CA API Gateway Simplifies Enterprise BYOD Mobile Access



Empower Mobile Employees with Secure Access to API-Driven Data & Functionality

The CA API Management Suite delivers a comprehensive family of solutions architected to secure enterprise APIs in a reliable and manageable way. It provides tools to address mobile app development and bring your own device (BYOD) as well as partner and cross-divisional SOA integration and API developer onboarding. From OAuth implementation to API traffic management, CA API Management Suite helps simplify the process of adapting data for mobile consumption while maintaining a productive and secure environment.

The Problem

The "bring-your-own-device" (BYOD) movement within enterprises is gaining traction as more and more employees are using their own mobile devices—from iPads to Androids to iPhones—to access corporate data and applications. At the other end of the spectrum, forward-thinking companies that want to realize the benefits of having an empowered mobile workforce have already begun providing their employees with tablets. All of these users are now starting to demand line-of-business applications that can help them be more productive and efficient when they are out of the office but IT still has to ensure that security and privacy are maintained.

How can you facilitate the creation of mobile applications to empower your field workers while still providing for security?

The Solution: CA API Management Suite

The CA API Management Suite empowers enterprises to provide the resources developers require in order to quickly build out mobile applications against enterprise APIs that securely deliver corporate data and functionality to mobile devices. CA Technologies also simplifies the process of adapting data for mobile consumption by transforming it to a compressed JSON format and providing security features such as data encryption and redaction. The CA API Management Suite comprises:

- CA API Gateway Provides enterprise-grade API security and traffic control
- CA API Developer Portal Streamlines developer onboarding and management, as well as API reporting
- CA Mobile API Gateway The power of the CA API Gateway plus an SDK to enable enterprise-grade SSO for mobile users
- Enterprise Service Manager Enables API migration and lifecycle management
- OAuth Toolkit Simplifies the implementation of two- and three-legged OAuth

Of course, mobile-resident applications will do little more than create islands of information if they cannot securely connect back to the enterprise's systems of record. Therefore, CA Technologies provides the ability to:

- Layer on screening for threats and enforce data privacy
- Authenticate and authorize against a corporate IAM system
- Track and log all interactions originating from the field

Enable Mobile Developers	
API Documentation &	Provide versioned documentation to help mobile developers quickly understand how to use your APIs
Resources	Provide resources such as sample applications, code libraries and sample requests/response pairs
API Key Management	Optionally gate the generation of API keys/OAuth secrets for each developer application Create, assign, suspend and revoke API keys
Registration	 Register, approve and manage third-party organizations, partners and internal developers Manage users with built-in role-based access control (RBAC)
API Analytics	 Generate API reports that track and meter API usage, successes versus errors, latency etc. Generate application reports that show latency, usage, successes versus errors etc.
Implement Secure OAuth	
Specifications	Supports OAuth 1.0a, OAuth WRAP and OAuth 2.0 Provides sample two- and three-legged OAuth implementations that can be configured to your needs
Encryption	 Support for TLS/SSL encryption over the wire Support for a variety of cryptographic algorithms, including HMAC, RSA and SHA Support for asymmetric signatures using RSA
Security Token Service (STS)	Built-in STS can issue and validate OAuth access tokens, optionally with HMAC or RSA signature methods and SHA-1, SHA-256 or SHA-512 encryption
Simplify API & Data Security	
Security & Compliance	 Powerful message content filtering, redaction and encryption tools help identify and suppress leakage of sensitive information (credit card numbers etc.) PCI-DSS installation and configuration guide makes it possible to configure and deploy the API Proxy as part of a PCI-compliant process
Threat Protection	 Protect against cross-site scripting (XSS), SQL Injection, XML content/structural threats and viruses Protection from common Web-based attacks, including cross-site request forgery (CSRF), man-in-the middle and message replay Track failed authentications and/or policy violations to identify patterns and potential threats Validate HTTP parameters, REST query/POST parameters, JSON data structures, XML schemas etc.
Adapt APIs	
API Aggregation & Orchestration	 Create and expose virtual APIs tailored to specific consumers/formats, like mobile Sequence backend calls and aggregate responses to provide richer results from a single query
API Transformation	Transform legacy API and data formats (such as SOAP and XML) to REST and JSON
Compression	On-the-fly gzip compression reduces response size
Manage APIs	
API Lifecycle	 Automated migration of API policies between environments (from dev to test, east to west etc.) with full dependency resolution decreases migration risk Support for automatic API versioning, including rollback to any previous version Global security settings, threat detection profiles etc. can be reused across multiple APIs to save time and ensure consistency
SLA/Performance Control	 Enforce availability through throttling and/or rate limiting to ensure SLAs and quality-of-service priorities Prioritize traffic to specific APIs based on SLAs Limit API access based on user, time of day, IP address etc. Route traffic based on geography, IP address, backend response times etc. for optimum performance Define custom data and identity caching parameters for optimal performance tuning
Auditing/Logging	Log files provide a granular audit trail of all API connections mediated by the API Proxy
Supported Standards	
XML, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, Radius, SAML, XACML, OAuth, PKCS, FIPS 140-2, Kerberos, X.509 Certificates, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, POP3, IMAP4, HTTP/HTTPS, FTP/FTPS, MQ Series, JMS, Raw TCP, Tibco EMS, WS-Security, WS-Trust, WS-Federation, WS-Addressing, WSSecureConversation, WS-I BSP, WS-MetadataExchange, WS-Policy, WSSecurityPolicy, WS-PolicyAttachment, WS-SecureExchange, WS-I, WSIL, UDDI, WSRR, MTOM, IPv6, WCF	

For more information, please visit ca.com/api

CA API GATEWAY SIMPLIFIES ENTERPRISE BYOD MOBILE ACCESS

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.