FLEXIBLE MULTI-FACTOR AUTHENTICATION

ASCENDID - SECURE, SIMPLE, UNIFIED.

AscendID is a fully automated cloud service, providing strong multi-factor authentication, simplified, unified administration at significantly reduced TCO.

It can be a challenge to protect your organisation's confidential information and infrastructure, yet enable authorised users to access all the resources they need, no matter where or when. Multi-factor authentication cloud service from AscendID can satisfy your compliance needs.

AUTHENTICATION IN THE CLOUD

AscendID deploys and manages a distributed estate of tokens securing cloud, on-premises and virtualised resources.

AscendID offers extensive authentication options including truly frictionless behavioural biometrics that leverage keystroke dynamics, swiping patterns and more, user-friendly fingerprint and facial biometrics and other proven multifactor solutions as well as a suite of innovative e-signature products - like CRONTO® graphical cryptograms.

THE COMPLETE SOLUTION

Deployment of AscendID typically takes hours rather than weeks, and no infrastructure resources are required.

With existing token investment leveraged rather than discarded, the benefits of AscendID's lower operational costs and management simplicity can be achieved immediately.

Flexible and scalable, AscendID delivers strong authentication with ease of administration. Single Sign-On (SSO) is supported, allowing access from diverse end-points, including desktops, laptops, tablets and smartphones. The service integrates seamlessly with a broad range of leading vendor solutions.

AscendID's extensive feature set includes broad APIs, automated workflows, vendor-agnostic token support and tailorable administration processes.

OUTSTANDING USABILITY

- Static, lost or stolen password problems eliminated, reducing help desk call rates.
- Flexibility, protecting every access point, including critical portal sites, SaaS solutions, and eBusiness and eCommerce applications.
- Unrivalled seven-year battery life and two-year warranty on hardware tokens as standard.
- Natively integrated application security technology that dynamically monitors application execution to detect and prevent attacks on mobile applications.
- Multi-tenanted certified UK data centres.
- Full SAML 2/SOAP integration.
- Cost-effective service, offering significant TCO savings over inhouse solutions.
- Web app SSO (Single Sign On).
- Flexible service inclusions, contract lengths and billing options.
- Fully SLA-backed service.
- Fully integrated with diverse services, including Office 365, Amazon cloud, Google Docs, Salesforce.com , Box, DropBox and Concur.
- Multiple plugins supported, including Microsoft IIS web server, Sharepoint, Outlook Web Access, Citrix Storefront, Remote Desktop, and Support of Office365 via ADFS3.0/4.0 and SBR.
- 36 pre-built reports available, ad hoc or scheduled, in PDF, HTML or XML format, and customized reports are available.
- Live service evaluations to enable power users and senior IT staff to prove the concept fully, before investing.
- High-Availability Architecture with an uptime exceeding 99.995%.
- AscendID‘s servers are hosted across independent PCI DSS and ISO-27001 Tier-3 aligned UK based Datacenters ensuring data security and sovereignty within the UK.

DEVICE-AS-A-TOKEN

Software solutions for all major smart devices platforms, and Windows.

CONTEXT-BASED AUTHENTICATION

Convenient, cost-effective secure remote access, with tokenless strong authentication.

PRIMARY AND EMERGENCY

via SMS and email makes OTP delivery easy and convenient which requires no software installation.

PUSH NOTIFICATION

Device-independent push notification that securely sends Secure Messages content between AscendID cloud and mobile device including alerts, transactions, and authentication data.

> AscendID security has greatly simplified the management of multi-factor access allowing us to focus on more strategic initiatives.

FACIAL BIOMETRICS

Your end users can experience truly frictionless and secure authentication using the latest Face Recognition technology.

WIDE RANGE OF MULTI-FACTOR AUTHENTICATORS

AscendID's authenticators include smartcards, audio and large button tokens for the visually impaired, and Challenge and Response Authenticators. AscendID delivers the broadest choice when it comes to access security methods so you can meet the needs of any user and any risk level (hardware or software, certificate-based authentication or traditional one-timepassword, SMS, and Push Notification)

ADMIN AND HELPDESK DASHBOARD

All administration functions are available through an intuitive web-based user interface. A dedicated overview of frequently-used functions empowers helpdesk staff to deliver end user support in the most cost and time efficient manner.

SELF MANAGEMENT

AscendID's self-service portal allows end users to self-assign and independently activate their tokens, at their convenience and without administrative intervention. This allows users to register and autoassign hardware or software tokens, enabling companies to efficiently deploy large volumes of tokens in just minutes.

Other user benefits include:

- User registration and auto assignment
- Authenticator activation
- Authenticator assignment
- Authenticator management (login test, PIN change, unlock)
- Virtual OTP (one-time password) requests
- Updates to users' Windows Active
- Directory passwords

INTER-OPERABILITY AT THE FRONT END

Relying on non-intrusive authentication enablement, AscendID can be integrated, using RADIUS, with Microsoft IIS-based applications such as Outlook Web Access, Citrix StoreFront and Microsort RDWeb Access, and, using SOAP, with any other Internet application. Additional modules are available for direct plug-in to various 3rd party systems, including Juniper SBR and Microsoft ADFS3.0.

MARKET LEADING TECHNOLOGY

- Physical tokens
- Soft tokens for iOS and Android
- Push notifications
- Biometric support
- Integration with leading SaaS applications
- Active Directory Integration
- User self-enrollment
- Auditing and Reporting

AUDITING AND REPORTING

Statistics gathered by the audit console as it monitors incoming and outgoing events provide the information necessary to effectively manage the remote access environment. Extensive XML or HTML formatted reporting is provided for helpdesk troubleshooting, as well as system and security auditing and accounting purposes.

Protect the Users in your organisation from data breaches with multi-factor authentication. Whether on-premise, in the cloud or both, AscendID provides multi-factor authentication (MFA) and single sign-on (SSO) solutions using multi-layered Adaptive Authentication with a frictionless user experience.

- Verify users with a wide range of multi-factor authentication methods: Push, Risk-Based, Hard Tokens, SMS, Face and Finger Biometrics, and more!
- Easily integrate multi-factor authentication (MFA) with all your corporate resources: VPNs, applications, and encrypted data files.
- Enforce access policy across your on-premises and cloud environments.
- Simplify login by offering a single sign-on (SSO) portal to all your cloud applications.

Security assurance is paramount to device and application reliability, and user peace of mind. Multi-factor authentication via notification and push, tokens, SMS and biometrics form the basis for corporate resource protection, such as virtual private networks and encrypted data files as well as applications and devices. With a single sign-on portal you can enforce access policy across your on-premises and cloud environments via a simplified login.

AscendID Access Gateway allows users to log in once to access all enterprise cloud applications from a single web portal. Unlike other single sign-on solutions, AscendID checks a user's identity and device health every time they access an application, without using an agent.

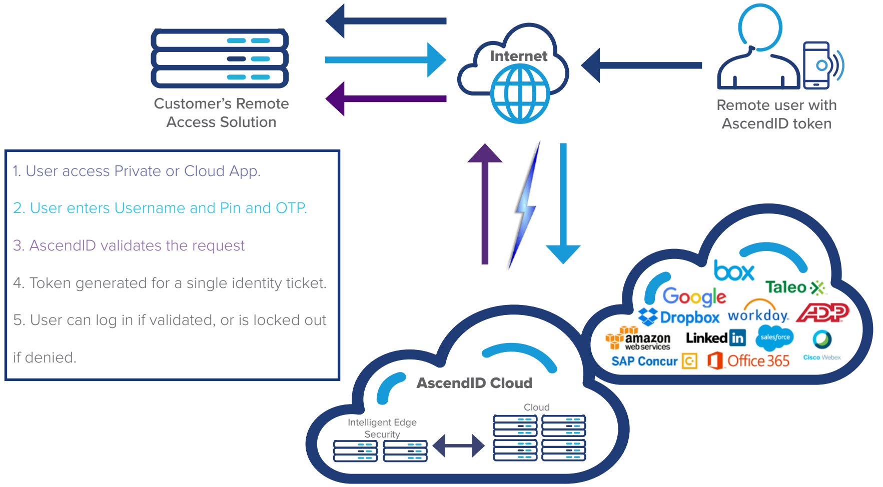
Protection covers:

Google Apps, Amazon Web Services, Box, Salesforce and Microsoft Office 365.

Support covers:

Security Assertion Markup Language (SAML) authentication standard, and a variety of Identity Providers (IdPs), including Active Directory, OpenLDAP, Google OIDC, Azure OIDC and SAML IdPs.

> AscendID has solved the issue of enforcing security on devices and services that have no user enforceable password policies with an easy to use, user-friendly service that integrates into nearly all devices.



1. User access Private or Cloud App.

2. User enters Username and Pin and OTP.

3. AscendID validates the request

4. Token generated for a single identity ticket.

5. User can log in if validated, or is locked out if denied.

COMPLIANT AND SECURE

CONTACT OUR SECURITY & COMPLIANCE TEAM

Technology has never evolved faster. Data has never been more valuable. Or so desired. From the moment customers provide their data over the phone, your organisation is vulnerable to cybercrime, data breaches and leaks. Contact centres must mitigate the risk: protect their reputation; protect their customers. Our experts have developed a suite of services to demystify the complexities of compliance and add certainty to service – enhancing your security and meeting regulatory obligations without ever compromising on the customer experience.

Secure

Assured and encrypted solution

Automated

Cloud and on-premises service

Authenticate

Non-intrusive and easily integrated

Accessible

Frictionless user experience

GET IN TOUCH

IP Integration Ltd
Integration House
Turnhams Green
Business Park
Pincents Lane
Reading, Berkshire
RG31 4UH

0118 918 4600

enquiries@ipintegration.com

www.ipintegration.com

linkedin.com/company/ip-integration

https://twitter.com/ipiltd