

RESUMO DA SOLUÇÃO  
O CA IDENTITY SUITE

# Governança e gerenciamento de identidades que capacitam usuários corporativos

Eliminando a lacuna entre a TI e o usuário corporativo

# Resumo executivo

## Desafio

Como líder de TI, executivo de segurança ou gerente de negócios, você está vivendo em tempos de mudanças e desafios. Os ambientes de TI estão se tornando cada vez mais distribuídos, complexos e heterogêneos. Entretanto, decidir quem tem acesso a que e aplicar essas diretivas de forma confiável é um desafio em vários sentidos, e algo que deve envolver todas as três constituintes: a TI, a segurança e os negócios.

Ao mesmo tempo, a TI está frequentemente recebendo orçamentos menores e menos recursos para cumprir com suas responsabilidades. Então, você precisa de uma maneira confiável, porém econômica, de atender a esses importantes desafios de identidades:

- Incluir com agilidade os novos usuários para torná-los produtivos o mais rapidamente possível.
- Garantir que todos os usuários tenham apenas os direitos de acesso apropriados, de acordo com suas funções atuais.
- Automatizar processos de identidade importantes para aumentar a eficiência e reduzir os custos.
- Identificar e impedir potenciais violações de diretivas (contas órfãs, direitos inadequados, etc.) antes que elas ocorram.
- Atender aos requisitos de auditoria sabendo quem tem acesso a quê.

E, por fim, um dos capacitadores mais importantes no ambiente de hoje é:

- Fornecer uma experiência simples e intuitiva, de modo que os usuários corporativos possam acessar seus serviços de identidade essenciais de maneira fácil e conveniente.

---

## Oportunidade

O crescente foco na capacitação de usuários corporativos tem criado muitos desafios para os usuários da maioria das soluções de gerenciamento de identidades existentes atualmente. Infelizmente, as poucas soluções que fornecem uma experiência de usuário razoável geralmente não têm a amplitude de recursos de provisionamento, gerenciamento de funções e governança nem a capacidade de expandir para oferecer suporte ao gerenciamento de identidades em toda a empresa. Isso obriga você a escolher entre amplitude de funcionalidades e facilidade de uso.

De maneira exclusiva, o CA Identity Suite ajuda a eliminar a divisão entre tecnologias de IAM e usuários corporativos. Ele é um pacote integrado de recursos de governança e gerenciamento de identidades que combina funcionalidades robustas com uma experiência intuitiva, conveniente e orientada aos negócios. Ele pode simplificar seus processos de gerenciamento de identidades, melhorar a satisfação dos usuários, oferecer suporte a aplicativos locais e na nuvem e fornecer escalabilidade no nível do consumidor. O melhor de tudo é que ele pode ser implantado de maneira fácil e rápida.

## Principais desafios da governança e do gerenciamento de identidades bem-sucedidos

Este documento destaca alguns importantes desafios do gerenciamento de identidades da empresa aberta de hoje, descreve o motivo pelo qual esses desafios podem impulsionar ou atrapalhar seus negócios e fornece uma visão geral dos recursos oferecidos pelo CA Identity Suite que podem ajudar sua organização a resolver esses desafios com êxito.

Cada um dos desafios a seguir tem um aspecto de negócios e um de TI. Antes, a experiência do usuário com serviços de identidades era dominada por um foco de TI, resultando em interfaces difíceis e satisfação reduzida. O ambiente atual, porém, exige uma ligação entre a TI e o usuário corporativo, a fim de expandir o uso de serviços de identidade e melhorar a experiência geral dos usuários. Vamos explorar os lados corporativo e técnico desses desafios.

Esses desafios exigem um extenso planejamento e devem fazer parte de todos os planos de distribuição:

- **Adoção pelos usuários** — Melhorar e simplificar a experiência geral do usuário a fim de aumentar a adoção de processos de identidade pelos usuários.
- **Solicitações de acesso** — Simplificar o processo de obtenção de acesso aos aplicativos de que os usuários necessitam.
- **Gerenciamento de riscos de direitos** — Impedir violações de diretivas de direitos.
- **Certificações de acesso** — Aumentar a produtividade de gerentes.
- **Acesso de usuários a aplicativos** — Fornecer uma maneira conveniente para os usuários acessarem seus principais aplicativos.
- **Análise de identidades em tempo real** — Garantir a eficiência dos serviços de identidade essenciais.
- **Desafios de implantação** — Melhorar o ROI (Return on Investment - Retorno sobre o Investimento) e o tempo para valorização.

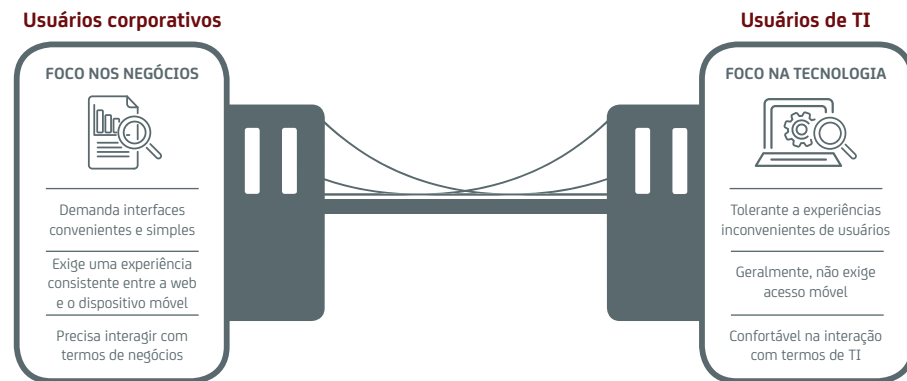
### O desafio: adoção pelos usuários

*"Meus usuários estão frustrados com a interface de usuário inconveniente de muitas das funções de identidade com que eles precisam lidar. Isso limita significativamente nossa capacidade de distribuir esses serviços a uma quantidade maior de usuários dentro da empresa."*

Um dos maiores desafios de realizar implantações de gerenciamento de identidades bem-sucedidas é que a experiência do usuário com serviços de identidade geralmente está altamente centrada na TI. Antes, talvez isso não fosse um problema. Mas, como o gerenciamento de identidades ultrapassa o domínio do usuário de TI puro, essa abordagem não é mais eficaz. A terminologia e os processos que talvez sejam habituais para um usuário experiente em TI podem ser confusos e frustrantes para a maioria dos usuários corporativos. O resultado é uma adoção reduzida de processos de identidades, carga de TI mais alta, falha ao cumprir com os requisitos regulatórios e frustração dos usuários. Os usuários precisam de aplicativos corporativos fáceis, rápidos e que não exijam treinamento, disponíveis no dispositivo de sua preferência. Eles precisam ser introduzidos a processos de identidade básicos, mas isso só funcionará se eles acharem a experiência simples, intuitiva e, acima de tudo, orientada a usuários corporativos, em vez de usuários de TI.

## A solução CA Identity Suite

De maneira exclusiva, o CA Identity Suite ajuda a eliminar a divisão entre tecnologias de IAM e usuários corporativos. Ele é um pacote integrado de recursos de governança e gerenciamento de identidades que combina funcionalidades robustas com uma experiência intuitiva, conveniente e orientada aos negócios. Ao aumentar a satisfação e a produtividade dos usuários corporativos, a experiência de usuário do CA Identity Suite foi projetada para melhorar drasticamente a proposta de valor da solução de IAM para grandes empresas, além de eliminar uma sobrecarga administrativa significativa da organização de TI.



Algumas das mais significativas vantagens da experiência do usuário que o Suite oferece incluem:

- Um catálogo de direitos com linguagem corporativa
- Um inicializador e um painel de aplicativo web e móvel
- Loja única – acesso centralizado e fácil a todos os serviços de identidade para usuários corporativos
- Experiência de carrinho de compras para acessar solicitações e fazer acompanhamentos
- Experiência semelhante à de redes sociais para acompanhar solicitações de acesso
- Ferramentas de aconselhamento proativas
- Aplicativos móveis que permitem que o usuário gere identidades a qualquer momento e em qualquer lugar

O CA Identity Suite também facilita a geração de painéis individualizados e personalizados, adaptados às necessidades exclusivas de funções específicas, como executivos, diretores de segurança e parceiros de negócios. Os administradores podem configurar uma interface com base na função do usuário e a quais serviços ele pode ter acesso. A interface do Suite também pode ser totalmente personalizada para as necessidades de identificação de marca de sua organização, incluindo o logotipo da empresa, o esquema de cores, as fontes, imagens de plano de fundo selecionadas e muito mais. Seu portal refletirá totalmente a identidade de sua empresa.

"Em uma pesquisa realizada por uma empresa de análises externa, 97% dos clientes participantes afirmaram que a experiência do usuário do Identity Suite era melhor em comparação com a da concorrência."

Fonte: Pesquisa da TechValidate

## O desafio: solicitações de acesso

"É difícil para meus usuários solicitar com facilidade o acesso aos aplicativos e sistemas de que precisam para trabalhar. O processo é complicado e os nomes dos recursos geralmente são confusos para meus usuários corporativos."

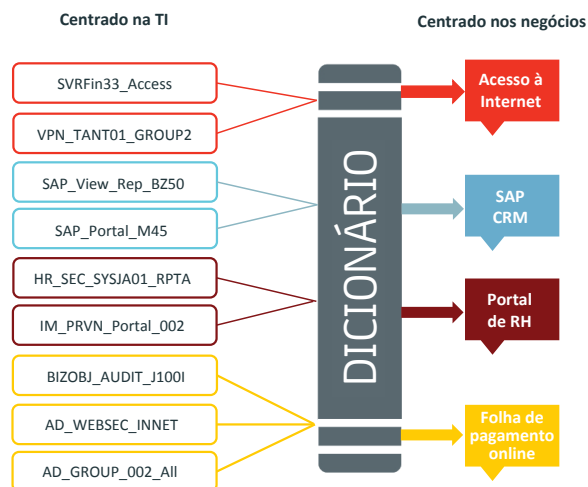
Os usuários precisam obter acesso aos aplicativos e aos dados de que necessitam de forma rápida e fácil e, ao mesmo tempo, manter a conformidade com os requisitos regulatórios. Entretanto, os sistemas de solicitação de acesso costumavam ter como base um conjunto de direitos que foram projetados para administradores que compreendiam seus significados, obrigando os usuários a aprender uma linguagem praticamente nova de termos de TI. À medida que mais e mais usuários corporativos estão se envolvendo com processos de identidade corporativos, essa experiência não intuitiva atrasa a adoção, diminui a satisfação e, geralmente, acaba envolvendo a equipe de TI para ajudar a responder perguntas de usuários corporativos confusos.

Uma nova maneira de interagir com os usuários corporativos é necessária, e a área de solicitações de acesso é um importante exemplo dos benefícios que essa nova abordagem pode proporcionar. Mas a TI tem necessidades válidas nessa área também, como a automação de processos de solicitação de acesso básico e a auditoria simples de solicitações e aprovações. Dessa maneira, recursos que atendam às necessidades de automação da TI e, também, sejam fáceis de usar por usuários corporativos são essenciais.

## A solução CA Identity Suite

O CA Identity Suite fornece uma experiência de "carrinho de compras" simples e intuitiva, que simplifica drasticamente o processo de solicitação de acesso. Modelado com base no conhecido processo de sites de compras de varejo, os usuários podem selecionar, de modo conveniente, funções e direitos necessários para executar suas tarefas, exibir privilégios atuais de acesso e verificar o status de solicitações anteriores.

O Catálogo de direitos corporativos de fácil uso é central para a maneira como o CA Identity Suite ajuda a fornecer uma experiência orientada aos negócios e simples. Ele traduz nomes de recursos criptografados, como "TSS\_MNG\_per\_view", em nomes mais intuitivos, como "Folha de pagamento online", tornando mais fácil para os usuários corporativos localizar os recursos de que necessitam. Você também pode agrupar aplicativos em categorias lógicas para um acesso ainda mais fácil; por exemplo, criando um grupo chamado "Acesso ao SRM" que inclui os aplicativos da SAP, os aplicativos da Oracle e os recursos da Salesforce de que os usuários corporativos geralmente necessitam. Tudo isso definido em termos familiares para esses usuários. A imagem a seguir destaca o mapeamento entre os termos centrados na TI e os termos centrados nos negócios que é executado pelo Catálogo.



O Identity Suite inclui ferramentas de aconselhamento proativas que simplificam bastante o processo de solicitação de acesso. O usuário pode ver sugestões de funções e os direitos de acesso de usuários semelhantes a ele. Esse conselho proativo ajuda o usuário a fazer a solicitação adequada em relação ao acesso desejado. Ele também fornece uma pontuação de risco com base no acesso solicitado e em quão "arriscado" esse direito de acesso pode ser. Dessa maneira, o usuário pode tomar uma decisão mais informada sobre qual acesso solicitar.

## O desafio: gerenciamento de riscos de direitos

*"Às vezes, os usuários recebem direitos por engano que violam nossa diretiva de segurança. Quero que essas violações sejam impedidas antes que ocorram."*

Direitos de usuário inadequados são a causa-raiz de várias violações públicas recentes. Isso é especialmente verdadeiro para usuários com privilégios, pois eles tendem a ter direitos muito abrangentes. Entretanto, o princípio é o mesmo para todos os usuários — precisamos corrigir os direitos inadequados que violam a diretiva de segurança antes que sejam concedidos ("controle preventivo") e encerrar qualquer direito que possa já ter sido concedido anteriormente ("controle reativo"). A menos que controles eficazes estejam em vigor para ambos os casos, o risco será maior e as auditorias de conformidade serão mais desafiadoras.

De forma semelhante, às vezes as diretivas são alteradas e o acesso concedido há muito tempo passa a violar a nova diretiva. Durante certificações de acesso regular, isso precisa ficar muito visível para o gerente, de forma que também seja possível cancelar a certificação do usuário para esse direito de acesso.

### A solução CA Identity Suite

O CA Identity Suite permite que você formule, aplique e valide conjuntos de BPRs (Business Process Rules - Regras do Processo de Negócio) para implementar a segregação de tarefas e outras restrições lógicas relativas aos relacionamentos entre usuários, funções e privilégios. Por exemplo, uma BPR pode modelar uma restrição, como "pessoas com permissão para acessar X não podem ter permissão para acessar Y", ou uma relação de dependência, como "somente as pessoas com acesso A podem ter permissão para fazer B". Dessa maneira, as instâncias que violarem essas diretivas de segurança poderão ser impedidas antes de ocorrerem.

O Suite também pode avisar você se direitos conflitantes estiverem sendo solicitados (os Controles preventivos descritos acima). Ele atribui uma pontuação de risco com base no acesso que está sendo solicitado e na diretiva relacionada. A pontuação de risco baseia-se no usuário, em seus outros direitos e em qualquer fator contextual que possa ser relevante. O solicitante recebe esse nível de risco quando a solicitação de aprovação é feita, para que seja avisado de uma solicitação potencialmente imprópria. De maneira semelhante, o aprovador vê essa pontuação de risco durante o processo de aprovação, o que fornece total visibilidade que pode impedir a concessão de acesso de alto risco.

O Suite também fornece um Controle reativo para corrigir acessos inadequados que já foram concedidos. No momento da certificação, o Suite executa verificações de diretivas em relação ao acesso e informa você se o usuário tem direitos de acesso inadequados que violam alguma diretiva. O gerente vê as violações claramente marcadas para cada usuário, o que permite a correção imediata. Os dois tipos de controle podem reduzir significativamente os riscos de direitos inadequados serem concedidos ou permanecerem não detectados.

## O desafio: certificações de acesso

*"Quero tornar as certificações simples e intuitivas e, com isso, poder aumentar a produtividade de meus gerentes e simplificar minhas auditorias de conformidade."*

Já percebemos a importância de um recurso automatizado para traduzir as informações de acesso de usuários para o idioma e o formato apropriados para cada tipo de campanha de certificação que for realizada. Se os nomes dos acessos forem intuitivos e compatíveis com os negócios, se um fluxo de trabalho flexível puder ser projetado para atender às suas necessidades individuais e se o acompanhamento e o status de cada campanha for facilmente disponibilizado, seu programa de certificação terá mais probabilidade de ser bem-sucedido.

### A solução CA Identity Suite

Os recursos de certificação do CA Identity Suite baseiam-se no Catálogo de direitos de negócios, que torna muito fácil para que os gerentes compreendam os direitos de acesso de cada um dos funcionários e aprovem, rejeitem ou deleguem os direitos de acesso de cada usuário. Além disso, uma pontuação de risco é disponibilizada aos gerentes se um determinado direito de acesso, ou uma combinação de direitos, for particularmente arriscado. Ao possibilitar a visibilidade dessas classificações de risco, a certificação passa a ser não apenas uma proposta de "sim/não", mas algo que pode destacar os riscos que, de outra forma, não ficariam visíveis.

O CA Identity Suite tem a flexibilidade para oferecer suporte a vários tipos diferentes de campanhas de certificação, incluindo:

- **Certificação de entidades** — Usada para certificar os direitos de acesso associados a determinadas entidades de usuários, funções ou recursos por gerentes, proprietários de funções e administradores de recursos.
- **Recertificação** — Permite que você repita o processo de certificação com base em uma campanha anterior.
- **Diferencial** — Inicia uma campanha de certificação com base unicamente nos direitos que foram alterados entre o momento presente e uma campanha anterior.
- **Autoatestação** — Permite que cada usuário, em vez de um gerente ou um proprietário de recursos, certifique seus próprios privilégios. Esse tipo de campanha pode atender a alguns requisitos legais de certificação de segurança de dados.

As campanhas de certificação podem ser entediadas, demoradas e, no fim, ineficazes como uma atividade de redução de risco. O CA Identity Suite aumenta a eficácia desse processo a partir de um ponto de vista de segurança e conformidade e, também, do contexto de uma experiência simples e altamente intuitiva que os gerentes adoram.

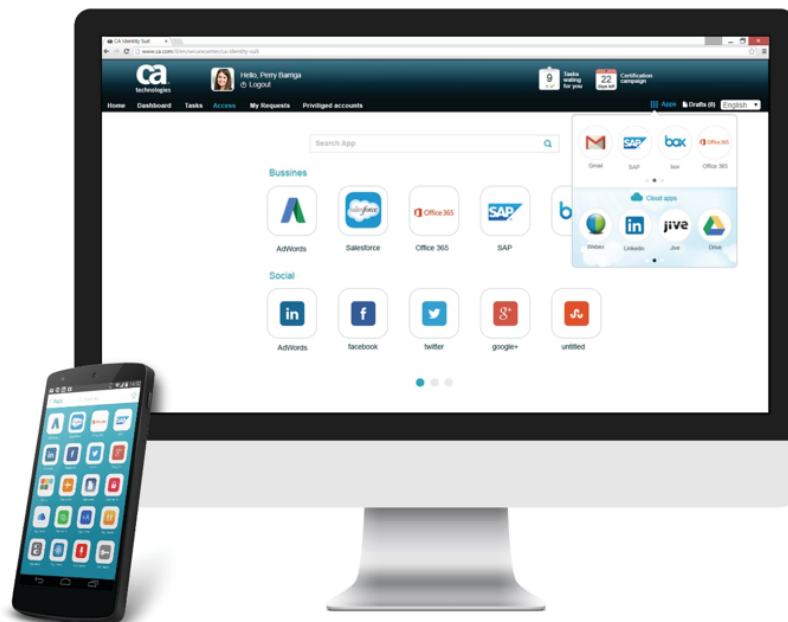
## O desafio: acesso conveniente a aplicativos

*"Gostaria que meus usuários tivessem um acesso muito fácil a todos os seus aplicativos (na nuvem e locais), mas apenas àqueles para os quais eles têm direitos de acesso apropriados para usar. Além disso, preciso de acesso fácil a todos os seus dispositivos."*

Os usuários ficam frustrados quando são confrontados com etapas complicadas para obter acesso a um de seus muitos aplicativos. Vários logons e a incapacidade de abrir aplicativos com facilidade é uma reclamação comum. Além disso, à medida que a mobilidade aumenta e os usuários se acostumam com a conveniência das interfaces desses dispositivos, a frustração e os desafios de produtividade podem aumentar. É necessário ter um método mais conveniente de obter acesso rápido e fácil aos aplicativos de cada usuário, que forneça logon único entre todos eles e inclua apenas os aplicativos que cada usuário tem autorização para acessar.

## A solução CA Identity Suite

O CA Identity Suite inclui uma plataforma inicial de aplicativos web e móveis que fornece aos usuários um painel único para acessar todos os aplicativos web, na nuvem e móveis autorizados de forma simples e rápida. A plataforma pode ser acessada em qualquer dispositivo e fornece recursos de pesquisa aprimorados. Após os usuários efetuarem logon no CA Identity Portal, qualquer aplicativo web estará a apenas um clique de distância, e todos os aplicativos que os usuários acessam em seus computadores desktop também estarão sempre disponíveis por meio do CA Identity Portal Mobile. Essa plataforma mantém os funcionários produtivos enquanto estão em trânsito com logon único completo para aplicativos web móveis em um formato compatível com a mobilidade.





## O desafio: garantir a eficiência do processo para cumprir os SLAs

"Alguns dos meus processos de identidade não estão funcionando muito bem, por isso estou recebendo reclamações de outros gerentes sobre os níveis de serviço oferecidos. Acontece que não tenho informações suficientes sobre a localização desses gargalos para corrigi-los."

Os processos relacionados a identidades muitas vezes são complexos e podem envolver etapas de fluxo de trabalho com vários estágios. Quando esses processos não funcionam com eficiência, como quando um conjunto de usuários simplesmente não consegue concluir uma tarefa em tempo hábil, todo o sistema pode ser prejudicado, impedindo que os objetivos de nível de serviço sejam atendidos. Isso pode resultar em pontos fracos de auditoria ou no simples aumento da ineficiência quando processos básicos, como certificações de acesso, não são concluídos de acordo com os objetivos estabelecidos para o serviço. Sem a visibilidade adequada da operação detalhada desses processos, talvez a causa dos problemas não possa ser identificada e muito menos corrigida rapidamente.

## A solução CA Identity Suite

O CA Identity Suite fornece análises de extensão em tempo real para que a operação dos principais processos de identidade possa ser compreendida e otimizada de forma mais completa. Isso pode ajudar a identificar os gargalos e garantir que seus SLAs (Service Level Agreements - Contratos de Nível de Serviço) essenciais sejam atendidos. Como um exemplo simples, o gráfico abaixo é uma exibição com base em tempo dos SLAs atuais no mês passado, além de números importantes, como os SLAs médios, máximos e mínimos para um determinado processo. Ele também mostra a taxa de entrada de novas solicitações, em comparação com cada dia do mês anterior, e um resumo da disposição (concluída, rejeitada) de todas essas solicitações. Esse recurso fornece um insight significativamente aprimorado ao gerente para que os processos possam ser otimizados e o estado completo de todos esses processos possa ser visualizado facilmente.



## O desafio: implantação difícil

*"A implantação da minha solução de gerenciamento de identidades é demorada e difícil. Em primeiro lugar, a simples instalação e configuração do software leva dias. Depois disso, às vezes alguns casos de uso básicos demoram semanas para entrar em execução porque preciso ter um código personalizado e definir fluxos de trabalho, diretivas e a interface de usuário."*

A implantação de uma solução robusta de gerenciamento de identidades pode ser desafiadora e cara. Alguns recursos básicos podem facilmente levar semanas para entrar em execução. Além disso, todos os requisitos, como conectores para aplicativos personalizados, podem acabar com os recursos e exigir muito tempo.

### A solução CA Identity Suite

O CA Identity Suite reduz *significativamente* o tempo necessário para implantação e execução com estes recursos:

- **Virtual Appliance (vApp).** O vApp elimina a fase tradicional de instalação e fornece uma imagem de máquina virtual pré-instalada e pré-configurada, pronta para ser executada em configurações de produção em plataformas comuns de virtualização. O Virtual Appliance incorpora um sistema operacional protegido, um servidor de aplicativos e o software CA Identity Suite. Ele também tem um suporte integrado para procedimentos comuns de DevOps, como configurações de alta disponibilidade, ajustes de capacidade, agregações de log, patches de plataforma e atualizações de software.

Para implantar serviços de identidade, basta arrastar o nome do serviço até o nome da máquina apropriada para que a instalação seja feita automaticamente. Se você arrastar o mesmo serviço até várias máquinas, todos os mecanismos de comunicação para alta disponibilidade (balanceamento de carga, tolerância a falhas, etc.) serão feitos automaticamente. Não é preciso fazer configurações manuais, que costumam ser demoradas e estão sujeitas a erros. A economia de tempo é significativa.

O resultado dessa abordagem é uma redução expressiva do tempo para valorização e TCO (Total Cost of Ownership - Custo Total de Propriedade), permitindo que você obtenha mais resultados com a mesma equipe e orçamento. Esse método também permite economizar milhares de dólares por ano em custos de licenciamento de software, pois todos os componentes do sistema principal podem ser implantados livremente, sem a necessidade de licenças adicionais.

- **Deployment Xpress (Depx).** O DepX representa uma melhoria radical na forma como o software de gerenciamento de identidades é implantado. Ele consiste em um conjunto de cenários de usuário pré-configurados para casos de uso comuns que a maioria das organizações geralmente exige, incluindo ingresso de usuários, redefinição de senhas, certificações de acesso, ingresso de parceiros, entre outros. Cada cenário tem todos os elementos necessários para uma implantação fácil, como interfaces de usuário de modelo, fluxos de trabalho e definições de diretivas. O gerente simplesmente escolhe os cenários necessários, os coloca no carrinho de compras e conclui o pedido. Nesse momento, todos esses elementos principais são carregados automaticamente no Identity Suite e implantados. É possível fazer personalizações nesses elementos (como a identidade visual corporativa para a interface), mas códigos personalizados não são necessários. Esses cenários aceleram o processo de implantação e podem reduzir significativamente o tempo para valorização de uma implantação de serviços típicos de identidade.
- **Outras ferramentas Xpress.** O Identity Suite inclui ferramentas adicionais que simplificam significativamente o processo de gerenciamento de seu ambiente de implantação, incluindo:
  - O Connector Xpress simplifica o processo de criação de conectores para aplicativos desenvolvidos internamente e facilita a conexão com sistemas que não têm conectores para uso imediato.
  - O Config Xpress permite que você mova componentes de maneira mais rápida e fácil entre os ambientes de armazenamento temporário para obter um gerenciamento da configuração simplificado e um tempo de teste funcional adicional.
  - O Policy Xpress permite que você configure diretivas que executem seus exclusivos processos de negócios complexos. Isso geralmente é feito com códigos personalizados, mas essa ferramenta com base em assistente permite que você crie diretivas internamente em horas, em vez de exigir semanas de programação.

## Principais recursos

O CA Identity Suite fornece os principais recursos a seguir:

- Portal de autoatendimento de identidades ("loja única") — centraliza dados de direitos e fornece um carrinho de compras intuitivo para a solicitação de acesso.
- Redução significativa do tempo de implantação, de dias para minutos.
- Catálogo de direitos compatível com os negócios — faz com que as solicitações de acesso e a certificação de direitos fiquem mais compreensíveis para os profissionais corporativos.
- Análise proativa — informa, previne e alerta o usuário corporativo sobre possíveis violações de diretivas.
- Provisionamento de usuários para uma ampla variedade de aplicativos no local, serviços de SaaS e sistemas não conectados.
- Autoatendimento de usuários — permite que os usuários gerenciem suas próprias informações para reduzir a carga da TI.
- Deployment Xpress — os modelos pré-configurados de casos de uso simplificam bastante a implantação inicial e o gerenciamento contínuo.
- Personalização sem código personalizado — recursos avançados, como o ConfigXpress, o PolicyXpress e o ConnectorXpress, permitem que você personalize sua infraestrutura de gerenciamento de identidades sem códigos personalizados.
- Limpeza de privilégios — analisa os direitos de sistemas existentes e realça privilégios em excesso ou desnecessários.
- Modelagem de funções com um mecanismo de análise avançada de patente pendente — ajuda a classificar de maneira eficiente volumes muito grandes de informações de usuários e privilégios a fim de detectar funções em potencial.



Conecte-se à CA Technologies em [ca.com/br](http://ca.com/br)



A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da economia 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).

Copyright © 2016 CA, Inc. Todos os direitos reservados. Todas as outras marcas utilizadas aqui pertencem às suas respectivas empresas. Este documento não contém nenhuma garantia e é fornecido apenas para fins informativos. As descrições de funcionalidades podem ser exclusivas para os clientes aqui representados, e o desempenho real do produto poderá variar.

A CA não oferece consultoria jurídica. Este documento e qualquer produto de software da CA mencionado neste documento não devem servir como um substituto de sua conformidade com quaisquer leis (incluindo, mas não se limitando a, qualquer lei, estatuto, regulamentação, regra, diretiva, política, padrão, diretriz, medida, requisito, ordem administrativa, ordem executiva, etc.; coletivamente, "Leis") mencionadas neste documento. Você deve consultar a assessoria jurídica competente sobre quaisquer Leis mencionadas neste documento.