DATASHEET

LTS Secure IDENTITY MANAGEMENT

Comprehensive & Secure Identity Management

Ensure that all cloud apps, On Premise Applications, IoT Devices and on Mobile leverage a single identity store. LTS Secure Identity Management is an administrative area that deals with identifying individuals in a system (an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Allows you to comprehensively and securely manage the complete identity lifecycle of users, devices, and things. From identity to device registration, provisioning, synchronization, reconciliation, and more, your users and customers can feel safe as they move between devices and services

Along with LTS Secure Access Management, LTS Secure Identity Management has the potential to provide greater access to organizations, which can drive productivity, satisfaction and, ultimately, revenue. At the same time, it keeps a record of the identity of every individual in order track his activity and check who is misusing his/her access related privileges.

Features	Benefits
Role-based Provisioning	■ Create and manage roles assigned to users based on organizational need and structure such as job function, title, geo, etc. Assign and remove entitlements and resources consistently and rapidly.
REST API	■ Comprehensive and simple RESTful interfaces provide an API for managing all core functions of user admin, sync & reconciliation, and the decoupled UI enables custom-tailored solutions with sample configurations for scalable user administration. ■ Pluggable server-side scripting engine provides Javascript and product-wide Groovy support out of the box for extensibility and customization.
Flexible Data Model	■ Supports choice of data model to meet the needs of your deployment – either a data full model for current data or data sparse model for faster access. The object-based model isnot hard-coded and provides flexibility to define many different schemas, objects, attributes, and relations.
Password Management	■ Ensure consistency across all applications and data stores, such as Active Directory and HR systems. Password policies enforce access rights with rules that can specify strength, aging, reuse, and attribute validation.

HIGHLIGHTS

- The only identity management solution on the market purpose-built for users, devices and things.
- Address privacy compliance throughprofile management by offering users the ability to configure privacy settings such as consent, and opt-in and opt-out.
- Improve registration rates with social registration and login options by utilizing standards based social IDPs such as Facebook, Google, and LinkedIn offered out-of-the-box. Additional OAuth2 standards based social providers can be plugged-in.
- Web scale architecture that is proven to support millions of identities, provisioning thousands of identities per second with high availability.
- Visualize identity relationships through the LTS Secure Identity Management, management console.
- Manage constantly changing digital relationships including user to user, user to thing, thing to thing, and more through intuitive admin UI and end-user dashboards
- Lightweight RESTful model provides developers with an agile approach to build out custom identity workflows with minimal effort using industry standards JavaScript and Groovy.
- Offers many out-of-the-box connectors for integrating across traditional on-premises systems as well as cloud applications such as Google Apps, Azure, Office 365, Workday, Salesforce, and Marketo.
- Deploy on-premise or in the cloud, including AWS, Azure and others.

Features	Benefits
Cloud SaaS Connectors	■ Simplifies connectivity to cloud-based SaaS resources such as Salesforce, Microsoft and Google Apps with out-of-the-box connectors. ■ Centralized management of identity data across resources guarantees consistency with ability to synchronize and reconcile bi-directionally, on-demand or as a scheduled update.
Synchronization and Reconciliation	■ Synchronization delivery guarantees enable roll-back if one or more remote systems are unavailable, for both on-demand and scheduled resource comparisons. ■ Reconciliation discovers new, changed, deleted, or orphaned accounts to determine user access privileges to detect and synchronize changes to accounts, entitlements, and passwords, and perform user access remediation tasks.
Data Model Visualization	■ Visualize identity relationships through the LTS Secure Identity Management, management console. Plus build customized dashboards, integrated with Kibana, that include bar, line, scatter plots, and pie charts that give shape to the data that LTS Secure Identity Management is handling.
Shared Services	■ The Common Audit Framework provides a means to log data consistently across the LTS Secure Identity Platform™, and enables you to correlate 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 CSV files, JDBC connections, Syslog, JMS, and Elasticsearch (part of the ELK stack).
Self-Service & Profile Management	■ User self-service significantly reduces help desk costs and increases user productivity by automating password reset and ensuring compliance with a secure, centralized password policy. ■ Allows end-users to create and manage profiles, configure privacy settings, and give consent for data-sharing.
Social Registration & Authentication	■ Accelerates registration and login by using any social IDP that supports OpenID Connect or OAuth 2.0 such as Facebook, Google, and LinkedIn to gain insight and build common user profiles for a centralized single view of the customer.
Workflow Engine	■ Provides workflow-driven provisioning activities, whether for self-service actions such as requests for access,or for admin actions such as updating entitlements, on/off boarding, bulk sunrise or sunset enrollments,handling approvals with escalations, or performing maintenance. The embedded Activiti engine supports BPMN 2.0 for standards based business focused management.
OpenICF Connector Framework	■ Leverages the new OpenICF 1.5 framework (Open Source Identity Connector Framework) for resource connector development, including amongst others, a PowerShell Connector, a Generic Scripted Connector that allows for integration with anything that Groovy supports; REST, SOAP, JDBC, JSON etc.

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

LTS Secure