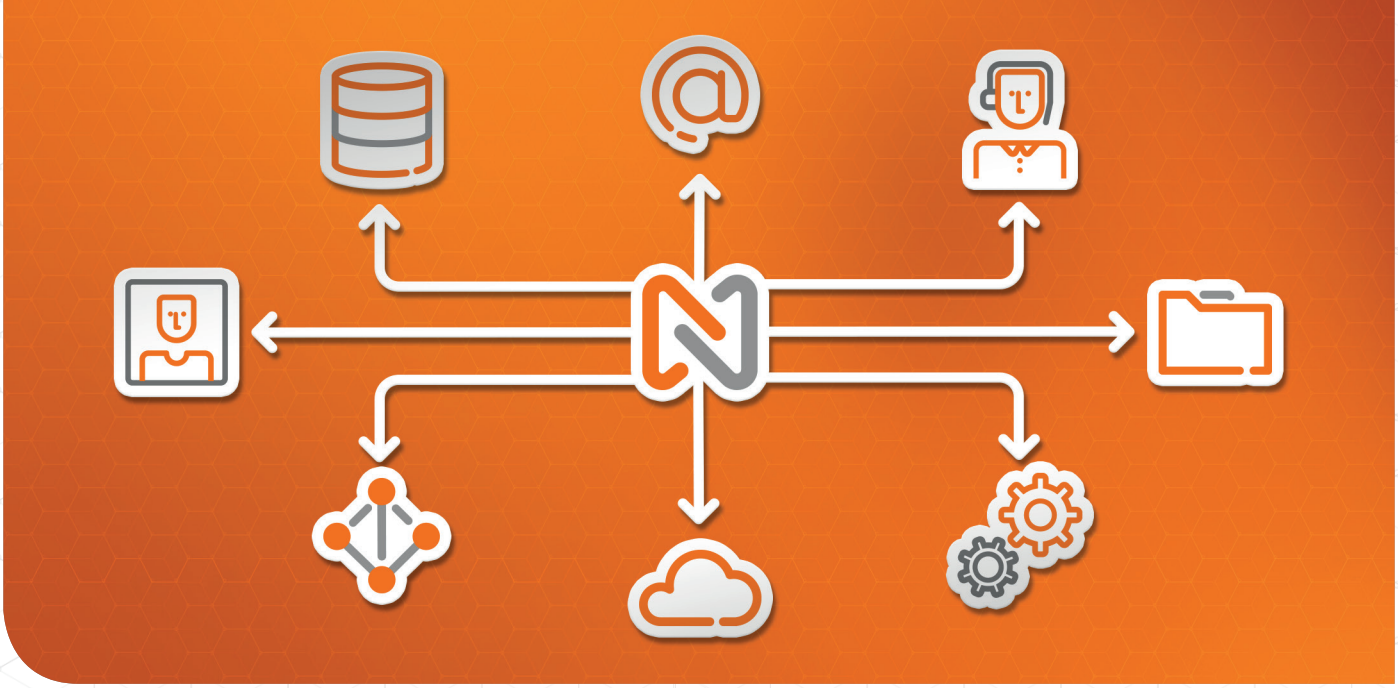
NetAdmin SOFTWARE

NETADMIN®

IAM 3.5

Identity and Access Management



Visão geral

Em sua versão 3.5, a solução NetAdmin IAM reúne diversas funcionalidades para automatizar o ciclo de vida das contas de usuários e provisionar automaticamente permissões de acesso com base em perfis, nos sistemas de infraestrutura e de negócios.

Os usuários podem solicitar permissões de acesso adicionais em um portal de autoatendimento, com *workflow* de aprovação e provisionamento automatizado.

Principais benefícios

Mitigação de riscos
Revogação de acessos indevidos decorrentes de permissões excessivas ou incorretamente aplicadas.

Compliance
Conformidade com as normas e regulamentações pertinentes, a exemplo da ISO 27000, PCI DSS e da Lei Geral de Proteção de Dados (LGPD).

Auditabilidade
Rastreabilidade e facilidade de análise das atividades executadas para atendimento às demandas de auditoria.

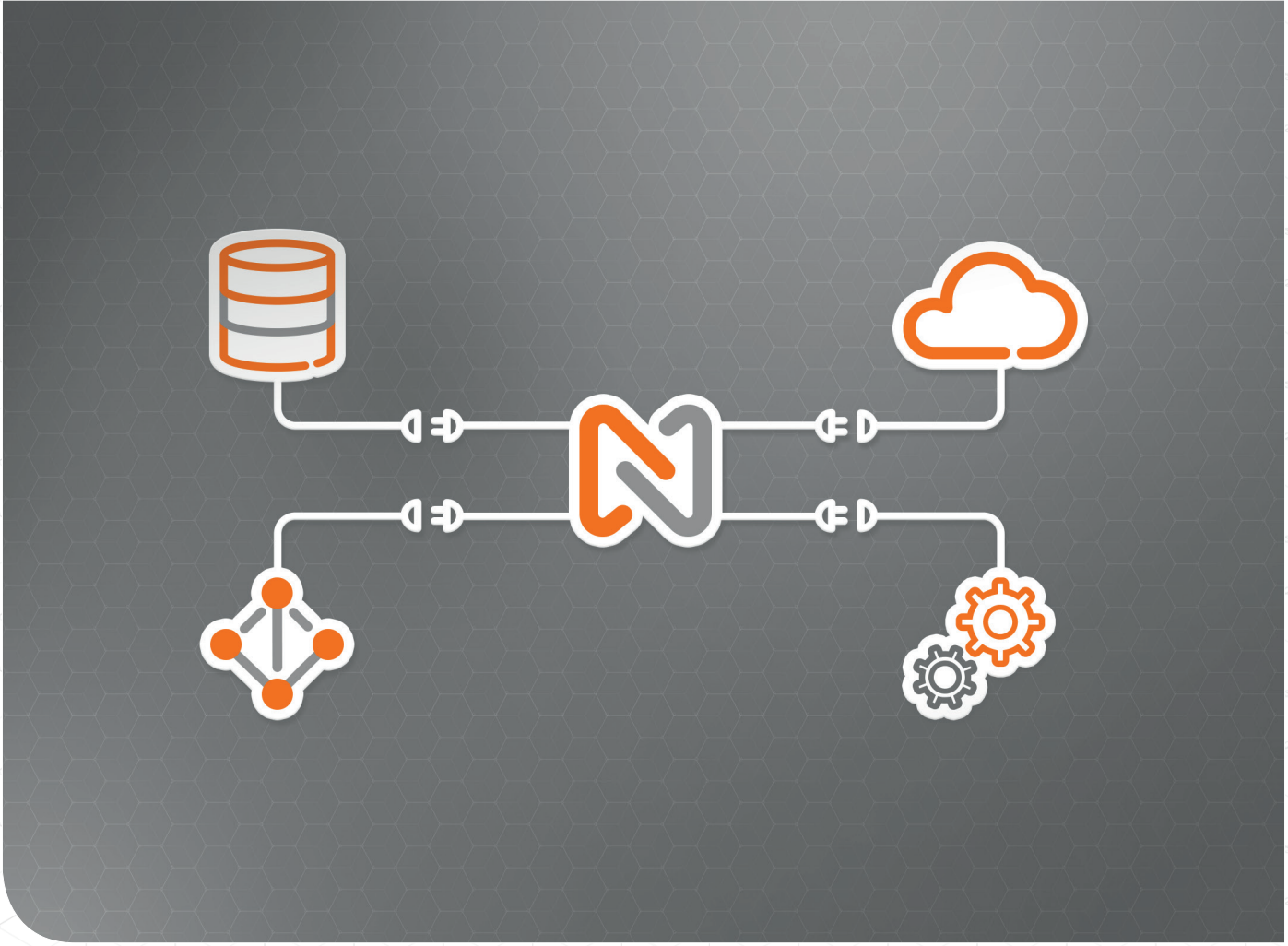
Eficiência operacional
Aumento da eficiência na gestão de acessos e redução do tempo de espera para os colaboradores desempenharem suas atividades.

Flexibilidade
Adequação às regras de negócio específicas.

Gerenciabilidade
Administração simplificada do ciclo de vida das identidades e acessos dos colaboradores, emissão de relatórios detalhados das ações realizadas e integração com diversos sistemas de mercado.

Consistência dos dados
Redução da vulnerabilidade, através da coerência entre a situação do colaborador e seus acessos aos sistemas e repositórios de dados na corporação.

Excelente relação custo-benefício
Licenciamento e implementação acessíveis para médias e grandes empresas. ■



Integrações

Integração com sistemas de RH

A automação da gestão de identidade e acessos é fortemente direcionada pelos dados cadastrais dos colaboradores no RH.

As informações dos colaboradores podem ser obtidas diretamente de um sistema de RH ou de outra base que consolide dados provenientes de diferentes sistemas. O NetAdmin IAM obtém as informações tipicamente por meio de *web service* ou pelo acesso a uma *view* de leitura na base de dados.

As informações obtidas são atualizadas de hora em hora – ou em um outro intervalo customizado – e, posteriormente, são classificadas e transferidas para a base de dados do NetAdmin IAM, de onde são utilizadas para os processos de automação.

Detecta automaticamente alterações nesses dados, não sendo necessário que o sistema fonte das informações o notifique sobre a ocorrência de eventos como contratação, promoção e demissão.

Além dos atributos padrão, os dados do RH podem ser complementados com quaisquer informações que venham a ser úteis na tomada de decisão dos processos automáticos do NetAdmin IAM.

Integração com o Active Directory (AD)

O Active Directory (AD) é o serviço de diretório mais frequentemente utilizado pelas organizações.

Enquanto sistema de uso corporativo, o NetAdmin IAM é integrado ao AD tanto para autenticação como para autorização, assim como também pode ser integrado ao Office 365 ou operar de forma não integrada.

Integração com sistemas integrados ao AD

Um sistema é considerado de autenticação integrada ao AD quando ele utiliza apenas as senhas do AD e não senhas próprias. ▶

Integrações

Já a autorização integrada ao AD se caracteriza quando um sistema respeita os grupos de segurança do AD para controlar as permissões de acesso dos usuários nesse sistema.

O NetAdmin IAM gerencia os sistemas integrados ao AD (por autenticação ou autorização) através do módulo *Active Directory Management* (ADM).

Integração com sistemas de mercado não integrados ao AD

Para controlar as permissões de acesso em diferentes sistemas, o NetAdmin IAM utiliza conectores[1] que abstraem os detalhes técnicos e proporcionam uma abordagem uniforme de gerenciamento.

A empresa NetAdmin disponibiliza diversos conectores previamente desenvolvidos para sistemas de mercado, o que agiliza a implantação de projetos. Novos conectores são constantemente desenvolvidos.

Integração com sistemas legados não integrados ao AD

Sistemas legados podem utilizar esquemas de segurança muito peculiares. Ainda assim, por meio do desenvolvimento de conectores específicos, os mesmos podem ser gerenciados pelo NetAdmin IAM.

As tecnologias comumente empregadas no desenvolvimento de conectores no NetAdmin IAM são: *web services* REST, LDAP, SSH e acesso direto à base de dados.

Integração com sistemas ITSM

O NetAdmin IAM pode provisionar, por meio de conectores, permissões de acessos nos sistemas ITSM (*IT Service Management* - Gerenciamento de Serviços de TI) ou sistemas de chamados, assim como faz com os demais sistemas.

Adicionalmente, pode interagir com o ITSM para outras finalidades.

A interface web do NetAdmin IAM, utilizada para execução de ações sob demanda, requer que o operador informe o número do chamado associado à ação a ser realizada para registro dessa informação nos logs de auditoria. O número informado pode ser validado no ITSM para que apenas números de chamados que estejam em aberto e na posse do respectivo solucionador sejam aceitos.

O NetAdmin IAM pode ser acionado pelo ITSM por meio de *web services*, de forma que ações relacionadas à identidade e acesso possam ser executadas automaticamente em reação à eventos internos do ITSM.

O NetAdmin IAM pode acionar o ITSM para nele executar ações como a abertura e fechamento de chamados por meio do acionamento de um *web service* ou envio de e-mail com formatação preestabelecida.

Integração com sistemas SIEM

O NetAdmin IAM pode encaminhar os eventos de segurança gerados ou coletados para sistemas SIEM (*Security Information and Event Management* - Gerenciamento e Correlação de Eventos de Segurança). Alguns dos eventos gerados incluem: ações administrativas realizadas na plataforma (concessão ou revogação de acesso) e situações de anormalidades (acessos concedidos diretamente nos sistemas gerenciados).

Em respostas aos eventos de segurança, o NetAdmin IAM disponibiliza diversas ações sobre as identidades e/ou acessos que podem ser acionadas pelo SIEM, através de *web services* ou pela própria ferramenta.

A integração com os sistemas SIEM é feita pelo protocolo SYSLOG.

Integração com outros sistemas

O NetAdmin IAM pode ser acionado por quaisquer outros sistemas que necessitam realizar ações ou obter informações relacionadas a identidades e acessos.

Qualquer função do NetAdmin IAM, seja nativa ou customizada, pode ser publicada por *web service* REST.

Qualquer método externo, disponível em outros sistemas, pode ser acionado pelo NetAdmin IAM por meio de chamadas de *web service*, banco de dados, SSH ou outro protocolo aceitável pelo sistema remoto. ■

[1] Conector é um *middleware* que realiza a integração do NetAdmin IAM com softwares de outros fabricantes.

Gestão de identidade

Correlação entre diferentes contas de um mesmo usuário em múltiplos sistemas

O NetAdmin IAM pode integrar repositórios de identidades de diferentes padrões e tecnologias através do uso de conectores.

Permite relacionar as contas de acesso que um mesmo colaborador possui em diferentes sistemas, mesmo que as nomenclaturas utilizadas sejam diferentes.

As informações cadastrais dos colaboradores são mantidas entre todos os repositórios de identidade gerenciados.

As configurações de identidades também são realizadas em todos os sistemas envolvidos, garantindo coerência entre eles.

Criação automática de contas para colaboradores recém-admitidos

O NetAdmin IAM detecta automaticamente novos registros na base do RH, sem necessidade de notificação.

O NetAdmin IAM cria automaticamente contas no AD e nos demais sistemas que o colaborador precise utilizar com base em parâmetros configurados.

Os atributos das contas são preenchidos de acordo com os dados provenientes do RH.

Informações como *login*, nome de exibição (*display name*) e endereço de correio podem ser geradas automaticamente utilizando as regras de nomenclatura da empresa.

Uma senha aleatória é gerada e enviada por e-mail para a chefia imediata do colaborador. A conta do colaborador é configurada para exigir alteração da senha no primeiro *logon*.

Ações adicionais podem ser associadas ao processo de criação de contas, tais como a criação de caixa postal, alocação de licenças e outras.

Criação de contas sob demanda para colaboradores

Nem todos os colaboradores cadastrados no RH precisam ter acesso à rede desde o primeiro dia de trabalho. Em casos como esses a criação automática de contas no AD é dispensável.

No entanto, há situações nas quais esses colaboradores podem precisar de uma conta sob demanda. Tal processo pode ser realizado pelos operadores do Service Desk em atendimento a uma solicitação de serviço.

A criação de contas realizada sob demanda requer que exista um registro para o colaborador em questão no RH, uma vez que seus dados serão utilizados para a criação da conta e, assim, irão garantir a conformidade do processo.

Criação excepcional e/ou emergencial de contas para novos colaboradores

O NetAdmin IAM é capaz de criar contas para colaboradores que ainda não constam na base do RH. ▶

Gestão de identidade

Posteriormente, quando o registro correspondente for detectado na base do RH, a conta previamente criada será automaticamente vinculada ao novo registro e, a partir de então, será tratada como uma conta regular.

Sincronismo de atributos entre o RH e o AD

Os atributos originados na base do RH são considerados mandatórios e mantidos sincronizados com o AD.

Ações adicionais podem ser incorporadas ao processo de sincronização, como movimentar a conta para determinada Unidade Organizacional (OU) no AD ou incluí-la nos grupos correspondentes aos seus atributos no RH.

Efetivação de estagiários e transferência de empregados entre empresas de um grupo empresarial

Mudanças nas relações de trabalho dos colaboradores comumente geram novas matrículas e essa situação deve ser tratada pela Gestão de Acessos (GA).

Nesses casos, o NetAdmin IAM pode tanto criar novas contas e desabilitar as antigas como adequar as contas antigas para reutilização.

Caso a opção seja pela adequação das contas, todos os procedimentos necessários serão realizados automaticamente.

Desabilitação temporária por afastamento

Com os objetivos de reforçar a segurança da informação e evitar passivos trabalhistas em casos de férias, licença-maternidade e outros motivos de afastamento, as contas dos colaboradores podem ser automaticamente desabilitadas na data do afastamento e reabilitadas na véspera do retorno.

É possível emitir alertas sobre quais motivos de afastamento provocarão a desabilitação das contas.

Cargos gerenciais podem ser tratados como exceções para que suas contas permaneçam habilitadas durante os períodos de afastamento.

Um controle dinâmico de exceções permite que determinados colaboradores em férias tenham suas contas reabilitadas temporariamente.

Desabilitação permanente de desligados

O NetAdmin IAM detecta a rescisão de colaboradores na base do RH e desabilita automaticamente as respectivas contas na data apropriada.

Além de desabilitar todas as contas associadas ao colaborador desligado, ainda revoga suas permissões em todos os sistemas, move a conta para uma Unidade Organizacional (OU) específica e notifica a chefia imediata sobre as ações realizadas.

Se assim for configurado, quando decorrido determinado tempo após a desabilitação – por exemplo, seis meses mais tarde – as contas serão permanentemente excluídas do AD.

Outras ações podem ser vinculadas ao processo de desabilitação, a exemplo da desassociação de caixa postal, liberação de licenças e outras.

Desabilitação emergencial

Se houver a necessidade de desabilitar emergencialmente a conta de um colaborador cuja informação de rescisão ainda não consta na base do RH, um comando com essa finalidade pode ser acionado.

Além de desabilitar imediatamente a conta, o sistema força o *logoff* caso ela esteja em uso e impede a reabilitação da mesma pelos operadores do Service Desk.

Gerenciamento pelo Service Desk

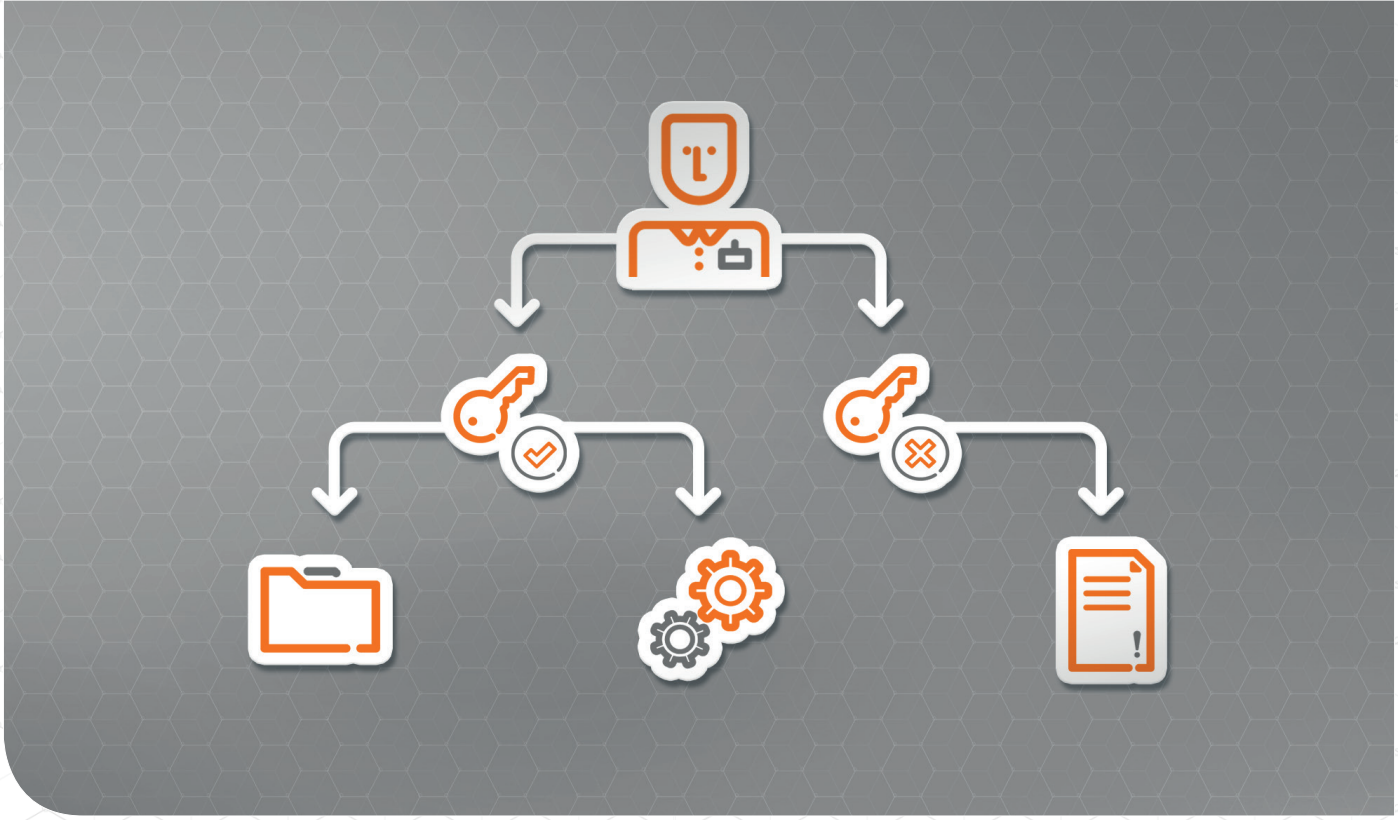
O NetAdmin IAM fornece uma interface na qual os operadores do Service Desk podem realizar ações administrativas nas identidades gerenciadas pelo sistema, tais como habilitação e desabilitação de identidades e criação de identidades sob demanda.

Classificação de contas de usuário

Todas as contas de usuário habilitadas podem ser classificadas como de empregados, estagiários, terceirizados, serviço, teste, etc.

Desta forma, o IAM gerencia somente as contas classificadas e vinculadas a uma identidade, evitando alterações indevidas no ambiente.

As contas que não foram classificadas são apresentadas em um relatório de contas órfãs. ■



Gestão de acessos

Inventário das contas e permissões atuais

Por meio do cruzamento de dados, o NetAdmin IAM realiza o inventário das identidades e permissões existentes em cada sistema gerenciado. Essas informações são utilizadas para o levantamento de perfis de acesso e detecção de alterações indevidas.

Gestão de Perfis e Funções

O NetAdmin IAM incorpora o conceito RBAC (*Role-Based Access Control* ou Controle de Acesso Baseado em Funções) e organiza os direitos de acesso em uma hierarquia de Perfis e Funções.

As Funções representam as transações individuais que são realizadas pelos colaboradores para suportar os processos empresariais e requerem permissões específicas em um ou mais sistemas. Já os Perfis agregam o conjunto de Funções que são regularmente desempenhadas por determinados colaboradores.

Um levantamento de perfis de acesso, apoiado pelo inventário das permissões atuais, fornece os subsídios para o cadastramento dos Perfis e Funções no NetAdmin IAM.

Os perfis de acesso podem ser dinamicamente associados aos colaboradores através de seus atributos cadastrados no RH, tais como cargo, departamento, empresa e chefia, dentre outros.

Em determinados casos, no entanto, pode ser inviável associar com precisão um perfil de acesso considerando apenas os atributos dos colaboradores. Há empresas que nomeiam cargos genéricos sem informação suficiente para uma tomada de decisão automática. Um exemplo dessa situação é a existência de dois profissionais denominados analistas financeiros em uma mesma empresa que exercem funções diferentes.

Nesses casos, os perfis podem ficar disponíveis para serem solicitados pelos usuários através de uma solicitação de serviço no ITSM ou no portal de autoatendimento do NetAdmin IAM.

Um colaborador pode ser associado simultaneamente a diferentes perfis, tendo como resultado o somatório de todas as permissões relacionadas.

Controle de segregação de funções

As ações que não devem ser desempenhadas por um mesmo usuário são cadastradas no NetAdmin IAM em uma matriz de segregação de funções, utilizada para identificar automaticamente essas situações e administrar controles compensatórios. ▶

Gestão de acessos

As violações às regras de segregação são identificadas, classificadas e associadas aos devidos controles compensatórios.

As situações de funções conflitantes são regularmente reavaliadas como parte do processo de recertificação de acessos.

Provisionamento automático de permissões de acesso

As contas recém-criadas ou que tiveram seus atributos-chave alterados no RH serão automaticamente provisionadas com os direitos de acesso apropriados, caso algum perfil de acesso esteja associado aos seus novos atributos.

Solicitação de permissão de acesso por autoatendimento

O NetAdmin IAM permite que os usuários solicitem acesso aos sistemas através de um portal de autoatendimento.

O administrador pode configurar os seguintes aspectos do portal de solicitação de acesso: cadastro do catálogo das permissões e serviços disponíveis; regras de elegibilidade de solicitantes; *workflow* de aprovação e gestores aprovadores e substitutos.

O *workflow* de aprovação das solicitações é flexível e pode ser configurado para consultar a chefia imediata e/ou o gestor do recurso através de correio eletrônico, com links para aprovação ou rejeição. Outras consultas podem ser configuradas, em série ou em paralelo.

Após a aprovação pelos gestores, as permissões são automaticamente aplicadas aos sistemas apropriados.

Diversas interfaces permitem o acompanhamento e controle das solicitações, sejam pelos solicitantes, aprovadores ou pela equipe de Gestão de Acessos (GA). Ações de cancelamento e alterações podem ser feitas nas solicitações em curso.

Todas as ações relacionadas ao processo de solicitação são detalhadamente armazenadas em logs de auditoria.

Provisionamento de permissões de acesso pelo Service Desk

As empresas podem disponibilizar a solicitação de permissões de acessos em seus catálogos de serviços.

Para a execução desses serviços, a equipe de primeiro nível de solucionadores do Service Desk utilizará a interface web do NetAdmin IAM e nela informará o número do chamado que está sendo solucionado.

Caso exista integração com o sistema de Service Desk, o número de chamado será validado para garantir que ele esteja na posse do operador.

A conta de serviço do NetAdmin IAM executará, em segundo plano, as ações apropriadas nos respectivos sistemas através dos conectores.

Todas as ações executadas geram trilhas de auditoria detalhadas tanto pelo portal de autoatendimento como pelo Service Desk.

O tempo gasto na execução da tarefa corresponde a uma fração do que seria necessário utilizando-se a console nativa do respectivo sistema.

Essa abordagem torna desnecessário que os operadores tenham conhecimentos técnicos e permissões administrativas em cada sistema, assim como dispensa o uso de diferentes consoles de gerenciamento.

Concessão de permissão de acesso temporário

Para atender a demandas específicas, pode ser necessário conceder um direito de acesso com um determinado prazo de validade.

O NetAdmin IAM permite que, ao conceder acesso a um usuário, seja informada uma data de expiração. Os direitos de acesso expirados são automaticamente revogados na data apropriada.

Um exemplo no qual esta funcionalidade pode ser utilizada é quando um funcionário substitui outro durante as férias. ▶

Gestão de acessos

Revogação automática de direitos de acesso obsoletos

O NetAdmin IAM pode ser configurado para revogar automaticamente os direitos de acesso obsoletos de um colaborador quando detectar alteração de cargo, departamento ou uma combinação de atributos-chave.

Esse procedimento garante que o colaborador não acumule permissões que não dizem mais respeito às suas atividades.

Reprocessamento de perfil de acesso

A normalização dos acessos de um colaborador pode ser alcançada com o reprocessamento dos seus perfis de acesso que, por sua vez, concedem os acessos apropriados ao cargo e revogam as permissões indevidas. Tal processamento pode ser simulado para auxiliar na modelagem de novos perfis sem causar impactos no ambiente produtivo.

Controle de horário de *logon*

O horário de *logon* permitido para cada colaborador pode ser automaticamente configurado em função dos atributos cadastrados no sistema de RH.

Um controle dinâmico de exceções permite que eventualmente o horário de *logon* de um colaborador possa ser estendido após a devida aprovação.

Essa funcionalidade existe com os objetivos de evitar passivos trabalhistas por meio de um controle efetivo das horas extras e reforçar a segurança da informação.

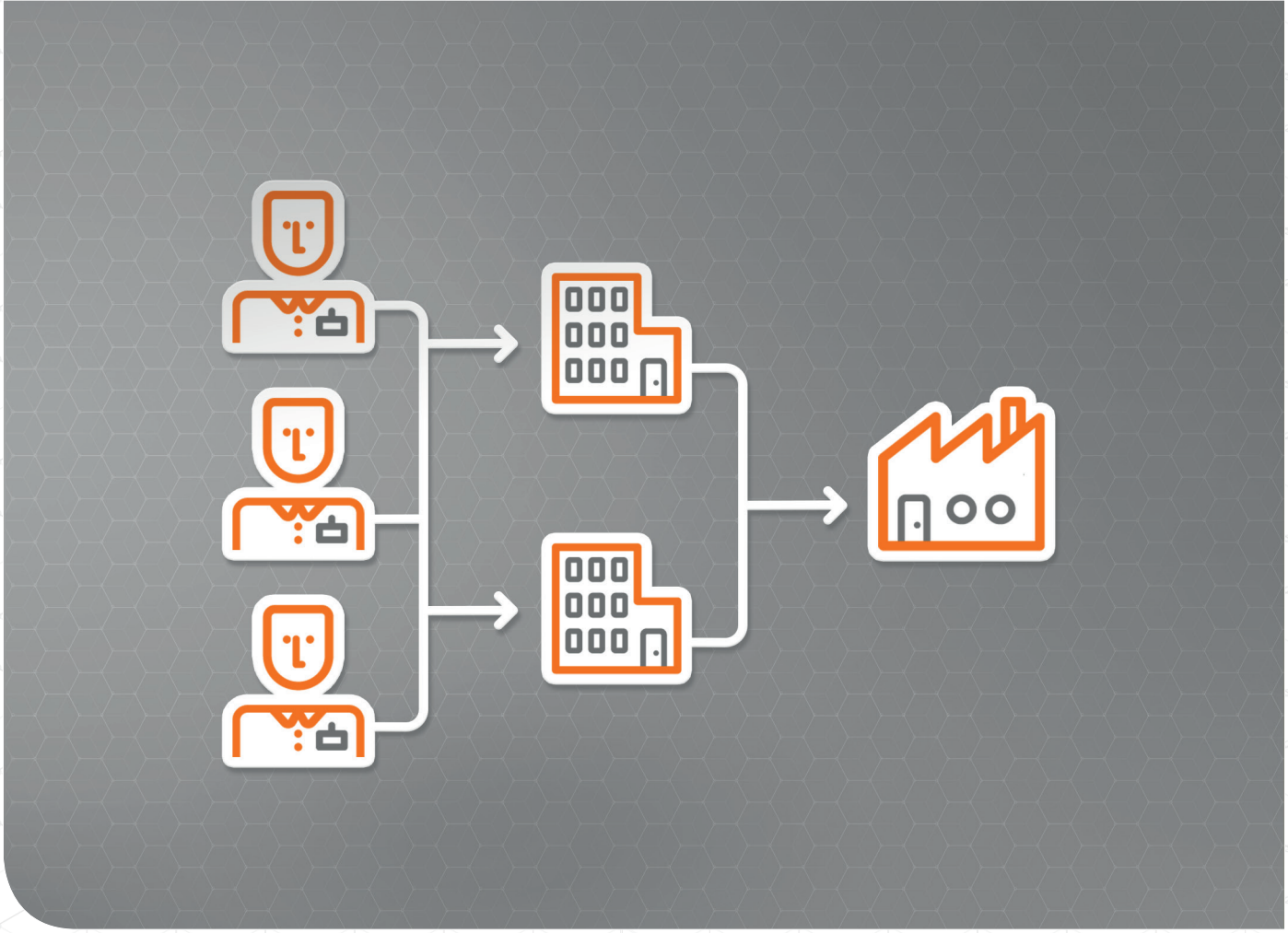
Recertificação periódica de acessos

O NetAdmin IAM permite a adoção de uma rotina agendada de recertificação de acessos a ser realizada pelos gestores e seus delegados.

O processo é disparado periodicamente e automaticamente de acordo com as configurações feitas pela equipe de Gestão de Acessos (GA) que, por sua vez, leva em conta os seguintes fatores: a data da última recertificação realizada; a classificação dos acessos envolvidos e o nível de risco associado aos acessos, dentre outros.

Os gestores utilizam uma interface que auxilia na compreensão dos acessos avaliados, facilitando a tomada de decisões. As ações de aprovação ou rejeição podem ser realizadas em lotes.

O processo de recertificação pode ser gerenciado pelo administrador da plataforma NetAdmin ou pela GA. Este processo conta com os seguintes recursos: relatórios de acompanhamento do processo; alteração do revisor e execução imediata da revisão. ■



Gestão de terceirizados

Cadastro de contratos, empresas contratadas e terceirizados

Para apoiar o gerenciamento das contas de colaboradores terceirizados, o NetAdmin IAM fornece um cadastro que vincula essas pessoas a suas empresas empregadoras e essas aos contratos com a empresa contratante. O número de identificação de cada contrato informado pode opcionalmente ser validado no ERP da empresa contratante.

A vinculação das contas a um contrato garante coerência de suas datas de expiração com a vigência do contrato, além de associá-las ao responsável pelo contrato.

Gestão das contas de terceirizados cadastrados em sistemas proprietários

Algumas empresas já possuem uma base de dados de terceirizados integrada aos seus processos de negócio.

O NetAdmin IAM pode utilizar os dados de uma base de terceirizados previamente existente para automatizar a gestão de identidade e acesso para esses colaboradores.

Gestão da data de expiração das contas de terceirizados

O NetAdmin IAM garante que todas as contas de terceirizados tenham uma data de expiração configurada.

As datas de expiração das contas de terceirizados são automaticamente limitadas ao término dos respectivos contratos, podendo ser antecipadas.

O NetAdmin IAM é capaz de identificar a proximidade da expiração de uma conta de terceirizado e notificar o responsável pela mesma para que solicite a prorrogação da data de expiração, se for necessário.

Gestão das permissões de acessos de terceirizados

As permissões de acesso das contas de terceirizados são gerenciadas da mesma forma que as dos demais colaboradores, inclusive com provisionamento automático e solicitação de acessos sob demanda. ■

Características adicionais

Escalabilidade

Os websites, serviços e bases de dados do NetAdmin IAM podem ser instalados em um mesmo servidor ou serem distribuídos em servidores especializados.

Os serviços responsáveis pela execução de ações automáticas podem ser instalados em múltiplos servidores, com distribuição da carga de trabalho entre eles.

Disponibilidade

Todas as informações operacionais do NetAdmin IAM são armazenadas em bases de dados relacionais que podem residir em servidores de bancos de dados configurados em *cluster*.

Os websites do NetAdmin IAM, incluindo o Portal de Troca de Senhas (PCP), os *web services* e a interface administrativa, podem ser implementados em ambientes de balanceamento de carga.

Segurança

O acesso dos usuários ao NetAdmin IAM é controlado por perfis, sendo que cada pessoa visualiza as informações e comandos apropriados.

Suporta o uso de protocolos seguros para comunicação entre seus componentes e os repositórios gerenciados, seja na camada de rede (a exemplo do IPsec) ou de transporte (a exemplo do HTTPS e do SSH).

As credenciais utilizadas no NetAdmin IAM para interação com outros sistemas são armazenadas com criptografia forte.

Gerenciabilidade

Todos os processos de automação do NetAdmin IAM podem ser monitorados individualmente quanto à ocorrência de eventuais falhas.

As configurações do NetAdmin IAM, incluindo as customizações da interface e conectores, são automaticamente versionadas, podendo ser revertidas se necessário. As configurações também podem ser transferidas entre ambientes de homologação e produção.

Usabilidade

A interface web é otimizada para os navegadores atuais e as soluções são portadas para diversos idiomas. ■

Relatórios

Investigação das permissões de acesso de um usuário

O NetAdmin IAM fornece uma visão consolidada de todas as identidades e permissões de acesso que um usuário possui nos diferentes sistemas da organização.

Também fornece o histórico detalhado das ações realizadas sobre a conta do usuário em questão, sejam automáticas ou sob demanda, incluindo o provisionamento e a revogação de acessos que ocorreram em todos os sistemas.

Investigação das permissões de acesso a um sistema ou recurso

O NetAdmin IAM permite visualizar as permissões de acesso de diferentes sistemas de maneira padronizada por meio de uma única interface.

Também é possível visualizar todos os usuários que possuem permissão de acesso a um determinado recurso, assim como o histórico de todas as ações de concessão ou revogação de permissões de acessos a um sistema ou recurso é consolidado.

Relatórios gerenciais, de conformidade e direcionados para auditoria

O NetAdmin IAM fornece inúmeros relatórios gerenciais para o acompanhamento da gestão de identidade e acesso.

Estão disponíveis relatórios específicos para a rápida identificação de não conformidades, assim como é possível gerá-los, sendo que alertas podem ser configurados para essas situações.

Também fornece os relatórios tipicamente solicitados pelas auditorias de segurança da informação, minimizando o esforço dos administradores para atender a essas demandas.

Notificações

O NetAdmin IAM permite que se cadastre indicadores para toda e qualquer informação coletada. Esses indicadores podem disparar um gatilho de alerta, a ser enviado de acordo com as configurações desejadas.

Relatórios customizados

Com o NetAdmin IAM é possível criar relatórios personalizados utilizando quaisquer informações coletadas no repositório, conforme a necessidade do usuário ou gestor. ■

NetAdmin SOFTWARE

NETADMIN® IAM 3.5

www.netadmin.software