DATASHEET

LTS SECURE ACCESS MANAGEMENT

One system to rule them all: users, devices, things, applications, and services

Our approach to access management? One system to download and deploy, complete with comprehensive access management capabilities. Say goodbye to integrating a grab bag of disparate products. Modern identity solutions need to employ a light touch when dealing with users, devices, services, and things, all while providing the highest possible security. Organizations need to deliver a rich and personalized experience and to provide modern, contexual authentication, as well as fine-grained authorization to protect and secure resources. They have to be able to provide identity and access services that are continuously secure, scalable, and can adapt to rapidly evolving demands.

LTS Secure Access Management, built from the lasted next generation technologies, provides the most comprehensive and flexible set of services required for consumer facing access management, as well as traditional access management capabilities. These services include authentication, mobile authentication, adaptive risk assessment, authorization, federation, single sign-on, social sign-on, basic self-service, privacy and consent, and high performance session management.

LTS Secure Access Management is part of the LTS Secure IDM & CASB Suite, the only commercial CASB offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform. The solution is built on a highly scalable, modular, extensible, and easy-to-deploy architecture. Context-aware capabilities enable your employees, customers, or citizens a personalized experience on any digital channel, whether a mobile device, connected car, home appliance, or whatever the next connected car, home appliance, or whatever the next connected innovation might be.

Features	Benefits
Advanced Authentication	■ Leverage contextual authentication to assess risk, invoking stronger authentication mechanisms only when necessary by evaluating who the user is and their context. ■ Updated, easy-to-use LTS Secure Mobile Authenticator app for iOS and Android provides one time passwords and push notifications. Or take the app source code and integrate directly into your own mobile applications. ■ Drive new customer adoption with social authentication, removing the need to complete lengthy registration forms.
Mobile Authentication	■ Enable passwordless logins using the Push Authentication feature with iOS and Android devices. ■ Provide frictionless multi-factor authentication using Push Authentications. ■ OATH and HOTP standards that allow one-time passwords on a mobile phone or other device to be used as an additional factor for authentication.
Authorization	■ Create sophisticated, context based and intelligent policies to deliver controlled access to resources with the GUI-based policy editor, using point and click, drag and drop operations. ■ Scripting can also be used to extend logic during policy evaluation to any resource type, not only URLs but external services or IoT devices and things.

HIGHLIGHTS

- "All-in-one access management solution that includes authentication, adaptive risk assessment, authorization, federation, single sign-on, social sign-on, basic self- service, privacy and consent, and high performance session management.

- Mobile authentication, including Push Authentication feature to verify users without the need for passwords, and multi- factor authentication capabilities, with an easy to use mobile app for iOS and Android.

- Easy configuration of authentication and authorization with the flexibility to manage users, devices, services, and things.

- Fine-grained and continuous authorization leveraging a powerful policy engine, configurable with an easy to use policy editor, extensible with JavaScript and Groovy, and consumable through policy REST APIs.

- View and analyze logging and audit information across the platform using the Common Audit Handler, now including support for Elasticsearch in the ELK stack.

- Flexible stateless and stateful architecture designed for the demands of large scale and elastic deployments such as DevOps environments with microservices, and IoT.

LTS Secure

Features	Benefits
Federation Management	■ Leverage standards to deliver seamless federation across organizations. ■ Incorporate SAML2 federation into authentication chains, enabling the use of federated identities in stronger multifactor authentication scenarios. ■ Supports OpenID Connect which makes it easier and faster to build solutions requiring additional identity information.
Single Sign-On	■ Provide Single Sign-on (SSO) services for multiple resources on one domain, across domains, or even across organizations, allowing the use of just a single authentication credential to access all resources.
Social Authentication	■ Drives new customer adoption by removing the friction of registration process in addition to simplifying sign-in.
Session Management	■ Highly flexible session management enables both stateless and stateful sessions. ■ Stateless session management allows for highly distributed deployments with nearly unlimited horizontal scalability, an ideal choice for securing microservices architectures. ■ Stateful session management enables complex, multi-site failover environments to be always available to end-users with very high uptime.
Shared Services	■ The Common Audit Framework provides a means to log data consistently across the LTS Secure Identity Platform, and enables correlation of events and transactions. Audit topics, such as access and activity, can be configured independently delivering the data you want to the appropriate business services. Includes handlers for CSB files, JDBC connections, Syslog, JMS and Elastic-search (part of the ELK stack). ■ Shared services can log and track transactions; used to build custom UIS; develop scripts using JavaScript and Groovy; and provide user self-services across the entire platform.
Developer Support	■ Develop against the platform's common RESTful APIs that enable JSON or XML over HTTP, allowing access to all the underlying authentication, authorization, and identity services. Also available java & CAPIs. ■ Secure Token Services automatically translates protocols for providers who support different standards for federation and authentication.
Performance, Scalability, High Availability, Elasticity	■ Support large-scale, highly available implimentations with millions of users, tens of thousands of concurrent sessions, and thousands of authentications per second. ■ An idea choice for securing high volume microservices environments with expanded stateless session support. ■ Leverage the embedded Lts Secure Directory Services as a configuration store, highly scalable and performent session persistent token and user store.
Standards	■ All major federation protocols: SAML 1.x SAML 2.0 (SP, IdP, ECP, and IdP Proxy), WSFederation (asserting, relying party). ■ Next gen-federation standards for cloud and mobile, including full implementation of OpenID Connect, OAuth 2.0, GSMA, and UMA (consumer, provider, authorizatin server), ensuring greater interoperability and consistent behavior for developers. ■ Export and import of policies via XACML.

To know more about LTS Secure, visit this website. http://www.ltssecure.com/

LTS Secure