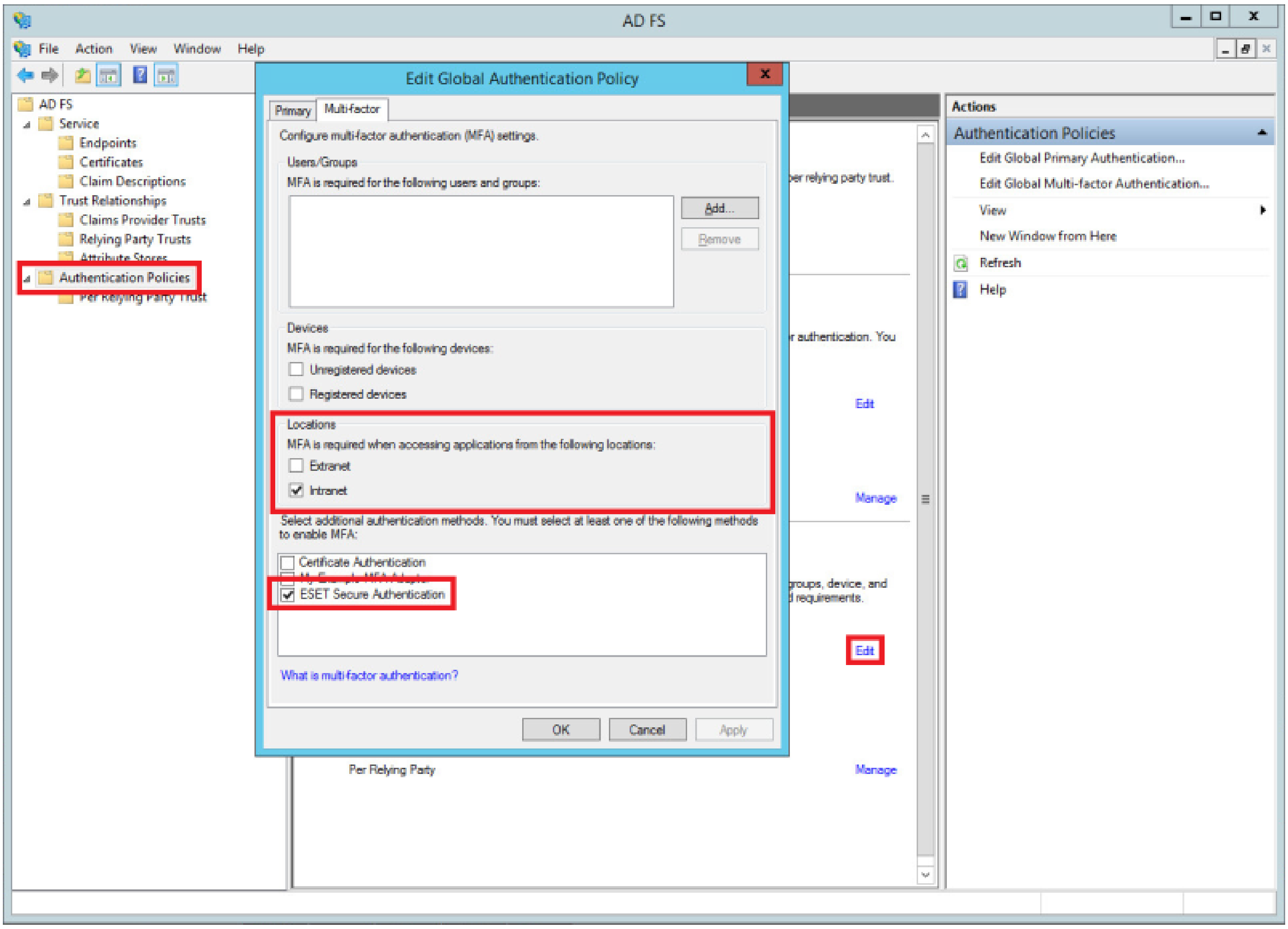
Web Application Protection

□ Microsoft Exchange Server
□ Microsoft SharePoint Server
□ Remote Desktop Web Access
□ Microsoft Dynamics CRM
□ Remote Web Access

Active Directory Federation Services (AD FS) Protection

☑ AD FS

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 before installation of the AD FS component of ESA.



Edit Global Authentication Policy

Primary | Multi-factor

Configure multi-factor authentication (MFA) settings.

Users/Groups

MFA is required for the following users and groups:

Add... Remove

Devices

MFA is required for the following devices:

☐ Unregistered devices

☐ Registered devices

Locations

MFA is required when accessing applications from the following locations:

☐ Extranet

☑ Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication

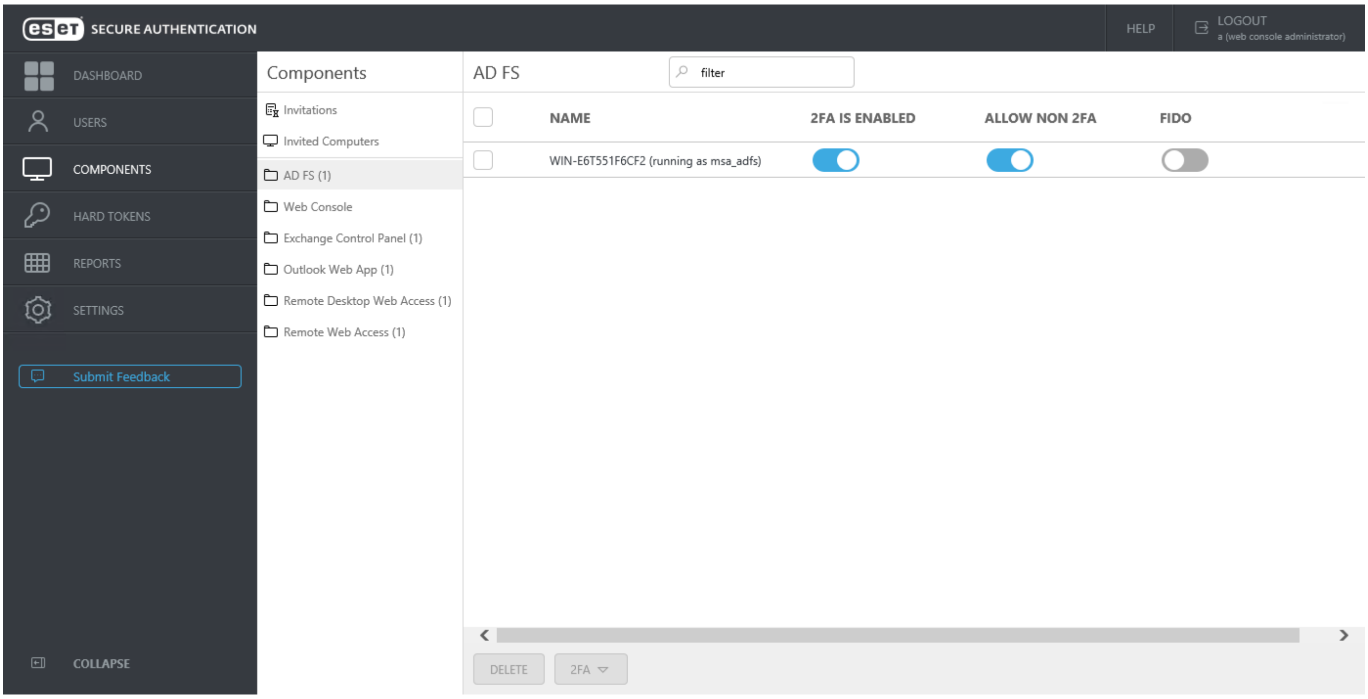
☐ My Example MFA Adapter

☑ ESET Secure Authentication

What is multi-factor authentication?

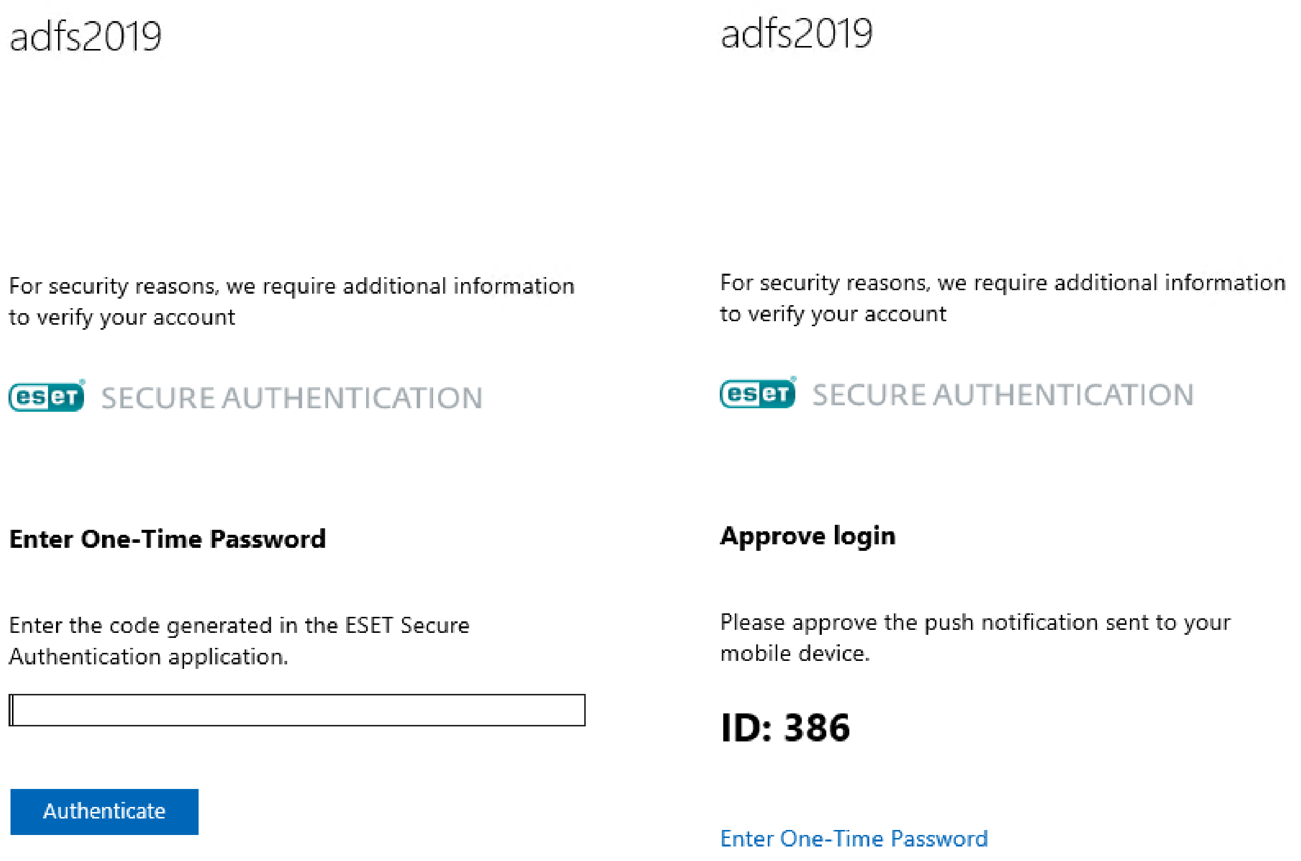
OK Cancel Apply

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



	NAME	2FA IS ENABLED	ALLOW NON 2FA	FIDO
□	WIN-E6T551F6CF2 (running as msa_adfs)	●	●	○

If a website requiring authentication verifies the identity against AD FS, and 2FA protection through ESA is applied to the specific AD FS, you will be prompted to type an OTP or approve the push notification or authenticate via FIDO after successful verification of identity:


adfs2019

For security reasons, we require additional information to verify your account

ESET SECURE AUTHENTICATION

Enter One-Time Password

Enter the code generated in the ESET Secure Authentication application.

Authenticate

adfs2019

For security reasons, we require additional information to verify your account

ESET SECURE AUTHENTICATION

Approve login

Please approve the push notification sent to your mobile device.

ID: 386

Enter One-Time Password

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

Custom logo

If you want a custom logo to be displayed on the screen waiting to type 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, AD FS protection, Identity Provider Connector) 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*".

Internet Explorer

Internet Explorer version 9 and 10 are supported web browsers.

AD FS Policies

ESA installer sets the following AD FS authentication rules:

```
c:[Type == "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value =
= "false"]

 => issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/authentica
tionmethod", Value = "http://schemas.microsoft.com/claims/multipleauthn");

c:[Type == "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value =
= "true"]

 => issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/authentica
tionmethod", Value = "http://schemas.microsoft.com/claims/multipleauthn");
```

The rules above automatically enable two-factor authentication (2FA) for both internal and external networks.

If you use a third-party AD FS app that does not work properly with 2FA, and you want to exclude specific users from using 2FA to access that app, then you must edit the AD FS policy.

1. Open Windows PowerShell and execute the following command. Then check the output of that command to verify that the only additional authentication rules are the ones listed at the beginning of this section.

```
Get-AdfsAdditionalAuthenticationRule
```

2. To remove additional authentication rules, execute the following command:

```
Set-AdfsAdditionalAuthenticationRule -AdditionalAuthenticationRules ' '
```

3. Open **AD FS Management**, click **Access Control Policies** > **Action** > **Add Access Control Policy**.

4. Add the following two Permit Users rules:

```
I.Permit Users
from esa_domain\ESA Users groups
and require multi-factor authentication

II.Permit Users
```

If the Authentication Server is installed in Active Directory Integration mode, the `esa_domain\ESA Users` group is automatically created during installation, while `esa_domain` is replaced with the domain name of the Authentication Server.

If the Authentication Server is installed in Standalone mode, you have to create a user group and assign ESA users to the group.

The two Permit Users rules above will ensure, that 2FA is required only for users belonging to the specified group. For all other users the 2FA authentication page is skipped.

5. Click **Relying Party Trusts**, assign the policy to the applicable relying party.

Custom ESA Service Account

To rename the ESET Secure Authentication Core Service Log On account in *Active Directory Integration* mode:

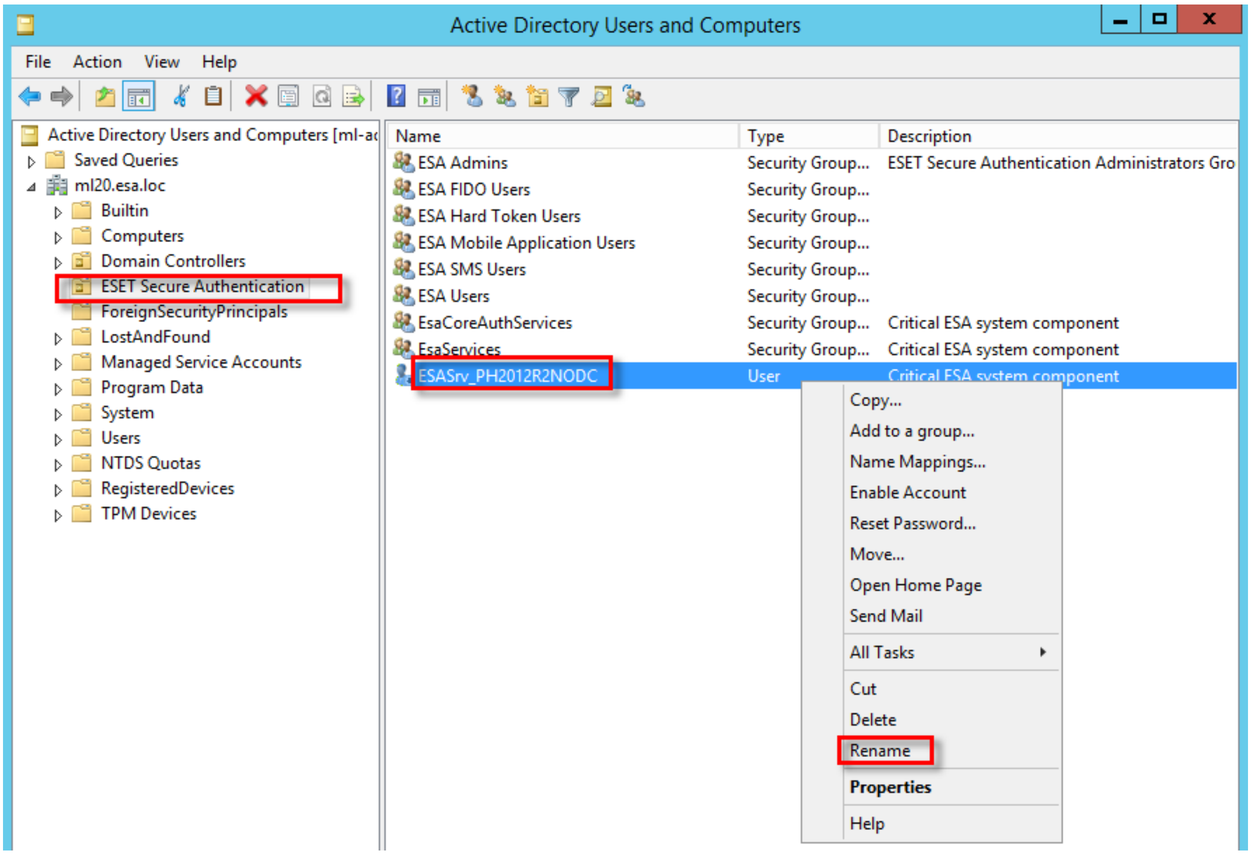
1. Open ADUC.

2. Navigate to **<your_active_directory_domain>** > **ESET Secure Authenitcation**.

3. Find the ESET Secure Authentication Core Service user, its name is made up of *ESASrv_* and the computer

name. For example, ESASrv_PH2012R2NODC.

4. Right-click the user, select **Rename**.



Name	Type	Description
ESA Admins	Security Group...	ESET Secure Authentication Administrators Gro
ESA FIDO Users	Security Group...	
ESA Hard Token Users	Security Group...	
ESA Mobile Application Users	Security Group...	
ESA SMS Users	Security Group...	
ESA Users	Security Group...	
EsaCoreAuthServices	Security Group...	Critical ESA system component
EsaServices	Security Group...	Critical ESA system component
ESASrv_PH2012R2NODC	User	Critical ESA system component

5. In the **Rename User** window define the desired name in the **Full name** and **User logon name** fields. Click **OK**.

6. Right-click the user, select **Reset Password**.

7. In the **New Password** window, type a temporary password. ESET Secure Authentication will change this password on the next run of the ESA installer (installation or upgrade of Authentication Server). Click **OK**.

8. Close ADUC.

9. To access Windows **Services**, press ⊞ + R, type *Services.msc* and press **Enter**.

10. Right-click "ESET Secure Authentication Core Service" service, select **Properties**.

11. In the **Log On** tab, select **This account**. Type the account name and the temporary password you defined, click **Apply** and then click **OK**.

12. Right-click "ESET Secure Authentication Core Service" service, select **Restart**.

Custom integration via API and SDK

ESET Secure Authentication provides native support for a variety of Microsoft Web Applications and Remote Access systems. For integration with custom systems, it provides a wide range of extensibility options allowing you to add two-factor authentication (2FA) to nearly any system that requires authentication.

There are two extension options: an Application Programming Interface (API) and a Software Development Kit (SDK). There are some key differences between the two products that will quickly help you decide which to use.

If you want to implement two-factor authentication in your product without installation of the Authentication Server, and you prefer to include essential libraries in your product environment and store user data in your product database, use the SDK.

Native Integrations

- RADIUS based systems such as VPN/UTM appliances, Citrix® XenApp™, VMWare® Horizon View™, etc. See more examples
- Microsoft Outlook Web App
- Microsoft SharePoint
- Microsoft Dynamics CRM
- Microsoft Remote Desktop Web Access
- AD FS

For further information on adding 2FA to systems not listed above, see the API and SDK chapters below.

API

The ESA API is a REST-like 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://127.0.0.1:8001`/, the API documentation is available at `https://127.0.0.1:8001/apidoc`.

What is new in API for ESET Secure Authentication 2.8 and later

- 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

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.

Configuration

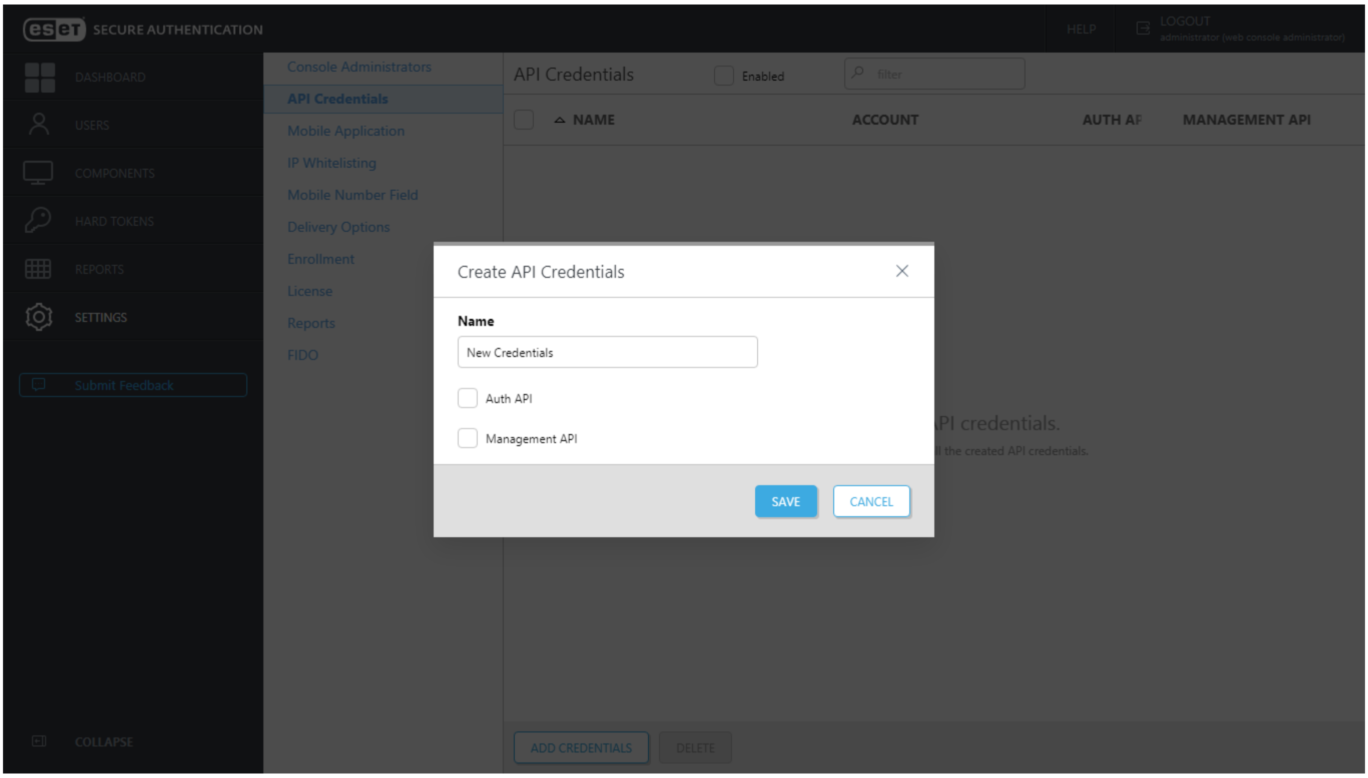
The API is disabled by default and must be enabled before use. When enabled, API credentials must be created to authorize requests.

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.



Create API Credentials

Name

New Credentials

□ Auth API

□ Management API

SAVE CANCEL

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

5. 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 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.

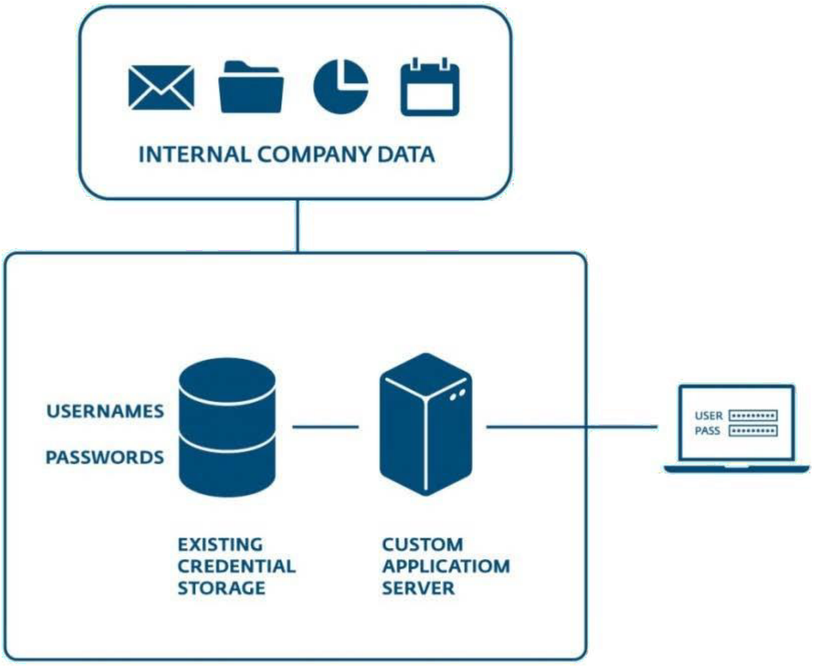
API Credentials

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.

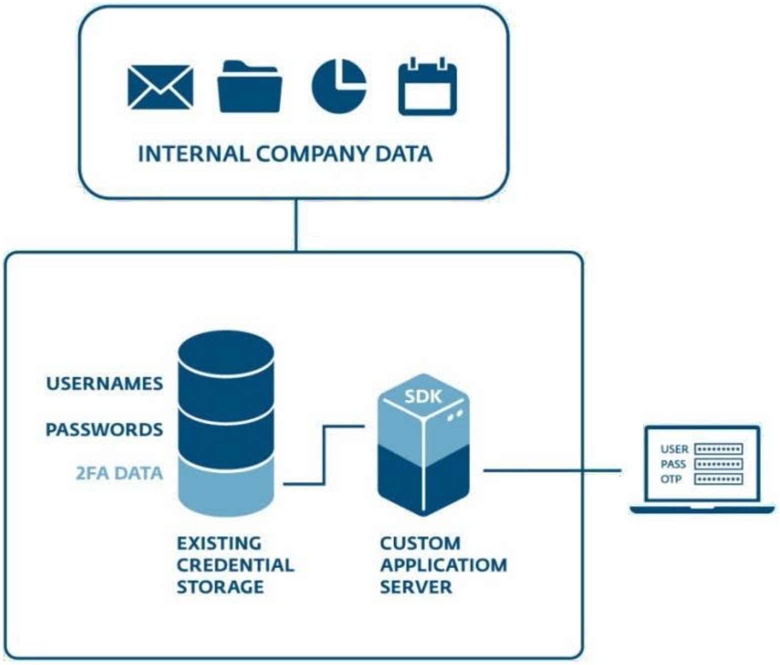
SDK

ESET Secure Authentication SDK provides both user management and authentication functionality. The SDK integrates with custom applications by storing 2FA data in the system's existing user database. This means that there are minimal external dependencies making it possible for system architects to add 2FA to nearly any custom system.

Before ESET Secure Authentication SDK integration:



After ESET Secure Authentication SDK integration:



Integration Overview

The ESET Secure Authentication SDK provides full functionality for integrating all aspects of 2FA into your custom system. This includes user authentication, management, logging, auditing and custom SMS gateway usage.

> The SDK for ESET Secure Authentication (ESA) does not support hardware tokens, push authentication and FIDO.

The SDK is available in .NET, PHP and Java and there is functional parity across all languages. Each language ships with:

- A client side library (source code)
- A language specific developer guide
- An SDK deployment guide
- Example usage code snippets in all languages

To obtain a copy of the SDK, please fill in the Enquiry form at ESET Secure Authentication product page.

To be able to use the ESA SDK, generate an API key and an API secret.

SDK License Activation

To use the ESET Secure Authentication SDK, you require an API key and an API secret. These credentials are derived from your ESET Secure Authentication license.

To derive your SDK credentials, register an account at https://eba.eset.com.

1. Log in to ESET Business Account portal.

2. Import your ESA license to ESET Business Account portal.

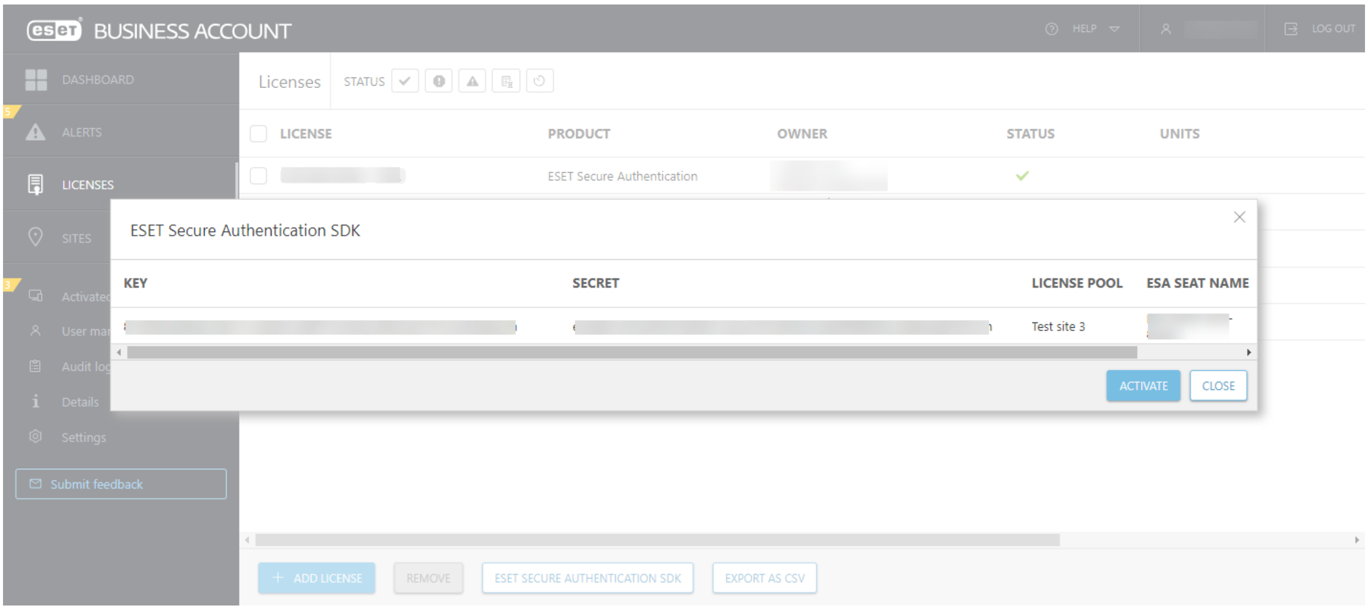
3. Click **License** > **ESET Secure Authentication SDK**.

4. Click **Activate**.

5. Select a license pool (site), that contains your ESA license.

6. Click **Activate**.

7. The portal will generate and display a unique key API key and API secret to use in ESA SDK.



LICENSE	PRODUCT	OWNER	STATUS	UNITS
[redacted]	ESET Secure Authentication	[redacted]	✓	

ESET Secure Authentication SDK

KEY	SECRET	LICENSE POOL	ESA SEAT NAME
[redacted]	[redacted]	Test site 3	[redacted]

See more information on managing SDK keys.

SDK in practice

The quickest way to get up and running with the SDK is to run the sample code.

Download the sample application .zip file from https://esa.eset.com/sdk/docs/samples/

The zip file contains a **README.txt** – follow the instructions therein.

Using the SDK

Users of the SDK can consult the ESET Secure Authentication SDK Developer Guide for instructions on integration with their platform.

The SDK Developer Guide is available here: https://esa.eset.com/sdk/docs/

This guide contains:

- How to reference the SDK library in an application
- An overview of how to use the SDK
- Detailed reference documentation for namespaces and classes

SDK System Integration

When the SDK has been evaluated, it must be integrated with your existing authentication system.

The following steps are required to integrate the ESET Secure Authentication SDK into a system:

- Extend the user storage database with extra 2FA fields
- Implement classes for reading and writing 2FA data for users
- Update existing login UI to accept OTPs
- Update existing user management UI to manage a user’s 2FA settings
- Implement optional components

Database requirements

The ESET Secure Authentication SDK stores a user's 2FA data in your existing database as a string. You will therefore need to add a column capable of storing unicode strings of varying length.

MySQL users	We recommend that you use the `TEXT` datatype
Postgres users	We recommend that you use the `character_data` datatype
Oracle users	We recommend that you use the `NCLOB` datatype
Microsoft SQL Server users	We recommend that you use the `nvarchar(max)` datatype

If you do not have a mobile telephone number field for each user, it is highly recommended that you create a field capable of storing mobile numbers (numeric strings of varying length). This will help to ensure compatibility with future releases.

Reading and Writing 2FA Data

The ESET Secure Authentication SDK exposes the `IUserStorage` interface that transports data between the SDK and your database; this interface must be implemented to read and write 2FA data (see the SDK Developer Guide for details).

The interface uses two methods that must be implemented, `loadUser` and `saveUser`.

loadUser

This method uses the following input parameter:

- string username - the user whose 2FA data will be retrieved

This method has the following return type:

- string data - the 2FA data for the user

In other words, the supplied username must be used to return the 2FA data for that user.

saveUser

This method has the following input parameters:

- string username - the user whose 2FA data you want to store
- string data - the 2FA data to store

This method has no return value. In other words, the SDK will provide the username and 2FA data – make sure that this data is written to the 2FA field in your user database.

Update Login UI With 2FA Methods

This section describes the authentication logic that must be implemented for 2FA users.

When a user has authenticated their static password against the existing system, the pre-authenticate method must be called for that user. This method checks the 2FA type for the user (SMS, Mobile App, etc) and sends an SMS OTP if required. It returns a result that contains the expected credential type, which must be used to guide the user during the logon process. Details of this type may be found in the Developer Guide.

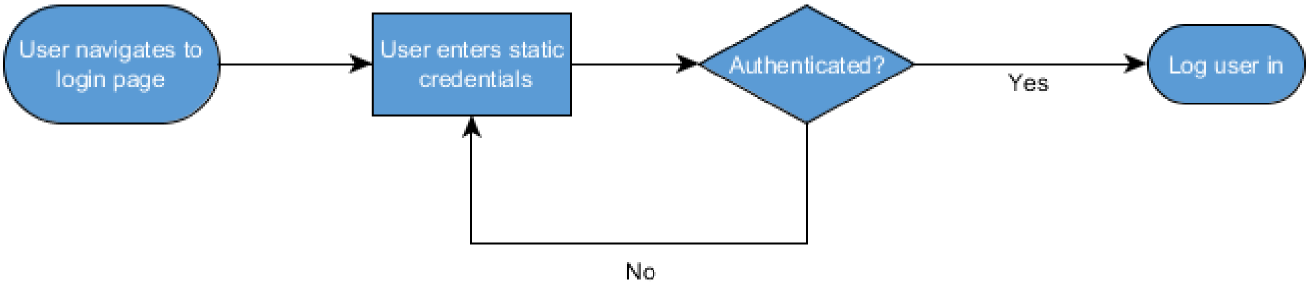


Figure 4: Single factor authentication logic (before integration)

An example of authentication logic after the ESET Secure Authentication SDK has been integrated is depicted in Figure 5.

Note that the logic for this will vary from system to system depending on the requirements.

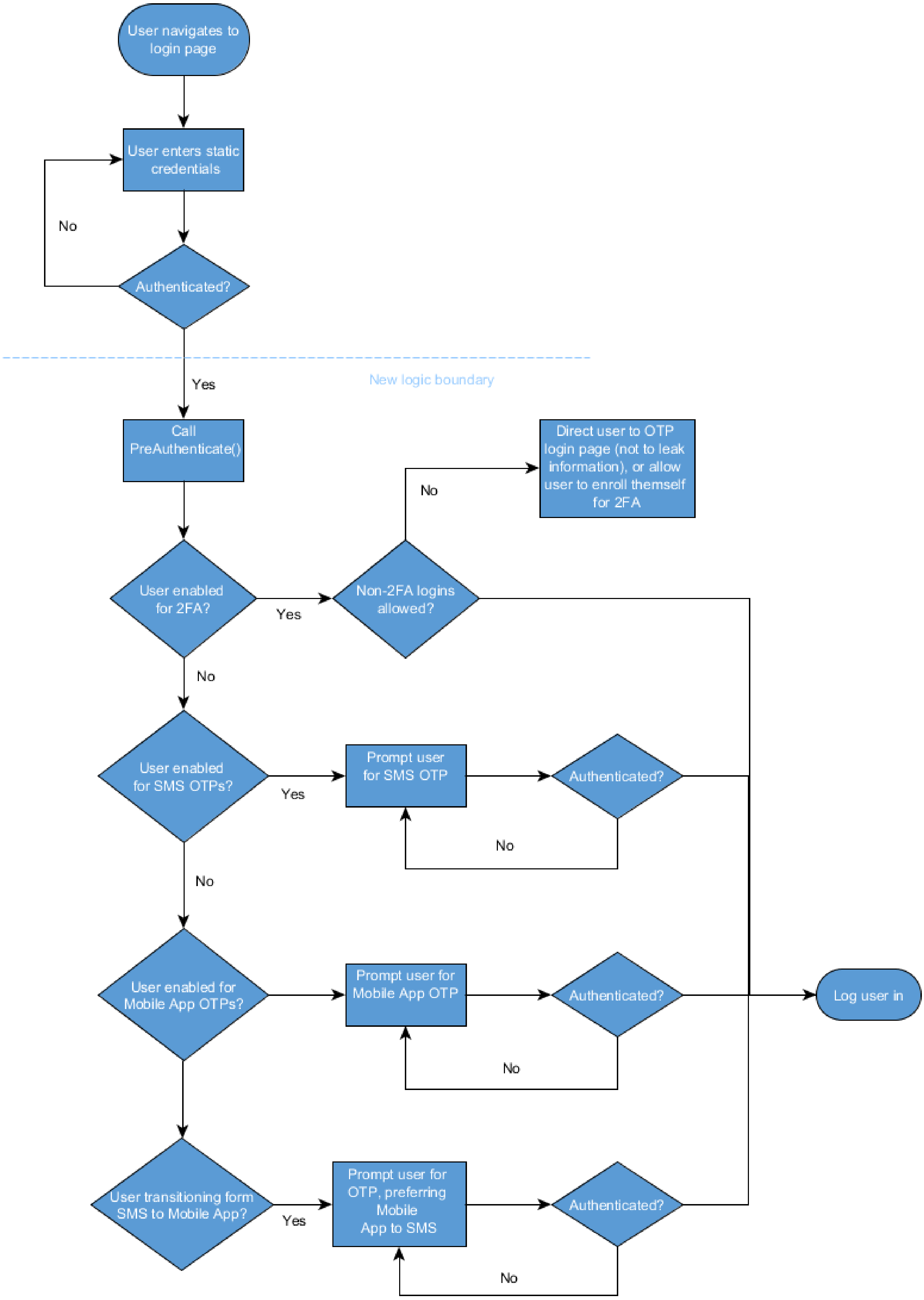

User navigates to login page
User enters static credentials
No
Authenticated?
New logic boundary
Yes
Call PreAuthenticate()
Direct user to OTP login page (not to leak information), or allow user to enroll themself for 2FA
No
User enabled for 2FA?
Yes
Non-2FA logins allowed?
No
User enabled for SMS OTPs?
Yes
Prompt user for SMS OTP
Authenticated?
No
No
User enabled for Mobile App OTPs?
Prompt user for Mobile App OTP
Authenticated?
Log user in
No
User transitioning form SMS to Mobile App?
Yes
Prompt user for OTP, preferring Mobile App to SMS
Authenticated?
No

Figure 5: Two factor authentication logic with ESA SDK

Update the Management UI to Enable/Disable 2FA For Users

User management is performed via the TwoFactorUser class. Users can be enabled for 2FA using mobile app OTPs or SMS OTPs. The transitioning state allows a user to upgrade from SMS to Mobile App OTPs. An administrator may perform user management, or users may enroll themselves.

The TwoFactorUser class exposes methods (actions) that may be performed on users.

Additional Components

The following components are optional.

Logging Integration (Recommended)

The ESET Secure Authentication SDK logs non-critical events via a logging wrapper, so as not to limit you to any logging framework. This means it is easy to use your existing logging framework. See the Developer Guide for further details.

Auditing Integration (Recommended)

The SDK audits various critical events via the IAuditor interface. If this interface is not implemented, auditing events are sent to the configured logger. The implementation is set with the setAuditor method of the TwoFactorConfiguration class.

Using an Alternative SMS Gateway (Optional)

The ESET Secure Authentication SDK sends SMS messages via the global ESET SMS gateway. You can configure your own SMS Gatewayby implementing the ITextMessageSender interface

Summary of differences

The following table summarizes the features described in this document.

Feature	API	SDK
Provides two-factor authentication	✔	✔
Provisions users via ESET's provisioning server	✔	✔
Uses ESET Secure Authentication mobile app to generate OTPs	✔	✔
Push authentication	✔	
Master recovery key	✔	
FIDO	✔	
Can be used to manage users	✔	✔
Designed for custom applications	✔	✔

Feature	API	SDK
Can be used to protect log-on	✔	✔
Requires developer to add to custom applications	✔	✔
Can be used to protect processes other than logon	✔	✔
Part of the standard ESET Secure Authentication product	✔	
Requires very little development to integrate	✔	
Stores user data in Active Directory or ESA database 1	✔	
Stores user data in client's own database		✔
Client can use own SMS gateway 2	✔	✔

1 Depends on the deployment type of Authentication Server.

2 Own SMS gateway can be achieved also via Custom delivery.

Reports

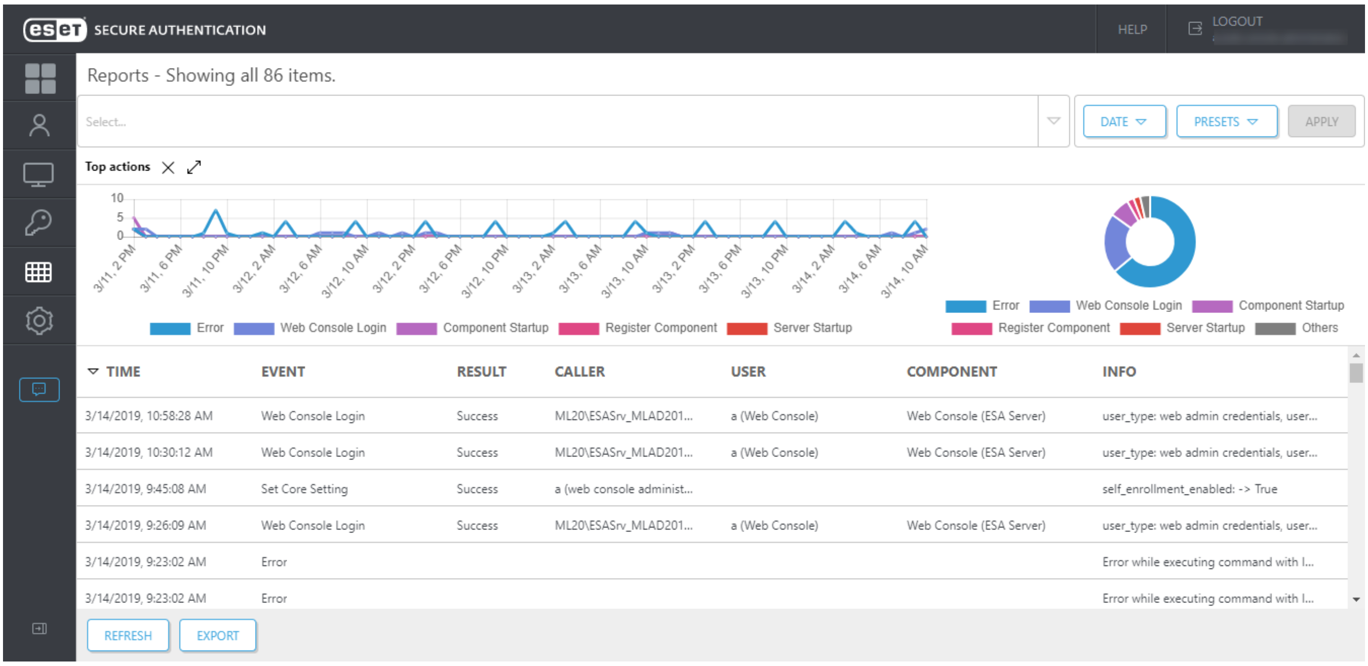
To be able to use the **Reports** screen in the ESA Web Console, it is essential to have an Elasticsearch installation available.

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.



Reports - Showing all 86 items.

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 administ...			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 I...
3/14/2019, 9:23:02 AM	Error					Error while executing command with I...

Example - filter successful Web Console logins

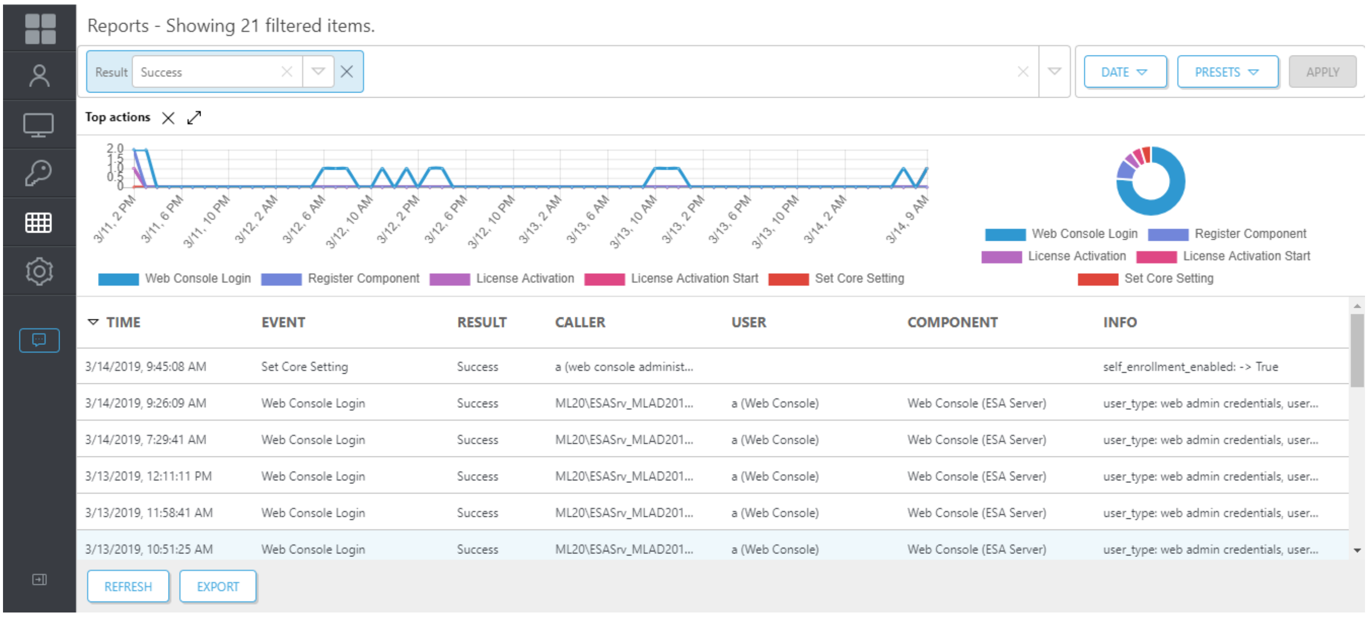
1. Click **Select** in the custom filter window, select **Event**.

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**.



TIME	EVENT	RESULT	CALLER	USER	COMPONENT	INFO
3/14/2019, 9:45:08 AM	Set Core Setting	Success	a (web console administ...			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...

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

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

  oSuccessful authentication attempts and failed authentication attempts (wrong OTP or MRK)

  oChanges to 2FA state, for example, when a user account becomes locked

- System auditing

  oChanges to ESA settings

  oWhen 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.

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).

ESA does not count the number of computers installed but the number of 2FA users. Customers can use ESA 2FA on various devices/integrations. For example, a user can use desktop logins, windows logins, Outlook Web Access, and others, which are still counted as one license unit.

Separate from USERs are OTP SMS license units, which are not mandatory, and not all customers use them. Customers using ESA OTP SMS as a 2FA method must buy a separate OTP SMS license and add it to their EBA/ESET PROTECT HUB account.

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 (Onboarding + Top-up)	0 SMS credits remain	Never	Never	Never

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	Disabled	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed

MSP options

Currently, Managed Service Providers (MSPs) have the following 2FA service options powered by ESET Secure Authentication:

Authentication Server on customers' premises

- MSP installs the Authentication Server on each customer's premise and activates each Authentication Server using an EBA or EMA account

- Web Console per customer

One Authentication Server on MSP's premises

- MSP installs the Authentication Server in high availability mode (multiple Authentication Servers) and activates the Authentication Server using an EBA or EMA account

- ESA components are installed per customer

- One Web Console for managing all customers. Each customer is imported to a separate realm—select a specific OU when synchronizing with LDAP

Multiple Authentication Servers in MSP's premises

- MSP installs an Authentication Server per customer and activates each Authentication Server using an EBA or EMA account

- Web Console per customer

i External access

External access to Web Console is recommended.

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.

Troubleshoot other issues using the following operations:

- Domain authentication
- Connection to the RADIUS server
- Configuration of VPN to connect to RADIUS
- Login via RDP secured by 2FA (installation of Remote Desktop plugin)
- How to add SMS Credits?

Component connection issues

If ESA components fail to connect to the ESA Authentication Server, adjust the connection parameters in the `C:\Program Files\ESET Secure Authentication\EIP.Core.WindowsService.EXE.config` file.

- **EsaServiceIdleTimeout**: Indicate how long to leave connections opened. Applies to **Active Directory**

Integration mode.

Default value: Two minutes

- **http.sys**: Indicate how long to leave HTTP connections opened (Web Console, customer API). It applies to **Standalone** installation mode.

To display the existing timeout setting, execute the following command in PowerShell:

```
netsh http show timeout
```

To change the timeout, execute the following command in PowerShell:

```
netsh http add timeout timeouttype=idleconnectiontimeout value=<seconds>
```

Replace `<seconds>` with the desired timeout in seconds.

- **EsaMaxSessions**: Throttling—maximum concurrent sessions

  Default value: 100 times processor count

- **EsaMaxCalls**: Throttling—maximum concurrent calls

  Default value: 16 times processor count

- **EsaMaxThreads**: .NET thread pool—maximum count of threads in the pool; influences maximum count of simultaneously handled requests

  Default value: 1000

- **EsaMinThreads**: .NET thread pool—create threads immediately up to this count; influences how quickly the thread pool reacts to the increasing count of incoming connections

  Default value: Count of processor cores

Example of an altered EIP.Core.WindowsService.EXE.config file

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="EsaServiceIdleTimeout" value="00:01:00" />
    <add key="EsaMaxSessions" value="100" />
    <add key="EsaMaxCalls" value="20" />
    <add key="EsaMaxThreads" value="2000" />
    <add key="EsaMinThreads" value="1000" />
  </appSettings>
</configuration>
```

- **EsaServiceIdleTimeout:** `hours:minutes:seconds` format

Windows Login protection does not work

You installed the Windows Login plugin on a computer and enabled 2FA for your user account. However, 2FA does not prompt the appropriate user account.

If another credential provider disabled the Windows Login plugin of ESET Secure Authentication, try one of the following options

- Reconfigure the other credential provider not to block ESA Windows Plugin.
- Uninstall the other credential provider.
- Disable the other credential provider manually by changing the following registry entry:

  1. Locate the following entry:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters/id`

  2. Add a new DWORD value to it with the following attributes:
  Name: Disabled
  Value: 1

If there are multiple login types available, allowing a user to bypass 2FA, try one of the following options

- Disable the other login types in Windows.
- Reconfigure the other credential provider not to display its login types.
- Remove the other credential provider.
- Disable the other credential provider manually by changing the following registry entry:

  1. Locate the following entry:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters/id`

  2. Add a new DWORD value to it with the following attributes:
  Name: Disabled
  Value: 1

Installation of Reporting Engine (Elasticsearch) fails

Installation fails when installing the Reporting Engine (Elasticsearch) on a machine with less than 2GB free RAM.

Applies to ESET Secure Authentication version 2.8.20.0.

New installation of Authentication Server and Elasticsearch

1. "Installing Elasticsearch service..." displays for a one minute.
2. The rollback process starts.
3. "Installation failed" message displays.

At this point, the Authentication Server and the Reporting Engine are not functional.

Change existing installation of Authentication Server

1. "Installing Elasticsearch service..." displays for one minute.
2. "Installation failed" massage displays.

At this point, only the Authentication Server remains functional.

In both cases, it is essential to remove the `elasticsearch-service-x64` service from Windows services.

1. Click the **Start** menu, type `cmd`.
2. Right-click **Command Prompt** in the search result, select **Run as administrator**.
3. Run the following command:

```
sc delete elasticsearch-service-x64
```

Known issues

For a list of known issues, refer to the following related Knowledgebase article.

Glossary

- 2FA - Two-factor authentication
- AD - Active Directory
- ADI - Active Directory Integration
- ADUC - Active Directory Users and Computers management interface
- ESA - ESET Secure Authentication
- ESA component - Windows Login plugin, Remote Desktop plugin, Web App plugin, AD FS protection, RADIUS Server, Identity Provider Connector
- ESA core or AS - Authentication Server that verifies the validity of an typed OTP.

- ECP - Exchange Control Panel
- FQDN - Fully qualified domain name
- GPO - Group Policy Object
- IdP - Identity Provider
- MRK - Master recovery key
- Online (Online mode) - An ESA component is in online mode if it can contact the Authentication Server via TCP/IP connection, or if it is installed on the same machine as the Authentication Server.
- Offline (Offline mode) - An ESA component is in offline mode if it is not installed on the same machine as the Authentication Server and it cannot even contact the Authentication Server via TCP/IP connection.
- OS - Operating System.
- OTP - an one time password, either with limited time validity (time-based OTP) or without limited time validity (event-based OTP).
- OWA - Outlook Web Access
- 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.

End User License Agreement

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement (hereinafter referred to as "the Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement. If You do not agree to all of the terms and conditions of this

Agreement, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software (hereinafter referred to as " Documentation "); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smart phones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights (hereinafter referred to as "License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses**. The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one computer system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as "MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent in which has the right to use the Software in accordance the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Business Edition**. A Business Edition version of the Software must be obtained to use the Software on mail servers, mail relays, mail gateways or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software**. OEM Software shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License.** The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall be also entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements**. To operate correctly the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software**. The Provider shall be entitled from time to issue updates to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled automatic installation of Updates. For the purpose of provisioning of Updates, License authenticity verification is required including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

b) **Forwarding of Information to the Provider.** The Software contains functions which collect data about the installation process, the Computer and/or the platform on which the Software is installed, information about the operations and functionality of the Software and information about other computers used as recipients of authentication messages and/or means of authentication based on authentication method chosen by End User (hereinafter referred to as "Information ") and then send them to the Provider. Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations.

The Software may require a component installed on other computer, which enables transfer of authentication messages and/or provide means of authentication. Information, which are subject to transfer contains limited set of data required to ensure authentication based on authentication method chosen by End User as specified in Privacy Policy and in compliance with relevant legal regulations.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer. You hereby agree to receive notification and messages including but not limited to marketing information.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival back-up copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are

permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement**. This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all back-up copies and all related materials provided by the Provider or its business partners. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. The End User shall be required to back up all existing data,

software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software**. The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any act, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies (hereinafter referred to as "Affiliates") being in violation of, or being subject to negative consequences under, Trade Control Laws which includes

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (hereinafter referred to as "Export Control Laws") and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (hereinafter referred to as "Sanction Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19.a of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. In case of a discrepancy between language versions of this Agreement, the English version shall prevail. This Agreement may only be modified in written form, signed by an authorized representative of the Provider, or a person expressly authorized to act in this capacity under the terms of a power of attorney.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

EULA ID: BUS-ESA-20-01

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Update and other statistics covering information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, anonymized IP address, configuration settings of product.

- For the purpose of authentication of provisioning and provisioning itself as well as for the purpose of overall functioning of product's features You might choose to use, We may need information such as user name, telephone number, token name, token ID, other token information, activation URL, license information, phone ID, notification ID, platform information.

- Crash dumps concerning components of products may be required enabling ESET to provide appropriate support and maintenance.

- Licensing information such as license ID and personal data such as name, surname, address, email address is required for billing purposes, license genuineness verification and provision of our services.

- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in logs or crash dumps itself and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject’s Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,

- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk