

# CA Mobile API Gateway



## Visão geral

O aplicativo móvel tornou-se o foco de novas oportunidades de receita, aumentando a produtividade dos funcionários e aprimorando as estratégias de negócios inovadoras. No centro desses objetivos está a necessidade de externalizar ativos de informações corporativas em formatos prontos para dispositivos móveis que possam ser facilmente consumidos por desenvolvedores móveis e os aplicativos que eles criam.

O CA Mobile API Gateway simplifica o processo de adaptação dos dados internos, dos aplicativos e da infraestrutura de segurança para uso por dispositivos móveis e na internet.

### Principais benefícios/resultados

- **Desenvolvimento rápido de aplicativos** – Adapte os serviços de back-end às APIs prontas para dispositivos móveis enquanto promove a externalização para comunidades de usuários
- **Segurança de ponta a ponta** – Proteja o aplicativo móvel por meio da transmissão para o back-end
- **Acesso conveniente** – Faça a autenticação uma vez e obtenha acesso a vários aplicativos usando Logon único e logon social
- **Proteção do back-end** – Diretivas granulares de usuários, aplicativos e dispositivos com base em riscos, com proteção contra ameaças à API
- **Desempenho otimizado** – Maximize o desempenho e garanta a escalabilidade com o cache de aplicativo, a integração na nuvem e os serviços de notificação

### Principais recursos

- **Adaptação** – Externalize serviços e dados como APIs móveis RESTful e modernas
- **Identidades e acesso** – Os protocolos OAuth e OpenID entregam recursos de autenticação de aplicativos móveis, logon social e Logon único
- **SSL mútuo** – Segurança com base em criptografia para o consumo de APIs
- **Segurança da API** – Proteja as APIs REST, SOAP e OData contra ataques de negação de serviço e a APIs
- **Otimização** – Armazene em cache as chamadas para aplicativos de back-end, minimize a largura de banda e melhore a experiência do usuário
- **Integração** – Centralize a conectividade entre redes sociais, serviços na nuvem e serviços de notificação

## Desafios de negócios

As empresas estão enfrentando uma série crescente de desafios de mobilidade ao tentar acelerar as inovações móveis e impulsionar os negócios. Aqui estão os desafios comuns na área de aplicativos móveis que devem ser superados:

**Dados inacessíveis.** Os sistemas e dados herdados são, com frequência, difíceis de serem externalizados de forma segura e confiável.

**Barreiras no desenvolvimento de aplicativos.** Aplicar a segurança dentro do processo de desenvolvimento pode significar um tempo extra significativo no ciclo de lançamento.

**A segurança como um fator de impacto na experiência do usuário.** Geralmente, a segurança pode inibir os processos de negócios e a adoção de aplicativos voltados ao consumidor.

**Gerenciamento e segurança de uma ampla gama de tipos de aplicativos.** Seja sua meta aproveitar os aplicativos web existentes, desenvolver novos aplicativos móveis nativos ou formar parcerias com provedores de aplicativos terceirizados, como o Salesforce.com, cada uma dessas metas exigirá diferentes soluções de gerenciamento e segurança.

## Visão geral da solução

**Adapte, otimize e integre com facilidade** — O Mobile API Gateway é um gateway de API de nível premium que oferece suporte a iniciativas de desenvolvimento e arquitetura de aplicativos móveis. Este gateway leve e de baixa latência é fornecido com controles integrados de segurança e gerenciamento, projetados para ajudar as empresas a expor seus ativos internos como APIs móveis com toda a segurança e confiabilidade, enquanto podem superar os importantes desafios relacionados a identidades, segurança, adaptação, otimização e integração.

**Proteja do cliente ao back-end garantindo acesso contínuo a usuários autorizados** — O Gateway vem com um Kit de Desenvolvimento de Software Móvel para desenvolvedores de aplicativos corporativos, que permite:

- O consumo seguro de APIs de back-end por meio da configuração de SSL mútua entre o Gateway e o dispositivo móvel.
- O Logon único (SSO) entre aplicativos e dispositivos móveis via sistemas de IAM corporativos ou logon social, para manter uma perfeita experiência do usuário.
- O aplicativo de referência de Logon único móvel, que organiza os aplicativos em um único console enquanto faz a integração com uma infraestrutura existente de IAM para entregar a funcionalidade de Logon único para vários tipos de aplicativos.
- A integração com o Samsung KNOX, que entrega a funcionalidade de Logon único com o SDK móvel, ao mesmo tempo em que permite aos clientes criar asserções de diretivas que requerem verificações da integridade do dispositivo e da containerização de aplicativos como condição para acessar as APIs.

Identidade	
SDK móvel	<ul style="list-style-type: none"> <li>Bibliotecas do lado do cliente, exemplos de código e documentação para ajudar os desenvolvedores a simplificar a implementação do Logon único e da SSL mútua.</li> <li>Capacidade de utilizar a segurança do sistema operacional do dispositivo para criar um recipiente de Logon único seguro.</li> <li>Fluxos de segurança com base em padrões e no OAuth 2.0, no OpenID Connect e na PKI.</li> <li>Chamada de API única para utilizar a segurança de criptografia (SSL mútua).</li> <li>Transferência, armazenamento e fixação seguros de certificados, adicionando confiança adicional à autenticação.</li> <li>Controle de acesso de geolocalização que aplica GPS, agregadores de geolocalização e coordenadas de operadoras às variáveis de contexto.</li> <li>Logon social móvel que permite que os usuários obtenham acesso a aplicativos móveis com credenciais sociais, como Facebook, LinkedIn e Salesforce.</li> <li>O Samsung KNOX Authenticator para CA Mobile SSO é um serviço Android fornecido no SDK do Samsung KNOX.</li> </ul>
Controle de acesso	<ul style="list-style-type: none"> <li>Suporte a certificados OAuth, OpenID Connect, SAML, X.509, LDAP, etc.</li> <li>Suporte à autorização de certificados SSL, Digest e HTTP básico do lado do cliente, etc.</li> <li>Samsung KNOX para APIs: asserção de diretivas (requireAttestation) para forçar o Samsung Knox Attestation Service como uma condição de acesso à API.</li> <li>Gerenciamento de recipientes e validação da integridade do KNOX.</li> </ul>
Integração de identidades	<ul style="list-style-type: none"> <li>Integração com sistemas corporativos de identidades, acesso, Logon único e federação, incluindo CA SiteMinder e o SOA Security Manager, LDAP, Microsoft Active Directory/Federated Services, Oracle Access Manager, IBM Tivoli (TAM e TFIM), RSA ClearTrust, Sun Java Access Manager e Novell Access Manager.</li> <li>Mapeamento entre tokens de acesso à web e mecanismos de troca de tokens móveis.</li> <li>Capacitação de SAML-to-OAuth.</li> </ul>
Segurança de dados de aplicativos móveis	
Proteção contra ameaças	<ul style="list-style-type: none"> <li>Validação de parâmetros de HTTP, parâmetros de REST query/POST, estruturas de dados JSON, esquemas XML, etc.</li> <li>Proteção contra ataques de script entre sites (XSS), de injeção de SQL e de negação de serviço.</li> <li>Controle as autenticações com falha e/ou as violações de diretivas para identificar padrões e possíveis ameaças.</li> </ul>
Proxy de transmissão de dados	<ul style="list-style-type: none"> <li>Protocolos proxy de transmissão móvel, como WebSocket e XMPP.</li> </ul>
Certificados de privacidade e digitais	<ul style="list-style-type: none"> <li>Instale a PKI e o gerenciamento de certificados com o HSM (Hardware Security Module - Módulo de Segurança de Hardware).</li> <li>Criptografia de curva elíptica rápida (em conformidade com os algoritmos Suite B da NSA).</li> <li>Suporte a FIPS 140-2 no hardware e no software.</li> </ul>
Adaptação e orquestração	
Orquestração de API	<ul style="list-style-type: none"> <li>Componha e orquestre APIs REST e OData de qualquer API de back-end herdada.</li> </ul>
Controles de SLA	<ul style="list-style-type: none"> <li>Controle o uso da API: limite para garantir que os serviços de back-end não fiquem saturados; limite por usuário, hora do dia, local, etc.; gerencie as cotas (por exemplo, número de usos/usuários por dia).</li> </ul>
Otimização	
Compactação	<ul style="list-style-type: none"> <li>Conversão de JSON e compactação de mensagem dinâmica.</li> </ul>
Cache de mensagens	<ul style="list-style-type: none"> <li>Armazene em cache respostas a solicitações de API comuns, reduzindo a carga de serviços no back-end.</li> <li>Execute a pré-busca do conteúdo da API de hiperídia.</li> </ul>
Agregação de solicitações	<ul style="list-style-type: none"> <li>Agregue respostas de dispositivos móveis para economizar processamento e latência no dispositivo.</li> </ul>
Integração	
Logon único em serviços na nuvem	<ul style="list-style-type: none"> <li>Ative e gerencie o Logon único de identidades corporativas em serviços na nuvem, como o Salesforce.</li> </ul>
Redes sociais	<ul style="list-style-type: none"> <li>Use um proxy e gerencie o acesso de aplicativos móveis a redes sociais e serviços, como Facebook e Twitter.</li> <li>Detecte e filtre conteúdo sensível/confidencial com depuração, rejeição ou redação subsequente de mensagens.</li> </ul>
Serviços de notificação	<ul style="list-style-type: none"> <li>Envie mensagens por diversas plataformas móveis (iOS, Android, etc.).</li> </ul>

Para obter mais informações, visite [ca.com/br/api](http://ca.com/br/api)

A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da era dos aplicativos. O software está no cerne de todas as empresas, em todos os setores. Do planejamento ao desenvolvimento e do gerenciamento à segurança, a CA está trabalhando com empresas de todo o mundo para mudar a maneira como vivemos, fazemos negócios e nos comunicamos – usando dispositivos móveis, as nuvens privada e pública e os ambientes distribuídos e de mainframe. Obtenha mais informações em [ca.com/br](http://ca.com/br).