CA API Management

The Industry's Leading Products for Enterprise-Scale API Management

ca technologies®

At a Glance

Increasingly, enterprises are opening their data and applications to partners, developers, mobile apps and cloud services. APIs provide a standardized way to open up information assets across the Web, mobile devices, Service Oriented Architecture (SOA) and the cloud. However, to make API information sharing safe reliable and cost-effective, enterprises must deal with critical security, performance management and data adaptation challenges. CA makes it simple for enterprises to address these challenges.

CA API Management combines advanced functionality for backend integration, mobile optimization, cloud orchestration and developer management. It is unique in its ability to address the full breadth of enterprise API management challenges.

Key Benefits/Results

CA API Management provides solutions for:

- **Developer Access** – Empower internal and external developers to leverage your APIs.
- **Mobile Access** – Securely connect the enterprise with mobile apps and smart devices.
- **Partner Access** – Share information and services across organizational boundaries.
- **Cloud Access** – Remove barriers to adoption of SaaS applications and cloud infrastructure.

Critical Differentiators

API Management includes a range of complementary products that are delivered pre-integrated with CA API Gateway:

CA API Developer Portal – Engage, onboard and educate internal and third-party developers via a branded online interface, to facilitate the creation of applications that leverage enterprise APIs.

API Service Manager – Manage the API lifecycle from development, to test, to production.

OAuth Toolkit – Control access to API-based resources using OAuth 2.0 and OpenID Connect

Security Token Service – Simplify identity federation and Single Sign-On (SSO) using OAuth and SAML.

The Role of Identity in API Management

As the enterprise looks to embrace cloud and mobile, they are faced with some serious business challenges, starting with the key issue: how do they maintain control over corporate apps and data once these leave the business? Additional challenges include:

Opening on-premises data and applications to third parties. Opening on-premises data and applications to third parties via APIs raises a range of serious security concerns. Additionally, API publishing creates challenges around ensuring scalability and manageability as adoption grows and adapting data for consumption by a range of constituents.

Protocol orchestration. As businesses migrate to the open enterprise model, there is a need to connect disparate data/applications across a multitude of environments—legacy to the cloud to mobile. The ability to connect these different solutions, their identity management, their protocols, and their data into a seamless solution is crucial.

Manageability. One of the biggest challenges that businesses face is how to manage a framework that consists of legacy solutions and open solutions—across data centers and the cloud. Further, any new solution must integrate with corporate reporting/analytics/BI tools inside the enterprise.

Solution Overview

CA API Management offers unmatched flexibility, performance and security. Available as hardware appliances or virtual machines, for deployment on-premises or in the cloud, they represent the best solution for securely exposing enterprise data and services.

CA API Management includes:

- **CA API Gateway** – Deploy the core functionality needed for enterprise-scale API security and management. Available in multiple editions to meet your specific needs.
- **CA Mobile API Gateway** – The power of the CA API Gateway with additional enhancements to power your mobile solution. Includes an SDK that enables enterprise-grade SSO (with integration with OAuth and OpenID Connect) and geo-location support, as well as security management of mobile devices – including Samsung Knox integration.
- **CA API Developer Portal** – A centralized portal that allows enterprises to engage, onboard, educate, and manage internal or external developers, publish APIs for consumption (e.g., documentation, code examples and grouping) and provide full analytics on API usage/performance.

CA API Gateways	
API Proxy	• Implement enterprise-grade threat protection and access control for APIs • Simplify the process of API composition, orchestration and lifecycle/performance management • Track API performance and generate an audit trail of all service interactions
XML Firewall	• Create SSO for SaaS applications and other cloud services • Securely integrate cloud services with on-premises IT systems • Track usage of cloud services to ensure compliance with regulatory requirements
SOA Gateway	• Enable secure SOA integration, partner connectivity and cross-departmental information sharing • Compose, edit, customize and enforce SOA Governance policies from a single, central location • Manage complex SOA architectures that span enterprise data centers and the cloud
Mobile Gateway	• Enforce access control, firewalling and data security for mobile apps that access enterprise resources • Adapt and optimize complex enterprise services for bandwidth-light mobile use cases • Securely integrate enterprise apps with the cloud, social networks and mobile notification services
CA API Developer Portal	
Developer Onboarding	• Support for both individual developers and larger partner organizations • Ability to define registrations as being automatically accepted or subject to approval • Support for both self-signup and managed enrollment
Developer Resources	• Discussion and support forums, integrated messaging etc. • API documentation, API explorer, API status, application reports etc.
Reporting and Analytic	• API reports that track and meter API usage, successes versus errors, latency etc. • Application reports that show latency, usage, successes versus errors etc.
Content Management	• Ability to define the look, feel, brand and content of the Portal • Support for both staging and production environments, as well as a content approval/publication/rollback processes, streamlining change management
Enterprise Service Manager	
API Migration	• Ability to automate the migration of API policies between environments (from dev to test, east to west etc.) with full dependency resolution, thereby decreasing migration risk • Support for automatic API versioning, including rollback to any previous version
Operational Metrics	• Configurable, out-of-the-box reports provide insight into API performance, making it possible to meter and track API/method usage for per-user billing, capacity planning, SLA compliance etc. • Real-time monitoring dashboard provides insight into API Gateway and network performance
Reporting and Analytic	• Ability to create changes to API policies and push them out to all Gateways in the enterprise
OAuth Toolkit	
Specification	• Supports OAuth 1, OAuth 2, and OpenID Connect • Provides sample OAuth implementations that can be
Security Token Service	
Specification	• All Gateways include a built-in STS that can issue and validate OAuth and SAML access tokens, optionally with HMAC or RSA signature methods and
Supported Standards	
XML, JSON, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, RADIUS, SAML, XACML, OAuth 1.0a/2.0, PKCS, Kerberos, X.509 Certificates, FIPS 140-2, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, POP3, IMAP4, HTTP(S), JMS, MQ Series, Tibco EMS, Raw TCP, FTP(S), WS-Security, WSTrust, WS-Federation, WS-SecureExchange, WSIL, WS-I, WS-Addressing, WS-Policy, SSecureConversation, WS-MetadataExchange, WS-SecurityPolicy, WSPolicyAttachment,WS-I BSP, UDDI, WSRR, MTOM, IPv6, WCF	

For more information, please visit ca.com/api