ESET
SECURE
AUTHENTICATION
Installation Manual
1. Overview

The ESA suite consists of the following component features:

- **The ESA Authentication Service**, which includes a REST-based API.
- **The ESA RADIUS Server**, which is used to authenticate VPN access.
- **The ESA Outlook Web App / Access (OWA) plug-in**, which is used to authenticate OWA access.
- **ESA Management Tools**:
  - ESA User Management plug-in for Active Directory Users and Computers (ADUC), which is used to perform user management.
  - **ESA Management Console**, which is used to configure the ESA services.

2. Supported Environments

The ESA Services and management tools have been tested and are supported on Windows 2003 Server, Windows 2003 Server R2, Windows Small Business Server 2008, Windows Server 2008, Windows Server 2008 R2, Microsoft Small Business Server 2011 and Windows Server 2012, in both 32-bit and 64-bit versions. Management tools are also supported on client operating systems from Windows XP SP3 and later, in both 32-bit and 64-bit versions.


The minimum supported Active Directory domain functional level is "Windows 2000 Native".

The installer automatically selects all components that can be installed on the current computer, with the exception of the Core Authentication Service, which is always selected by default. Should the user select a component that cannot be installed, the installer will inform the user of the exact prerequisites that are outstanding.

The ESA Mobile app is compatible with the following mobile phone operating systems:

- iPhone iOS 4.2.1 and higher
- Android™ 2.1 and higher
- Windows Phone 7 and higher
- Windows Mobile 6
- BlackBerry® 4.3 to 7.1
- Symbian® - all supporting J2ME
- All J2ME enabled phones

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

3. Installation Requirements

The installer must be run from the domain Administrator account (i.e. domain\Administrator).

ESA is supported on server operating systems from Windows 2003 Server SP2 and later, and on client systems from Windows XP SP3 and later, in both 32-bit and 64-bit versions.

**NOTE**: The Authentication Service and RADIUS Server components are compatible with Windows XP SP3 and later, but will not be supported on these client operating systems.

ESA supports the installation of components in a distributed environment, with all components installed on computers that are joined to the same Windows Domain. The prerequisites for the installation of each component are:

- **Authentication Service**:
  - Windows 2003 Server SP2 or later
  - .Net Framework version 4.0, full installation (not Client Profile)
- **Management Tools:**
  - Windows XP SP3 or later, or Windows 2003 Server SP2 or later
  - .Net Framework version 3.5 (4.0 may also be installed, but will not be utilized)
  - Windows Remote Server Administration Tools, Active Directory Domain Services component (RSAT AD DS)
  
  **NOTE:** RSAT was previously known as the Remote Administration Pack (adminpak) and is downloadable from Microsoft. In Windows Server 2008 and later, this component may be installed from the “Add Feature” wizard in the Server Manager. All Domain Controllers already have these components installed.

- **RADIUS Server:**
  - Windows 2003 Server SP2 or later
  - .Net Framework version 4.0, full installation (not Client Profile)

- **Outlook Web App / Access Plugin:**
  - Microsoft Exchange Server 2007 or later (64-bit only), with the Client Access role (Outlook Web App / Outlook Web Access) installed
  - .Net Framework version 3.5 (4.0 may also be installed, but will not be utilized)

---

**.NET Requirements**

- Core Server: .Net 4 or 4.5 Full Install
- RADIUS Server: .Net 4 or 4.5 Full Install
- OWA Plugin: .Net 3.5
4. Installation

All of the following components are required for an ESA installation:

- At least one instance of the Authentication Server
- At least one instance of the Management Tools
- At least one of the authentication endpoints (API, OWA or RADIUS)

All the components may be installed on a single machine, or they may be installed across multiple machines in a distributed environment. As is the case with distributed systems there are many possible installation scenarios. Only a single generic installation scenario will be described here, yet the steps described should generalize well to other deployment scenarios. The example installation consists of two sequences. After completing both, your deployment will correspond with Figure 1.
4.1 Installation of the Core components

From the machine hosting the ESA core service, run the supplied .msi file to start the installation. Ensure that you are running the correct installer for your OS architecture (x86 or x64). When prompted, make sure that the first three features are selected, as per Figure 2.

![Core components installation](image)

4.2 Installation of the OWA plugin

From the machine running your Exchange server, run the supplied .msi file to start the installation. When prompted, make sure that the last component is selected, as per Figure 3.

![OWA plugin installation](image)
5. Activation and Licensing

Once the ESA Server has been installed, it must be activated before it may be used. To activate your ESA Server, you will need an ESA license. This license can be obtained from your ESET distributor, or the demo license (in License.txt) shipped with the installer can be used.

To activate your ESA Server:

1. Launch the ESA Management Console.
2. Navigate to your domain node.
3. Enter the Username and Password for your ESA license.
4. The ESA Server will obtain its license automatically and display the current license information.

5.1 Licensing business rules

5.1.1 Overview

The ESA system allows enforcement of licenses based on the following three license parameters:

- User Total
- Expiry Date
- SMS Credits

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

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

5.1.2 Design Decisions

System Shutdown

In the case of extreme license violation, all 2FA users will be locked out of the system indefinitely until licensing issues are resolved.

User Limit Violation

If a user with a valid paid license exceeds their user limit, a warning notification will be displayed in the User Management plugin in the ADUC console and in the ESA Management Console. See sections 5.1.3 Warnings and 5.1.4 License States for more details.

5.1.3 Warnings

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

During User Management

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

During System Administration

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

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

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

Details of License States

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

<table>
<thead>
<tr>
<th>License Expiry</th>
<th>Warning</th>
<th>SMS Credits depleted</th>
<th>Violation (full functionality)</th>
<th>Violation (limited functionality)</th>
<th>ESA Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>less than 30 days before expiration</td>
<td>N/A</td>
<td>O more than the license expiry date more than/equal 7 days</td>
<td>more than 7 days after expiration</td>
<td>more than 30 days after expiration</td>
<td></td>
</tr>
<tr>
<td>less than 10% or 10 seats available, whichever is lowest</td>
<td>N/A</td>
<td>Active users exceed licensed users</td>
<td>more than 7 days after active users exceed license</td>
<td>Never</td>
<td></td>
</tr>
<tr>
<td>less than 10 SMS credits remaining (Onboarding + Top-up)</td>
<td>O SMS credits remain</td>
<td>Never</td>
<td>Never</td>
<td>Never</td>
<td></td>
</tr>
</tbody>
</table>

5.1.5 License Enforcement

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

<table>
<thead>
<tr>
<th>OK</th>
<th>Warning</th>
<th>SMS Credits depleted</th>
<th>Violation (full functionality)</th>
<th>Violation (limited functionality)</th>
<th>ESA Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
</tbody>
</table>
6. High Availability View

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

7. Configuration

All configuration of the ESA system will be performed via the ESA Management Console. The ESA Management Console is added as a Snap-In to the standard MMC console. The ESA Management Console may be accessed under Administrative Tools, as per Figure 4.
7.1 Configuring the ESA Application

Certain operating parameters of the ESA suite can be customized after installation. This chapter describes the override options available to the ESA administrator. Since default values are loaded if no options are specified, the settings are referred to as “overrides” in this chapter.

All override files are in XML format, with each override specified as a key-value pair inside the appSettings node. Below is the template to which ALL override files must conform, where x is an example key and y its value.

```xml
<?xml version="1.0"?>
<configuration>
  <appSettings>
    <add key="x" value="y" />  
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0")/>
  </startup>
</configuration>
```

7.1.1 Authentication Server Overrides

Overrides of the Core Authentication Server parameters are located in

```
%ProgramFiles%\ESET SecureAuthentication\EIP.Core.WindowsService.exe.config
```

This file may contain the following overrides:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Data Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EsaServicePort</td>
<td>The TCP port that the Windows Service listens on.</td>
<td>integer</td>
<td>8000</td>
</tr>
<tr>
<td>EndPointSecurityEnabled</td>
<td>Specifies whether authentication and authorization mechanisms between ESA components are active.</td>
<td>boolean</td>
<td>true</td>
</tr>
<tr>
<td>SendEndPointExceptionDetails</td>
<td>Enables or disables whether debug information is exchanged between components when a SOAP fault is encountered.</td>
<td>boolean</td>
<td>true</td>
</tr>
</tbody>
</table>

7.2 Configuring RADIUS

In order for your ESA RADIUS server(s) to be utilized by your existing VPN server, you will need to reconfigure your VPN server.

- **CLIENT SETTINGS**

Each server will only respond to RADIUS requests from a list of known clients, so at least one client should be created. Follow these steps to configure a client:

1. Right click the RADIUS server and select **Add Client**.
2. Select the new client and choose **Properties** from the list of available actions.
3. Configure the IP Address and **Shared Secret** for the Client so that they correspond to the configuration of your VPN device.
4. Optionally restrict VPN access to an existing Active Directory security group.
5. Optionally allow any existing non-2FA users to continue using the VPN.

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

6. Give the RADIUS client a memorable name for easy reference.

7. Once you are finished making changes, click **OK**.

8. Re-start the RADIUS Server.
   
   a. Locate the ESA RADIUS Service in the Windows Services (under **Control Panel - Administrative Tools - View Local Services**).
   
   b. Right Click on the ESA Radius Service and select **Restart**.

7.2.1 RADIUS Server Overrides

Overrides of the ESA RADIUS Server operating parameters are located in

%ProgramFiles%\ESET SecureAuthentication\EIP.Radius.WindowsService.exe.config

This file may contain the following overrides:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Data type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RadiusListenIp</td>
<td>The IP address that the ESA RADIUS Windows Service listens on.</td>
<td>string</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>RadiusListenPort</td>
<td>The IP address that the ESA RADIUS Windows Service listens on.</td>
<td>integer</td>
<td>1812</td>
</tr>
</tbody>
</table>

7.3 PPTP configuration

This chapter describes how to secure a PPTP VPN with ESET Secure Authentication (ESA) using either Microsoft Routing and Remote Access (RRAS) or Microsoft Network Policy Services (NPS).

**Requirements**

- Active Directory Domain Controller
- ESA Core Server
- ESA RADIUS Server
- RRAS/NPS VPN Server (We recommended that you test using normal Windows authentication before switching to 2FA)

**Installation**

For full installation details, see the chapter **Installation**.

- Install and license an ESA Core Server.
- Install at least one ESA RADIUS server.

**Notes**:

1. The RADIUS server should not be installed on the same machine as the VPN server, since RRAS/NPS already listen for RADIUS requests on port 1812.

2. If the ESA RADIUS server must be installed on the VPN server, configure RRAS/NPS to listen for RADIUS requests on a different port (e.g. 1645).
7.3.1 Configuring ESA
The ESA RADIUS Server will start automatically. Ensure that it is running by checking its status in System Services.

**ESA RADIUS Server Configuration**

1. Start the ESA Configuration Manager and navigate to the RADIUS Servers node. The RADIUS Server will appear automatically once it has been started.
2. Select the RADIUS Server and choose **Add Client**.
3. Configure the newly created client:
   a. Shared Secret: Choose a secure shared secret.
   b. IP: Enter the IP address of the RRAS Server.
   c. Authentication Method: Select the desired authentication method (OTP is recommended)
   d. Optionally configure pass-through authentication and group restrictions.
4. Restart ESA RADIUS Server (via System Services) to apply configuration changes.

**ESA User Configuration**

1. Start Active Directory Users and Computers and select the desired user.
2. Right-click the user, click **Properties** and then click the **ESA** tab.
3. Select the check box next to **Mobile Application**.
4. Select **Send Application to user**.
5. Ensure that the user has installed the application successfully and can generate OTPs.

7.3.2 Configuring your VPN to use ESA

If your VPN server is running RRAS only, follow the instructions in the **RRAS Configuration** section. If your VPN server is configured using NPS, follow the instructions in the **NPS Configuration** section.

7.3.2.1 RRAS Configuration

In Server Manager, right-click **Routing and Remote Access** under **Network Policy and Access Services** and select **Properties** from the context menu.

2. Click the **Security** tab and ensure that the authentication provider is set to **RADIUS Authentication**.
3. Click **Configure**....
4. Add your ESA RADIUS server with the same shared secret used in the **ESA Configuration** section (timeout = 5, initial score = 30, port = 1812, “always use message authenticator” disabled).
5. Click **OK** twice and then click **Authentication Methods**....
6. Ensure that the check boxes next to **PAP** and **MS-CHAPv2** are selected, and all others are deselected. See Appendix A for further information regarding these options.
7.3.2.2  NPS Configuration
1. On the server manager, open RADIUS Clients and Servers.
2. Right-click Remote RADIUS Server Groups and select New from the context menu to create a new group.

Configuring the ESA RADIUS Server group
1. Enter a name for the group, for example ESA RADIUS Server Group.
2. Click Add to add a RADIUS Server.
3. Click the Address tab and type the IP address of the ESA RADIUS Server in the Server field.
4. In the Authentication/Accounting tab, make sure that the Port is set to 1812 and enter the same shared secret you used in your ESA configuration.
5. In the Load Balancing tab, set the Number of seconds before request is considered dropped field to 30 seconds.

Configuring the RRAS Server to delegate authentication to ESA
1. Right-click Policies or Connection Request Policies and select Create new policy from the context menu.
2. In the Overview tab:
   a. Set the Policy name (for example ESA RADIUS Authentication).
   b. Set the Policy type as Remote Access Server (VPN Dial-up).
3. Set the date, time and any other necessary conditions in the Conditions tab.
4. In the Settings tab:
   a. Select Forwarding Connection Request -> Authentication.
   b. Select the radio button for Forward requests to and then select the ESA RADIUS Servers Group created previously.

   Warning: When using compound authentication (Password + OTP), only the PAP authentication protocol may be used. This will result in warnings from the RRAS Server and VPN Client, which can be ignored.

7.3.3  ESA Authentication Methods and PPTP Protocol Compatibility
This section explains which PPTP protocols are compatible with which ESA authentication methods. The VPN server must be configured to allow all protocols that clients might want to use. End-user VPN clients need only be configured for a single protocol.
Whenever more than one protocol is supported, VPN clients should be configured to use MS-CHAPv2 with 128-bit MPPE. This means that PAP is only recommended for Compound Authentication.

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>PAP</th>
<th>MS-CHAPv2</th>
<th>MS-CHAPv2 with MPPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS-Based OTPs</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Mobile-Application (OTP Only)</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Mobile Application (Compound Authentication)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Active Directory passwords without OTPs</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>
8. Managing users

All user management is done via the Active Directory Users and Computers management interface. Phones using the mobile application must have valid mobile phone number before they can be provisioned.

Provisioning a new mobile phone

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

**NOTE**: Mobile numbers must consist entirely of digits (for example, they must be in the format 421987654321, where 4 is the country code and 21 is the area code).
Click the ESET Secure Authentication tab to manage ESET Secure Authentication settings for a specific user.

The use of soft-token OTPs for a specific user:

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

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

1. Open the normal ADUC user view.

2. Hold CTRL and click to select the users you want to provision.

3. Right-click the group of users that you want to provision and select Properties from the context menu.

4. In the Properties for Multiple Items window, click the ESET Secure Authentication Tab.

5. Select the the check boxes next to Update Enabled Token Types and Mobile Application (leave the check box next to SMS-based OTPs deselected).
6. Click **Send Application**. Your client phones will receive a text message containing a link to the ESA mobile app download page.

![Image of Properties for Multiple Items dialog box with user information and options for enabling token types.]

<table>
<thead>
<tr>
<th>Username</th>
<th>2FA Locked</th>
<th>2FA Mode</th>
<th>Last Login</th>
<th>Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>David</td>
<td>No</td>
<td>SMS-OTP</td>
<td>2/22/2013 2:38:06 PM</td>
<td>0</td>
</tr>
<tr>
<td>donlit</td>
<td>No</td>
<td>None</td>
<td>Never</td>
<td>0</td>
</tr>
<tr>
<td>elie</td>
<td>No</td>
<td>Mobile App</td>
<td>2/22/2013 2:57:32 PM</td>
<td>0</td>
</tr>
<tr>
<td>Elvis</td>
<td>No</td>
<td>None</td>
<td>Never</td>
<td>0</td>
</tr>
</tbody>
</table>

**With selected users:**

- [ ] Update Enabled Token Types
- [ ] SMS-based OTPs
- [x] Mobile Application

**Options:**

- [ ] Unlock 2FA
- [ ] Send Application
- [ ] OK
- [ ] Cancel
- [ ] Apply
10. Outlook Web Access Integration

The ESA OWA integration module automatically adds 2FA into the OWA authentication process. To verify correct operation:

1. Make sure that in the ADUC management tool all users have ESA 2FA authentication enabled.
2. Open the OWA login page in a desktop browser.
3. Authenticate using normal AD username and password.
4. The ESA authentication page should now appear:
   a. If the user is enabled for SMS OTPs, a SMS text message will be sent containing an OTP that may be entered to authenticate.
   b. If the user has an installed the ESA mobile application installed on their phone, it can be used to generate an OTP to authenticate.

11. Authentication Methods

This chapter provides an overview of the authentication methods by which an Administrator of an ESET Secure Authentication (ESA) installation can grant access to the Outlook Web App (OWA) and VPN endpoints in his domain.

OTPs and Whitespace

OTPs are displayed in the mobile application with a space between the 3rd and 4th digits in order to improve readability. All authentication methods are agnostic to the presence of whitespace in the provided credentials, so a user can include or exclude the whitespace without affecting authentication.

11.1 VPN Authentication Methods

The following configurations are supported when authenticating via the VPN endpoint.
11.1.1 Compound Authentication

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

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

Supported PPTP protocols: PAP.

11.1.2 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 OTP authentication.

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

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

Supported PPTP Protocols: PAP, MSCHAPv2.

11.1.3 Mobile Application

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

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

Supported PPTP Protocols: PAP, MSCHAPv2.

Compound Authentication Enforced

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

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

Supported PPTP protocols: PAP.
11.1.4 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 PPTP Protocols: PAP, MSCHAPv2.

11.1.5 Non-2FA Pass-through

This scenario occurs if the user is configured for neither SMS-based OTPs nor Mobile Application 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 PPTP Protocols: PAP, MSCHAPv2.

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

11.1.6 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.

11.2 OWA Authentication Methods

11.2.1 SMS OTP

This scenario occurs if the user is configured to use only SMS-based OTPs. Note that SMS OTPs will not be delivered to accounts with 2FA authentication locked in the ADUC.

In this configuration, a user first enters their Active Directory password. They will then be prompted for an OTP, which will be delivered via SMS. The user then logs in with the OTP contained in the SMS.

11.2.2 Mobile Application

This scenario occurs if the user is configured to use only the Mobile Application.

In this configuration, a user logs in with their Active Directory password. They will then be prompted for an OTP. The user then logs in with the OTP generated with his Mobile Application.

11.2.3 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.

In this configuration, a user logs in with their Active Directory password. They will then be prompted for an OTP and will receive an SMS containing an OTP.

The user may log in with the SMS OTP or with the OTP generated using the Mobile Application.

If the user logs in with an OTP generated using the Mobile Application, SMS OTP authentication will automatically be disabled. On subsequent attempts, SMS-based OTPs will not be accepted as log in credentials.
11.2.4 Non-2FA Pass-through
This scenario occurs if the user is configured for neither SMS-based OTPs nor the Mobile Application and the OWA configuration option to allow non-2FA users to log in is selected.
In this configuration a user logs into their Exchange mailbox with their Active Directory password.

11.3 OTPs and Whitespace
OTPs are displayed in the mobile application with a space between the 3rd and 4th digits in order to improve readability. All authentication methods are completely agnostic to the presence of whitespace in the provided credentials, so a user may include or exclude whitespace without affecting authentication.

11.4 2FA Lockout
After 10 unsuccessful OTP authentications, it is assumed that an attacker is attempting to access the account and the 2FA is “locked”. What this means is that the user will be unable to authenticate using any OTPs, valid or invalid, and that the System Administrator will need to unlock the user’s 2FA in the ESA tab within the ADUC.

12. Known Issues
- On Blackberry devices, it is necessary to delete the ESA mobile application manually to remove old application data before you can install a new copy of the ESA mobile application.
- The ESET Secure Authentication tab for user management is only visible from the ADUC. It is not currently visible in any other management components.
- Certain Symbian phones display a low-resolution ESA mobile app icon.
- The ESA Admins AD security group is not removed during uninstallation.
- The ESA core can only be installed using the Administrator account.