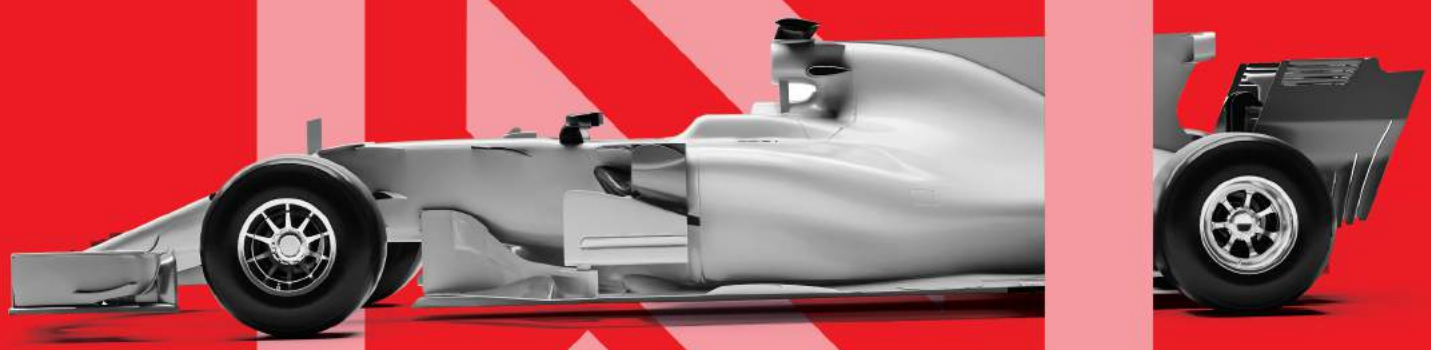
BUILD SOMETHING POWERFUL



Building something powerful entails building securely and thoughtfully. Neutrinos Platform provides smart ways to secure your applications with in-built standards and compliant, re-usable components which are consistent with the Neutrinos philosophy of building something powerful and easy at the same time. Learn about identity management, standard security compliance, Single Sign-On, role-based security policies, vulnerability checks and more.

NEUTRINOS

www.neutrinos.co

TABLE OF CONTENTS

Neutrinos Security Paradigm

Neutrinos Identity Server (IDS) is the central authentication point that offers credential management for each integrated resource of Neutrinos Platform and delivers an SSO experience. The feature of enterprise-grade password management provides the ability to centrally manage users of the organization with a set of policies that enforce corporate security standards. This is achieved using the Neutrinos Console which is the global console to manage the application environment. The Console:

- Assigns and revokes access to certain apps and deployment environments
- Learns the context around the user such as location and device
- Enables federation and removes the need of password usage
- Connects to various directories such as LDAP, OAuth systems (including HR Systems), and existing databases
- Enables API level access to customized pages, and provides service-flow level usage
- Offers auditing and compliance reporting

Security Features

Neutrinos complies with and accelerates the implementation of enterprise security requirements such as:

- Identity and access management
- Security compliance
- Single sign-on
- Auth strategies
- App security checks

- Role-based access control
- Auditing
- Encryption
- Vulnerability checks
- App deployment

Identity Management

Identity and access management of the components as well as the applications built using the Neutrinos Platform is handled by the **Neutrinos Identity Server (IDS)** which is a standards-compliant OAuth 2.0 authorization standalone and a certified OpenID Connect provider.

The OAuth 2.0 protocol provides API security via scoped access tokens. The OAuth connection uses TLS 1.2 and the connection is encrypted and authenticated using AES 128 and RSA key exchange mechanism.

Security Compliance

Neutrinos is OAuth 2.0 and LDAP compliant.

OAUTH 2.0 Compliance

OAuth 2.0 is an industry-standard protocol for authorization. The protocol focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.

Neutrinos hosts its own OAuth strategy called the Neutrinos Auth strategy using the Neutrinos IDS and also allows integrating with existing Google OAuth provider of an enterprise to authenticate and authorize apps. Thereby providing centralized enduser authentication with your existing identity management systems.

LDAP Compliance

Lightweight Directory Access Protocol (LDAP) is the industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol. It plays an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.

Neutrinos is LDAP compliant. It provides a simple configuration setting that takes less than 10 minutes to integrate with Active Directory and Azure AD to manage users and groups as well as to manage resources on deployment environments like Development, Testing or Production

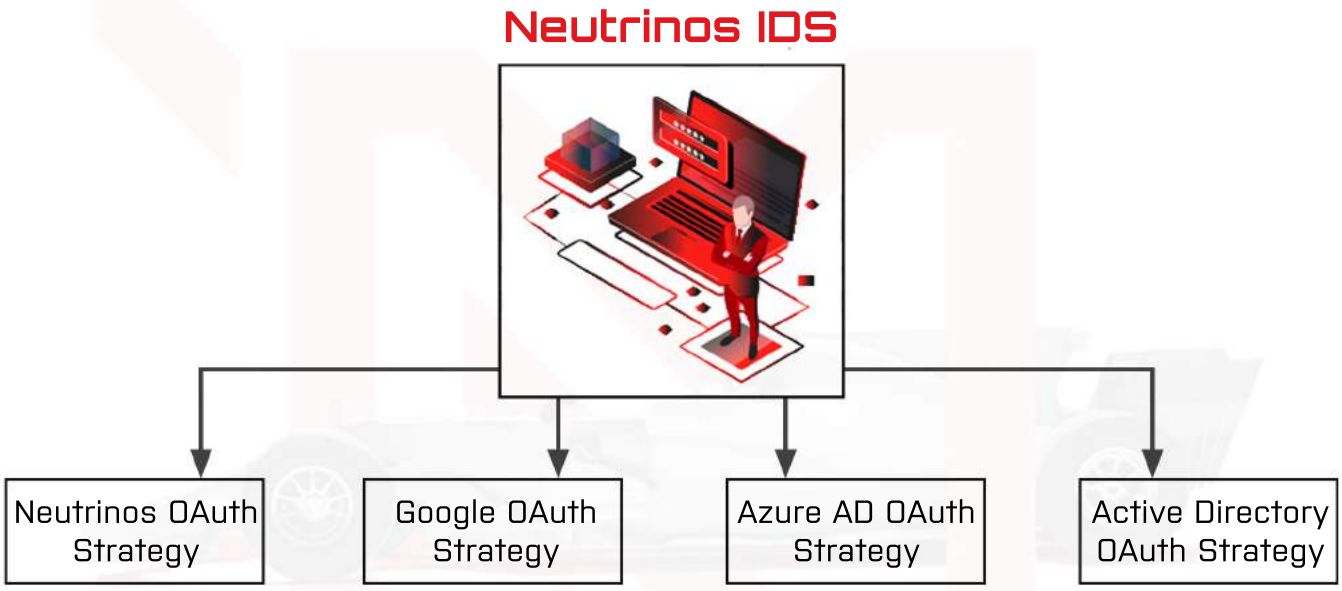
Single Sign-On (SSO)

Single Sign-on allows an enterprise authentication system to securely store and own all of the user credentials.
The Neutrinos SSO capability allows developers to easily unify logins across applications. A user can move seamlessly between applications without requiring any additional login.

The Neutrinos IDS provides user authentication and SSO functionality by maintaining all user's information on **Neutrinos**. Console is seamlessly integrated with the IDS and grants user tokens to control authorization and authentication of apps.

Auth Strategies

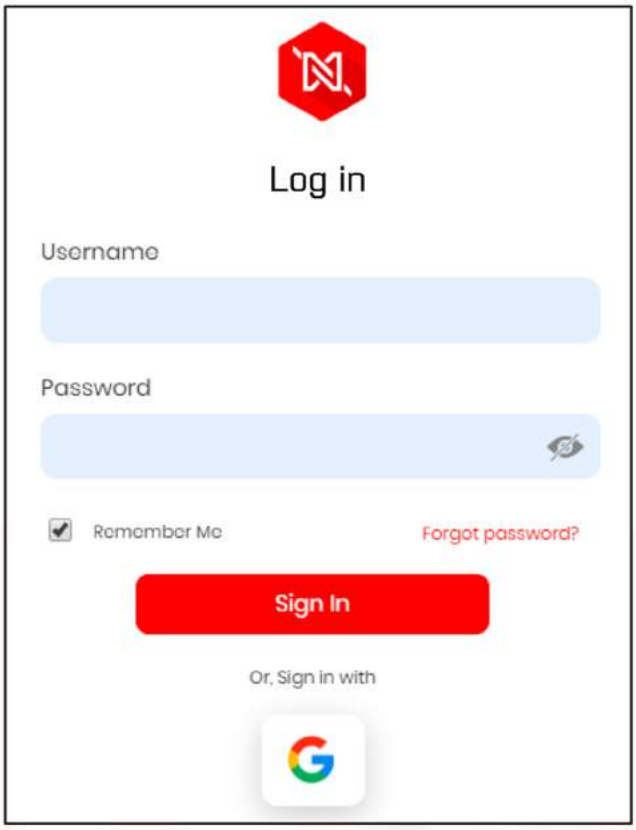
Neutrinos provides seamless integration with your existing Auth Strategies.



This reduces a huge overhead on the developer of implementing an SSO solution.

The development efforts of integrating Active Directory and Azure AD to your application is reduced from 5 working days to just 10 minutes. The development efforts of Integrating your app with Google Authentication is reduced from 10 working days to 10 minutes.

Based on the auth strategy you choose, the end user will be displayed with options to login to the app. For example, if Google auth strategy is enabled, the app login screen will show the sign-in with Google option, which when clicked will allow you to login with your Gmail credentials and logs you back to the application



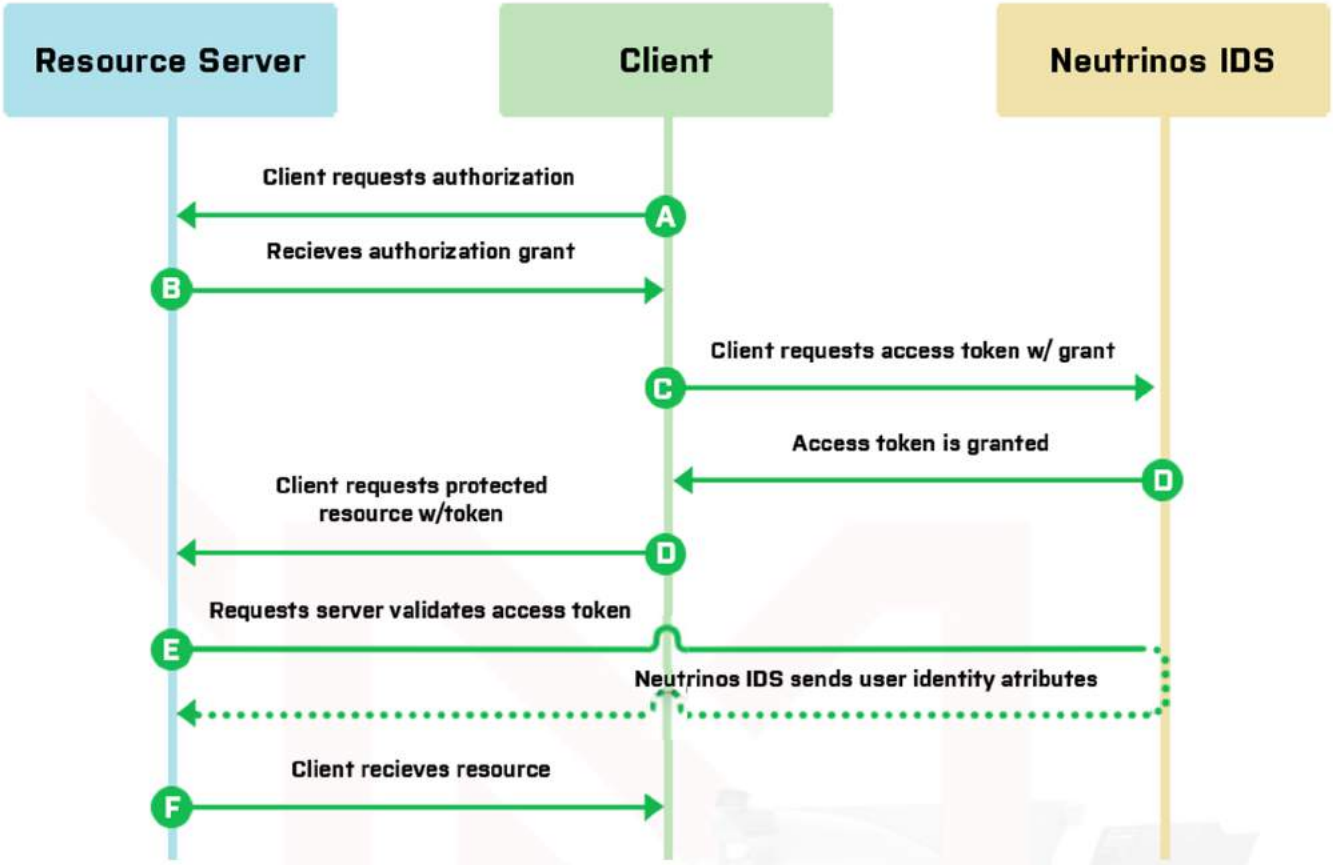
Behind the Scenes

This is what happens internally when you try to log in to an app or website created using Neutrinos Platform:

Step 1: The Neutrinos IDS server first checks to see whether you've already been authenticated. If you have, it gives you access to the app or the website.

Step 2: If you haven't, it asks you to log in and checks your username and password against the information in the database. Or, if you are using any external OAuth provider such as Google, the OAuth provider takes care of the authentication. After the authentication of the user, the Neutrinos IDS takes care of the authorization of the user.

Step 3: After authentication and authorization, you will be taken to the app or the website.
The authentication verification data is usually on the server side and the browser sends the cookies to the server for session validation.



The encrypted secure session tokens can be configured for session expiry according to customer's needs (from minutes to hours) and enables sessions restrictions. IP address restrictions are supported per custom requirements.

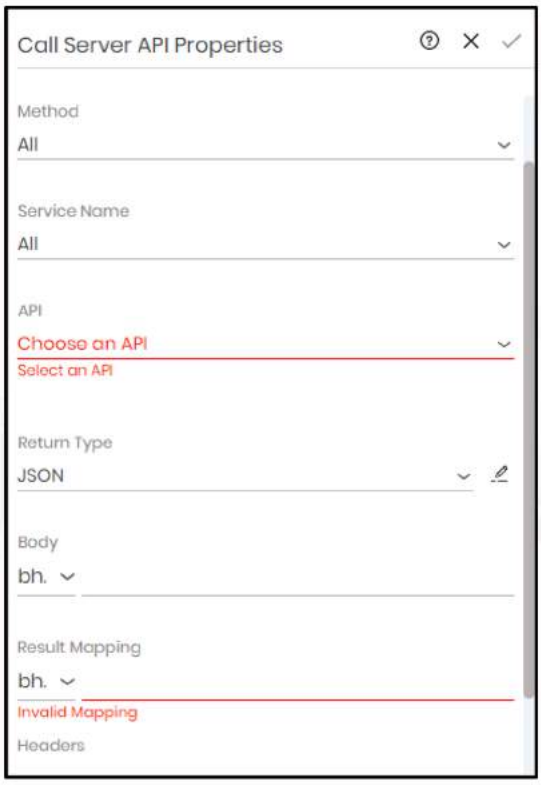
Developers using the Neutrinos platform to develop their applications can introduce customized multi factor authentication (MFA) within their application by using reusable widgets like the Finger Print Authentication widget which is available on the Neutrinos Store (Marketplace) combined with the business logic developed using Services Designer of Neutrinos.

MFA combined with directories integration (AD, Azure AD) allows for tiered access to applications and platform resources.

App Security Checks

Neutrinos Studio, the IDE for app development, warns the developer at design-time about potentially unsafe application patterns and incorrect configurations. It provides exception handling and logger settings for the server apps and allows you to configure errors and hints while developing apps.

It also validates the user input for each component before saving it.



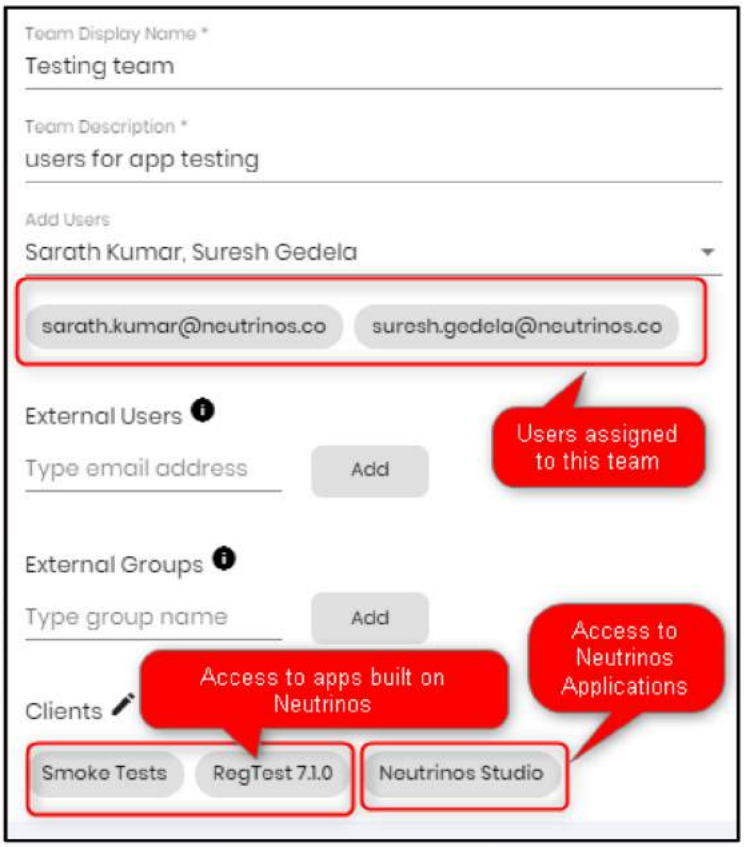
This features also enables API level access to customized pages, and provides Service-flow level usage.

Role-based Access Control

Role-based access control restricts access to your application's pages depending on specific application level roles. It also restricts access to Neutrinos Applications such as access to Neutrinos Console, Studio, etc.

You can define application-level permissions using Neutrinos Console and create different teams with different access rights.

The example below shows how Neutrinos enables teams to visually set user profile access rights and enable authentication of Neutrinos applications and apps built on Neutrinos:



After the users are registered to use an application, role-based access control ensures that only authorized users are allowed to perform specific business functions.

Auditing

Neutrinos provides you with highly effective audits that helps you quickly track down security threats. The platform traces the user's usage of the number of logins and access to various parts of the platform.

- It provides code traceability by providing error logs, comments, and exceptions on the code that is generated.
- It enables controlled configuration management by providing integration to the source code control of user's choice.
- It also provides audit trail traceability through role-based access control and secure session-based access on the platform.

Encryption

Neutrinos strengthens data privacy and confidentiality by providing encryption of sensitive data. It supports customer-controlled encryption key lifecycles by creating custom modules for encryption as per the customer requirements.

In addition, the platform also provides user authentication combined with networklevel security by IP address and session restrictions. Sessions restrictions are implicit on the platform and IP address restrictions are supported as per custom requirements.

Vulnerability Checks

Neutrinos uses secure code patterns that protect applications from common web and mobile vulnerabilities.

During app deployment, Neutrinos security checks proactively warn developers of potential security issues as they publish their applications.

For Example:

- Cross-site scripting attacks are handled by implementing input validation in the Neutrinos web application parameters and by implementing HTML encoding to sanitize user inputs.
- The number of request attempts to reset password is handled by implementing the reCAPTCHA feature to limit the password reset requests and by implementing password reset mail restrictions.
- CORS misconfiguration and blocking of third-party miscellaneous sites is handled by using a whitelist of allowed domains to acces and share resources.

When new code vulnerabilities are found in generated code, Neutrinos fixes them in subsequent releases. Apps can automatically incorporate the new security fixes after upgrading their current releases, reducing the customer cost of maintaining apps built on Neutrinos.

App Deployment

Cloud deployment of apps built on Neutrinos Studio is hosted on the Google Cloud Platform(GCP), and can thus leverage the benefits of Google Security. Apps can also utilize other benefits of the Cloud platform such as auto-scaling, auto-provisioning, auto-healing, etc.

Neutrinos supports a large variety of deployment options that allow you to run your apps on a public, virtual private, private, hybrid, or multi cloud or via a traditional (virtual) server.

Conclusion

Neutrinos Platform supports or permits users and applications to share a single, common infrastructure and code base. This is achieved with the help of the Neutrinos IDS which:

- Allows role-based Authentication and Authorization to access all platform components and parts of the platform
- Provides Single Sign on to all platform components thus permitting all authorized users to share common code base
- Provides federated outputs.
- Accelerates your app development experience by allowing seamless integration to any external OAuth provider.
- Accelerates user adoption of apps by providing a more positive experience and reducing password fatigue.
- Reduces overhead on the developer of implementing an SSO solution for the enterprise apps.
- Lowers customer support costs by dramatically reducing pass word-related support calls.
- Simplifies username and password management by reducing both IT efforts and opportunities for mistakes.

Read More

Simplifying Single Sign-on with Neutrinos identity server-
https://www.neutrinos.co/simplifying-single-sign-on-with-neutrinos-identity-server/

Configure your Application to use an Identity Server-
https://www.youtube.com/watch?v=JHDA07jeGg4&t=36s

NEUTRINOS

Neutrinos is a Multi-experience Development company that offers a platform to ideate, transform, and build complex enterprise applications within days – or sometimes hours. Neutrinos is headquartered in Singapore and has operations across South Africa, South East Asia, India, and the USA.

comms@neutrinos.co

www.neutrinos.co