



#### Visão geral dos principais recursos:

- **Aprovisionamento de usuários baseado em funções e políticas**
- **Fluxo de trabalho incorporado**
- **Integração de diretórios**
- **Suporte a uma ampla gama de sistemas de destino**
- **Input automatizado com suporte a Universal Feed**
- **Integração com outras soluções eTrust™ Security Command Center**

#### Novidades

- **Integração com eTrust Identity and Access Management**
- **Interface comum com Identity and Access Management**
- **Fluxo de trabalho avançado para gestão de processos corporativos**
- **Suporte a SPML (Service Provisioning Markup Language)**
- **Novas opções para RSA ACE SecurID e Oracle Application**
- **Aprimoramentos no desempenho**
- **Ações de provisionamento baseadas em horário**
- **Sincronização bidirecional de senha**



## eTrust™ Admin r8.1

O eTrust™ Admin automatiza o provisionamento, desativação de usuários e gerenciamento de senhas em sistemas, aplicações, recursos físicos e Web Services distintos, alinhando sistemas computacionais e aplicações com processos corporativos de missão crítica. O eTrust Admin suporta uma ampla variedade de conectores e ferramentas baseadas em padrões, para gerenciamento e segurança dos atuais ambientes computacionais on-demand, com retorno mensurável sobre o investimento.

### Desafios de provisionamento de usuários em um ambiente seguro, on-demand

Vários fatores estão convergindo para a imposição de fortes pressões sobre as empresas atualmente. O enorme poder das tecnologias web está aumentando, resultando em mais preocupações relacionadas à privacidade e segurança dos ativos de informação. Os clientes, parceiros e funcionários esperam serviços on-line e personalizados, disponíveis ininterruptamente. Com as empresas ávidas por oferecer melhor acesso às suas aplicações, elas acabam se deparando com um número cada vez maior de riscos desconhecidos.

O volume de informações pessoais armazenadas nos repositórios dos sistemas, aliado à natureza onipresente da Internet, fez com que o público exigisse maior proteção contra acesso não-autorizado às informações pessoais. Os governos responderam com normas sobre privacidade e integridade dos registros de saúde, financeiros e de dados pessoais. Além disso, a computação on-demand aumenta drasticamente a necessidade de identificação e gerenciamento de acesso, devido à necessidade de provisionar, auditar e reforçar políticas de segurança.

As empresas vêm utilizando a tecnologia web para atender aos crescentes desafios, reestruturando aplicações e serviços e colocando-os on-line. Isso

resultou no crescente aumento do número de identidades individuais, pois cada aplicação exige um ID, senha de usuário e regras de gerenciamento de senhas específicas para autenticação dos usuários. Cabe ao usuário lembrar uma enorme quantidade de senhas, pois escrevê-las pode abrir uma brecha na segurança. Além disso, o esforço administrativo necessário para provisionamento manual e a sobrecarga que envolve a reconfiguração de senhas aumentaram os gastos administrativos.

Os analistas informam que 30% de todas as chamadas para os help desks referem-se à reconfiguração de senhas. Outros relatórios indicam custos consideráveis relacionados à perda de produtividade quando um usuário não consegue ter acesso imediato aos serviços necessários para executar sua função. O problema de desativar usuários também continua a atormentar as empresas. Sabe-se que durante a vida profissional de um funcionário, chega-se a provisioná-lo para pelo menos 16 sistemas — mais ele só é desativado de no máximo 10. O problema das contas fantasma continua, portanto, apresentando um risco de segurança para as empresas.

Igualmente de grande importância nos ambientes on-demand é a completa integração, fundamental para a eficiência operacional, redução ou contenção de custos, diminuição de riscos e rápida facilitação de novos serviços.



## O caso de negócios estratégico para provisionamento e gerenciamento de senhas

Para atender a esses desafios, a Computer Associates International, Inc. (CA) oferece o eTrust™ Identity and Access Management.

Um elemento essencial na arena de Gestão de Identidade e Acesso está garantindo que funcionários, clientes, parceiros e fornecedores tenham acesso aos sistemas certos, com o nível apropriado de privilégios. O eTrust Admin cria as contas necessárias em vários sistemas distintos, recursos físicos e Web Services e automatiza completamente o provisionamento de usuários com informações de origens confiáveis, como bancos de dados das áreas de recursos humanos. Além disso, a administração delegada possibilita a atribuição de capacidade de administração limitada para o usuário, administração do fluxo de trabalho e gerenciamento de senhas para ajudar os administradores de help desks, enquanto o auto-atendimento permite que os próprios usuários reconfigurem suas senhas, o que ajuda a agilizar operações, reduzir os chamados de suporte e eliminar erros humanos. Poderosos recursos de auditoria e registro de todas as ações de provisionamento garantem melhor administração e manutenção dos contratos de nível de serviço.

Entretanto, de nada adianta maior eficiência operacional sem melhor nível de segurança. O eTrust Admin desativa usuários automaticamente e funcionários temporários assim que eles deixam a empresa, removendo rapidamente seus privilégios de acesso, eliminando com isso “contas fantasma” e reduzindo os pontos de entrada de hackers.

A legislação sobre identidade está reavaliando o ambiente de TI e os desafios de atender os requisitos regulamentares referentes à privacidade, maior segurança e mitigação de riscos continuam. A administração de usuários baseada em políticas ajuda a garantir que somente pessoas autorizadas tenham

acesso aos recursos confidenciais. Além disso, avançados recursos para registro de eventos e relatórios atendem as demandas dos auditores no que se refere a como o acesso ao sistema é concedido e utilizado. O eTrust Admin oferece sincronização de senhas em todos os sistemas, economizando tempo e melhorando a eficiência das operações. A sincronização das senhas reduz o número de IDs e senhas exclusivas existentes — eliminando a necessidade de anotar as senhas, reduzindo assim os riscos à segurança.

Melhores relacionamentos com os elementos garantem agilidade dos negócios. O eTrust Admin ajuda a garantir que as pessoas tenham acesso imediato aos recursos necessários — aprimorando assim a experiência do usuário, os relacionamentos com parceiros de negócios e clientes e minimizando a perda de produtividade.

### Recursos e funções diferenciados

**Administração de usuários baseada em políticas e funções.** Através da administração baseada em funções, o eTrust Admin administra seus usuários de acordo a função de cada um deles. Essa forma de administração de usuários controla o acesso necessário em todos os diferentes sistemas.

- **Aprovisionamento de acesso e baseado em funções e políticas.** Mantém todas as contas de usuário em rígida conformidade com as políticas de acesso corporativo.
- **Administração do acesso de usuários.** Administra holisticamente todos os privilégios dos seus usuários dos recursos físicos e contas de TI.
- **Aprovisionamento e desativação.** Cria, modifica e reativa contas de usuários em sistemas heterogêneos, com base na função do usuário.
- **Integração com diretório.** O eTrust Admin integra-se com qualquer diretório compatível com LDAP (Lightweight Directory Access Protocol) V3. Além disso, inclui uma versão especial do eTrust™ Directory que permite a configuração das informações de configuração do eTrust Admin.
- **Opções de diretório.** A opção Generic LDAP possibilita a integração com aplicação ERP ou diretório capacitado para LDAP. A ODBC Option possibilita a integração com qualquer sistema que utilize um banco de dados relacional como repositório de informações sobre usuários.



- **Suporte a uma ampla gama de sistemas destino.** A interface aberta amplia a gestão de usuários para aplicações desenvolvidas internamente ou de terceiros via APIs (Application Program Interfaces) abertas, SDKs (Software Development Kits) e/ou SPML (Service Provisioning Markup Language). A SPML permite a integração com produtos, inclusive com aplicações ERP. O eTrust Admin aprovisiona seus usuários para a mais ampla gama de sistemas destino.

**Suporte automatizado à entrada de informações.** O eTrust Admin inclui uma opção Universal Feed que pode ser utilizada para automatizar totalmente a administração de contas.

- **Informações obtidas de sistemas de RH.** As informações são inseridas no mecanismo de fluxo de trabalho do eTrust™ Admin e todas as contas são criadas ou atualizadas automaticamente. As alterações realizadas nos sistemas de RH refletem-se automaticamente no eTrust Admin. As contas ficam sempre atualizadas com os dados pessoais.

**Suporte a auto-atendimento.** O eTrust Admin alia sua interface web de auto-gestão com um componente ágil e customizável de auto-atendimento. O auto-atendimento permite que os usuários reconfigurem e desbloqueiem senhas de contas e visualizem e gerenciem suas informações de usuário. Inclui também um mecanismo de confirmação configurável que permite aos departamentos de TI definirem mecanismos de autenticação segundo as normas mais rígidas.

- **Integração com o eTrust Security Command Center.** O registro de eventos de acesso é peça fundamental na estratégia de gerenciamento de acesso. Os eventos do eTrust Admin podem ser processados pelo eTrust Security Command Center e consolidados em uma completa auditoria de identidade.

## Novidades da versão 8.1

**eTrust Identity and Access Management.** As empresas precisam

gerenciar as identidades de ponta a ponta. O eTrust Admin, componente do eTrust Identity and Access Management, oferece aprovisionamento, administração de usuários e gerenciamento de senhas para uma ampla variedade de recursos de TI e não-TI. Inclui também avançada integração com componentes IAM de auditoria e reforço de acesso.

- **Interface gráfica de usuário do eTrust Identity and Access Management.** O eTrust Admin compartilha uma interface web administrativa e um portal comuns com todos os componentes do eTrust Identity and Access Management. Mais especificamente, o gerenciamento de políticas e o gerenciamento de usuários apresentam uma visão administrativa comum de todas as identidades e seus respectivos acessos.

**Fluxo de trabalho.** O eTrust Admin alia-se sua aplicação User Provisioning Workflow com Advanced Workflow para gerenciamento dos processos corporativos.

- **Advanced Workflow para gerenciamento dos processos corporativos.** O componente Advanced Workflow oferece um kit de ferramentas Workflow que pode ser utilizado para a criação de processos customizados de fluxo de trabalho. O kit inclui também uma série de processos de amostra que demonstram a funcionalidade que pode ser obtida com o Advanced Workflow.
- **Aprimoramentos no fluxo de trabalho.** O eTrust Admin Work Flow oferece aprimorados recursos de busca, maior controle para os aprovadores da área administrativa e técnica, além de possibilitar o gerenciamento de funções dentro do fluxo de trabalho.

**Suporte à SPML (Service Provisioning Markup Language).** O eTrust Admin oferece um serviço SPML Service com Request Authority via linha de comando que suporta o padrão SPML definido pelo órgão de definição de padrões OASIS (Organization for the Advancement of Structured Information Standards). As operações de adição, modificação e exclusão suportam comunicação SPML síncrona e assíncrona. O padrão SPML viabiliza a integração com produtos como soluções de ERP e RH, bem como com outros terminais gerenciados SPML para aprovisionamento.



### **Aprimoramentos no desempenho.**

- **Maior paralelismo para o Admin Server e seus agentes.** O tempo de resposta do usuário final aumenta graças ao paralelismo do eTrust Admin.
- **Suporte a configurações de failover e balanceamento de carga.** É possível usar vários servidores eTrust Admin em um único domínio em ambientes com carga alta. As atividades de lote podem ser transferidas para um servidor à parte configurado para operar com diferentes DSAs do eTrust Directory, eliminando assim a interferência no desempenho dos servidores Admin interativos. Os clientes podem ser configurados para failover de um servidor Admin para outro.

### **Aprimoramentos operacionais.**

- **Sincronização bidirecional de senhas.** A senha bidirecional facilita a captura e propagação das alterações de senhas via eTrust Admin originadas a partir de terminais gerenciados. A sincronização de senhas bidirecional é fornecida pelo Microsoft Active Directory, eTrust CAACF2, eTrust CA-Top Secret e Microsoft Windows NT.
- **Ações temporais.** No eTrust Admin, as ações de ativação, desativação e exclusão podem ser comandadas por atributos de data para o usuário global.
- **Movimentação e renomeação de objetos.** No eTrust Admin, os usuários globais, funções e políticas podem ser renomeados. Ele também suporta realocação de objetos (movimentação de um objeto de um local na hierarquia do diretório para outro). Essas operações também são válidas para namespaces customizados.
- **Gerenciamento de recursos.** O eTrust Admin gerencia os recursos nativos como diretórios internos, ACLs e arquivos privativos no eTrust Access Control e eTrust SSO. Isso inclui a remoção de recursos quando há mudança de cargo ou quando um funcionário sai da empresa.
- **Novos relatórios.** Mais relatórios disponíveis no eTrust Admin. Entre eles:
  - Object Count by Type (Número de objetos por tipo)

- User Count by Status (Número de usuários por status)
- List of Suspended Users (Lista de usuários suspensos)
- List of Expired Users (Lista de usuários com senhas vencidas)
- List of Users expire in n days (Lista de usuários com senhas vencidas a n dias)
- List of Administrative Users (Lista dos usuários administrativos)
- List of Roles by Active Users (Lista de funções por usuários ativos)
- List of Users by Business Approver (Lista de usuários por aprovador)

### **Aprimoramentos administrativos.**

- **Aprimorada definição do escopo administrativo.** O eTrust Admin traz dois tipos de escopos de privilégios administrativos: escopo de grupo de usuários globais e escopo de grupo de usuários globais dinâmicos. O escopo de grupo de usuários globais permite que os administradores executem tarefas com relação aos usuários membros de um grupo e sobre suas respectivas contas. O escopo de grupo de usuários globais dinâmicos permite que os administradores executem ações em um grupo onde a associação é definida por uma expressão (por exemplo, todos os usuários globais cujo atributo local seja "Los Angeles") e não pela lista explícita de seus membros.
- **Funções, grupos e perfis de Admin aninhados.** Agora é possível aninhar funções, grupos de usuários e perfis de admin no eTrust Admin. O agrupamento de funções permite que os usuários com determinadas funções reúnam-se em um grupo que congrega determinadas funções específicas. Da mesma forma, um grupo de usuários globais pode ser colocado com um outro grupo de usuários globais. O mesmo acontece com o perfil admin, que pode ser agrupado com um outro perfil admin.

**Novas opções.** O eTrust Admin agora provisiona para os seguintes terminais gerenciados:

- **RSA ACE Secure ID Option.** Esta opção suporta as funções explorar, criar, modificar e excluir para contas e grupos RSA ACE Server. É possível atribuir permissões SecurID para uma conta.



- **Oracle Applications Option.** Esta opção possibilita a administração de usuários de aplicações Oracle E-Business Suite, apresentando um ponto comum para administração de todos esses usuários: cadastramento de diretórios, exploração dos mesmos para trabalho com objetos a serem gerenciados e correlação de suas contas com usuários globais via políticas específicas a ambientes Oracle.
- **eTrust Access Control Application Security (eTrust ACAS) Option.** O eTrust Admin agora suporta o novo recurso ACAS do eTrust Access Control.
- **eTrust Single Sign-On For Advanced Policy Server Support.** Esta opção aprovisiona o eTrust Single Sign-On, r7.0 ou superior.

- **Universal Provisioning Option.** Esta opção oferece um mecanismo para que o eTrust Admin envie solicitações alertando o administrador do sistema sobre um sistema não gerenciado. Ela é indicada, mas não se limita, àqueles namespaces com os quais o eTrust Admin não possui uma interface de provisionamento direta.

**Opções aprimoradas.** Foram feitos aprimoramentos nas opções do eTrust Admin para Microsoft Active Directory, eTrust Access Control, Microsoft Exchange 5.5, Microsoft Exchange 2000, IBM Lotus Notes Domino, Oracle, OS/400, SAP e UNIX.

**Para obter mais informações, ligue para 1-800-875-9659, ou acesse [ca.com](http://ca.com)**

## Plataformas suportadas

eTrust Admin Opções			eTrust Admin Server Plataformas
Sistemas operacionais	Groupware	Bancos de dados	
Windows <ul style="list-style-type: none"> <li>o NT</li> <li>o 2000</li> <li>o 2003</li> </ul> Linux: Red Hat, SuSE Linux for OS/390 SUN Solaris HP-UX HP Safeguard IBM AIX Tru 64 IRIX AS/400 NSK Safeguard <ul style="list-style-type: none"> <li>o Open VMS</li> <li>o S/390</li> <li>o Z/OS</li> <li>o AS/400</li> </ul>	Exchange 2000 Exchange 5.5 Lotus Notes Domino Novell Bindery Novell NDS	IBM DB/2 Informix Advantage™ Ingres® Active Directory/ ADAM MS SQL Sybase Oracle Enterprise Relational Database	Microsoft Windows 2000/2003 Server
	Aplicações de ERP	Genéricas	Mainframe
	Oracle e-Business Suite PeopleSoft SAP	Universal Feed SAP Aplicações de ERP	eTrust CA-ACF-2 eTrust CA-Top Secret IBM RACF

