ESET

SECURE AUTHENTICATION

Custom integration via the SDK and API

ENJOY SAFER TECHNOLOGY™

ESET **SECURE AUTHENTICATION**

Customer Care: www.eset.com/support

REV. 8/11/2017

Contents

1. Overview

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.

This document describes when and how to use these options.

2. Native Integrations

ESET Secure Authentication natively supports:

- RADIUS based systems such as VPN/UTM appliances, Citrix® XenApp™, VMWare® Horizon View™, etc. A full list is available here.
- Microsoft Outlook Web App
- Microsoft SharePoint
- Microsoft Dynamics CRM
- Microsoft Remote Desktop Web Access

If you wish to add two-factor authentication to a Microsoft Web Application, see the product manual for details.

For integration with RADIUS systems such as VPN appliances, choose the integration guide you are interested in.

For further information on adding 2FA to systems not listed above, see the API and SDK chapters below.

3. Key Benefits Extensibility Overview

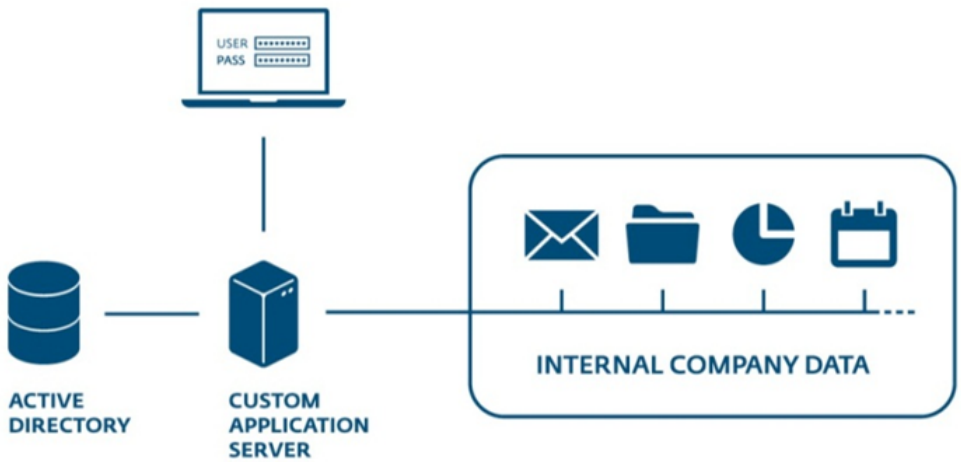
ESET Secure Authentication provides two extension options: an Application Programming Interface (API) and a Software Development Kit (SDK). There are some key differences between the two products that will quickly help you decide which to use.

3.1 API Overview

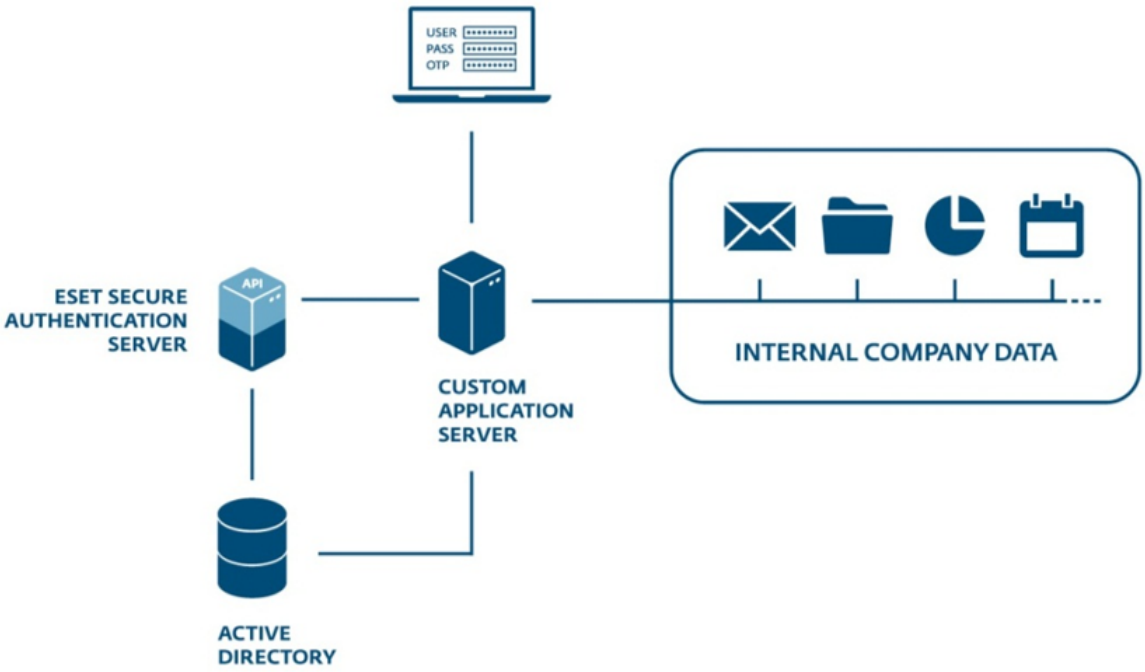
The API is an authentication API: it provides authentication functionality only. It does not provide user management features such as enabling users for 2FA or unlocking locked accounts. Therefore, the API should be used for adding 2FA to authentication systems where users are already stored and managed in Active Directory.

For user stores that are not Active Directory based (such as MySQL), use the SDK.

Before ESET Secure Authentication API integration:



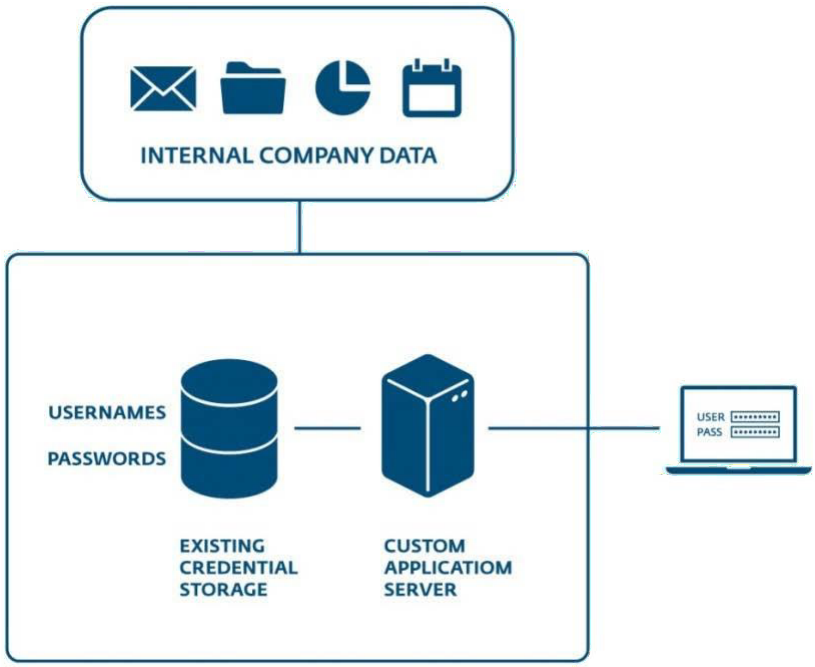
After ESET Secure Authentication API integration:



3.2 SDK Overview

The 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:

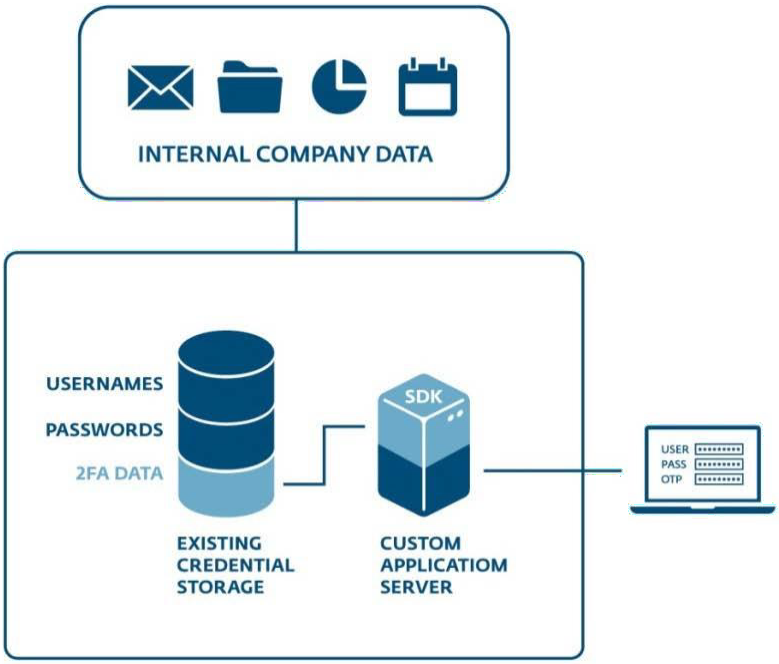


Figure 2: After ESET Secure Authentication SDK integration

The remainder of this document provides instructions for obtaining the SDK, using the example code and finally integrating the SDK into your existing platform.

4. Adding 2FA using the API

The ESET Secure Authentication API provides a RESTful interface for user authentication. Integration requires implementation of the necessary REST calls during your existing authentication workflow.

The API is an extension of the standard Active Directory product and as such is automatically available when you install ESET Secure Authentication.

User 2FA settings are managed in the standard way by using Active Directory Users and Computers. There is therefore no requirement to add custom user management code to your system, greatly simplifying the integration requirements.

For instructions on configuring and using the API, see the User Guide.

5. Adding 2FA using the SDK

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.

Please note that the SDK for ESET Secure Authentication does not support hardware tokens.

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.

6. Summary of differences

The following table summarizes the features described in this document.

Feature	API	SDK
Provides two-factor authentication	✓	✓
Meets compliance standards	✓	✓
Provisions users via ESET's provisioning server	✓	✓
Uses ESET Secure Authentication mobile app to generate OTPs	✓	✓
Push Authentication	✓	
Designed for custom applications	✓	✓
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	✓	
Standard pricing model	✓	
Requires very little development to integrate	✓	
Requires Active Directory	✓	
Stores user data in Active Directory	✓	
Stores user data in client's own database		✓
Client can use own SMS gateway		✓