Guia do Administrador do Ivanti Neurons for MDM 91

Abril de 2023

Conteúdo

Sobre o Ivanti Neurons for MDM

Além de ser uma abordagem moderna à segurança móvel, o Ivanti Neurons for MDM fornece soluções de gerenciamento unificado de pontos de extremidade (UEM) em uma infraestrutura altamente escalável, segura e fácil de atualizar, compatível com milhões de dispositivos em todo o mundo.

- Atualizações instantâneas: obtenha atualizações automáticas de software e segurança e acesso a novos recursos assim que estiverem disponíveis.
- Escalabilidade sob demanda: dimensione sua implantação conforme as necessidades do negócio mudam, sem ter que se preocupar com o planejamento da capacidade.
- Minimize os custos de hardware: ao eliminar a necessidade de manter o hardware presencial, os serviços baseados em cloud exigem espaço zero para serem gerenciados.
- Tempo de atividade elevado e alta disponibilidade.
- Aproveite os investimentos já existentes: realoque os recursos de TI da manutenção de hardware para tarefas mais estratégicas que agregam valor ao negócio.

É possível visualizar os resumos de "Resumo de novos recursos" na página 6 disponíveis nesta versão.

Resumo de novos recursos

Esta seção apresenta os resumos de novos recursos e aprimoramentos que estão disponíveis nesta versão. Referências à documentação descrevendo estes recursos e aprimoramentos também são disponibilizados, quando disponíveis.

"Recursos e aprimoramentos gerais" abaixo

"Recursos do iOS, macOS e tvOS" na página 8

"Recursos do Windows" na página 8

"Recursos da Defesa contra ameaças móveis" na página 9

Recursos e aprimoramentos gerais

- **Adição da coluna Status de Instalação do Aplicativo para dispositivos iOS, macOS e Android**: a partir da versão atual, a coluna Status de Instalação do Aplicativo na guia Aplicativos Disponíveis, na exibição Detalhes do Dispositivo, exibirá o status dos aplicativos no dispositivo. A coluna Status de Instalação do Aplicativo aparece por padrão.

  Não é possível classificar pelo status de instalação do aplicativo.

  Para mais informações, consulte "Introdução a dispositivos" na página 183.

- **Delegação com distribuição personalizada habilitada para configurações de Certificado e VPN por Aplicativo**: a partir da versão atual, os administradores globais poderão autorizar administradores de espaço a editar o certificado para todos os dispositivos e para a opção de distribuição personalizada.

  > As alterações de distribuição são aplicáveis somente ao espaço específico. Todos os outros espaços continuam herdando as configurações de distribuição de espaço padrão.

  - Configuração de VPN por aplicativo - já estão disponíveis opções de distribuição personalizadas
  - Configuração de certificado - opções de distribuição personalizadas agora estão disponíveis

    Para mais informações, consulte "Configuração do certificado" na página 538 e "Configuração VPN por aplicativo" na página 883.

- **Nova regra adicionada ao construtor de regras**: o atributo de filtro Dispositivo Registrado foi adicionado aos construtores de regras em Grupos de Dispositivos. O atributo permite filtrar os dispositivos que foram registrados em um horário específico. Para mais informações, consulte "Grupos de dispositivos" na página 202.

- **Atualizadas as permissões em Visualizar PIN de Registro do Usuário**: quando você aplica a função personalizada Visualizar PIN de Registro do Usuário, os usuários podem visualizar o PIN de outros usuários que tenham o mesmo nível de acesso ou privilégios menores e não podem criar PINs para outros usuários. Para mais informações, consulte "Gerenciamento de funções" na página 1177.

- **Suporte ao atributo Departamento no provisionamento de usuários SCIM**: a partir desta versão, o atributo Departamento será suportado no provisionamento de usuários SCIM. Para mais informações, consulte "Mapeando atributos" na página 1256.

- **Atualizado o processo Limpeza de Dispositivo**: o processo Limpeza de Dispositivo foi atualizado como segue:

  - **Configurações de dispositivos desativados** - renomeado para Dispositivos desativados. Foram adicionadas opções agendadas de frequência de desativação.
  - **Excluir configurações de dispositivos desativados** - renomeado para Excluir dispositivos desativados. Foram adicionadas opções agendadas de frequência de exclusão.
  - **Excluir dispositivos apagados** - opção adicionada na versão atual.

    Para mais informações, consulte "Configurações de Limpeza de Dispositivo" na página 1170.

Recursos do iOS, macOS e tvOS

- **Renovação automática de certificados para dispositivos iOS**: a partir desta versão, o certificado Go Client para dispositivos iOS é renovado automaticamente dentro de 30 dias após o vencimento.
- **Renovação automática de certificados de identidade de dispositivo N-MDM para dispositivos Apple**: a partir desta versão, o certificado de identidade de dispositivo para dispositivos Apple é renovado automaticamente dentro de 30 dias após a expiração.
- **Novos detalhes de dispositivo foram adicionados**: foram adicionados estes novos detalhes de dispositivo para dispositivos iOS e macOS:
  - **Versão de compilação suplementar**
  - **Extra da versão/SO suplementar**

    Os detalhes da versão estão disponíveis da seguinte forma:
    - Dispositivos > Dispositivos > Detalhes > Visão geral
    - Dispositivos > Dispositivos > menu suspenso Selecionar colunas
    - Pesquisa avançada > construtor de regras
    - Política personalizada > construtor de regras
    - Espaços > construtor de regras
      Para mais informações, consulte "Introdução a dispositivos" na página 183, "Política personalizada" na página 1106, "Gerenciamento de espaços" na página 1190.

Recursos do Windows

- **Definir a prioridade do aplicativo durante a instalação**:ao instalar um aplicativo do Windows, o administrador pode definir o nível de prioridade no qual a instalação do aplicativo deve ocorrer. Para obter mais informações, consulte "Configuração do aplicativo" na página 354.
- **Reordenar scripts de pré ou pós-instalação para arquivos .EXE**: o administrador agora pode reordenar os scripts ou arquivos de pré ou pós-instalação e priorizá-los para arquivos .EXE. Para mais informações, consulte "Gerenciar aplicativos Windows" na página 425.

- **Suporte para adicionar ícones ao carregar aplicativos internos do Windows**: ao carregar aplicativos internos do Windows para o App Catalog, o administrador agora pode incluir ícones junto com os aplicativos. Para mais informações, consulte "App Catalog" na página 301.
- **Instalação de aplicativos EXE durante o registro no Autopilot**: os aplicativos .EXE serão instalados nos modos de implantação automática e orientado ao usuário durante o processo de registro no Autopilot. Para mais informações, consulte "Configuração de perfis do Windows Autopilot" na página 1324.
- **Gerenciamento de aplicativos EXE em dispositivos Windows**: os aplicativos .EXE podem ser gerenciados nos modos de autoimplantação ou pré-provisionamento em dispositivos Windows. Para mais informações, consulte "Gerenciar aplicativos Windows" na página 425.
- **Suporte a dispositivos Windows LTSC**: o Ivanti Neurons for MDM agora oferece suporte a dispositivos instalados no Windows LTSC.
- **Configuração personalizada de CSP**: o administrador pode criar, configurar e distribuir CSPs personalizados usando o esquema OMA-URI. Para obter mais informações, consulte "Configuração personalizada" na página 459.

Recursos da Defesa contra ameaças móveis

A Defesa contra ameaças móveis (MTD) protege dispositivos gerenciados contra ameaças e vulnerabilidades móveis que afetam o dispositivo, a rede e os aplicativos. Para mais informações sobre recursos relacionados à MTD, conforme aplicáveis para a versão atual, consulte o Guia de soluções defesa contra ameaças móveis para sua plataforma, disponível na seção DEFESA CONTRA AMEAÇAS MÓVEIS na página de Documentação do produto da Ivanti.

Cada versão do guia MTD contém todos os recursos da Defesa contra ameaças móveis que foram completamente testados e estão disponíveis atualmente para uso tanto em ambientes de cliente e de servidor. Por causa da diferença entre as versões do servidor e do cliente, as novas versões do guia MTD ficarão disponíveis com a versão final da série quando os recursos estiverem totalmente operantes.

Introdução

Esta seção oferece visões gerais da configuração e utilização dos recursos que requerem interação no portal do Ivanti Neurons for MDM. Esta seção contém os seguintes tópicos:

Visão geral da solução

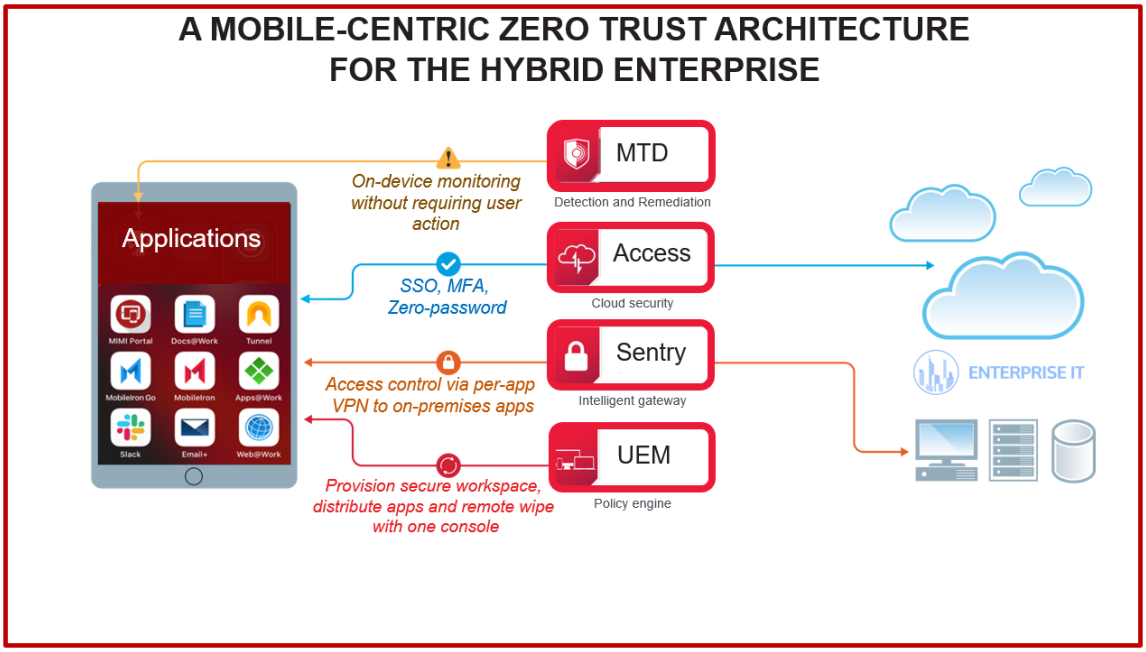
O acesso contínuo a dados de negócios em dispositivos móveis e outros endpoints fora da rede corporativa exige um foco dedicado à segurança. Para atender às necessidades de segurança atuais, as empresas devem considerar como elas podem:

- Provisionar endpoints como telefones celulares e laptops
- Conceder acesso baseado em um conjunto de dados imperativos
- Proteger dados em repouso e em movimento
- Impor medidas conforme necessário

A solução da Ivanti para esse problema moderno atende a todos os desafios. Você pode monitorar endpoints e acionar políticas adaptáveis para remediar ameaças, deixar dispositivos em quarentena e manter a conformidade. Juntos, os componentes a seguir ajudam sua organização a realizar a estrutura Zero Trust centrada em dispositivos móveis:

- **Ivanti Neurons for MDM** – Ajuda a criar um espaço de trabalho seguro em qualquer dispositivo com apps, configurações e políticas para o usuário com base em sua função. Os usuários têm acesso fácil e seguro aos recursos necessários para a produtividade
- **Sentry** – Um gateway inteligente em linha que ajuda seu acesso seguro aos recursos presenciais
- **Access** – Ajuda a verificar o usuário, o dispositivo, o aplicativo, o tipo de rede e a presença de ameaças. A verificação adaptável do controle de acesso é a base do modelo Zero Trust. O Access oferece login único e segurança no Cloud
- **Defesa contra ameaças móveis** – A combinação do Ivanti Neurons for MDM com a Defesa contra ameaças móveis (MTD) protege os dados presenciais e na rede com criptografia de última geração e monitoramento de ameaças para detectar ataques em nível de dispositivo, rede e aplicativos

A ilustração a seguir mostra a visão geral da solução:



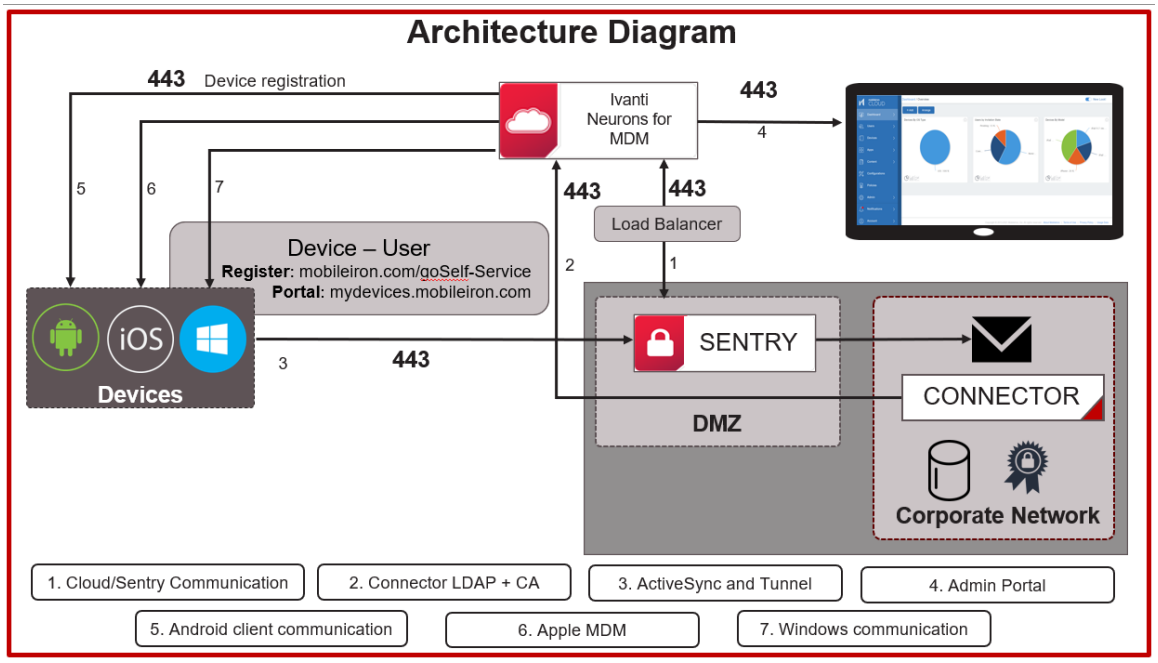
Principais recursos

A plataforma Ivanti Neurons for MDM oferece a visibilidade e os controles de TI necessários para proteger, gerenciar e monitorar qualquer dispositivo móvel ou desktop, corporativo ou pertencente ao usuário, que acesse dados empresariais de importância crítica. Ivanti Neurons for MDM A plataforma permite que as organizações protejam uma ampla gama de dispositivos de funcionários usados dentro da organização, além de gerenciar todo o ciclo de vida dos dispositivos, incluindo:

- Gerenciamento e aplicação da configuração de políticas
- Distribuição e gerenciamento de aplicativos
- Gerenciamento e distribuição de scripts para dispositivos desktop
- Ações do dispositivo
- Controle de acesso e autenticação multifator
- Detecção e remediação de ameaças

Diagrama da arquitetura

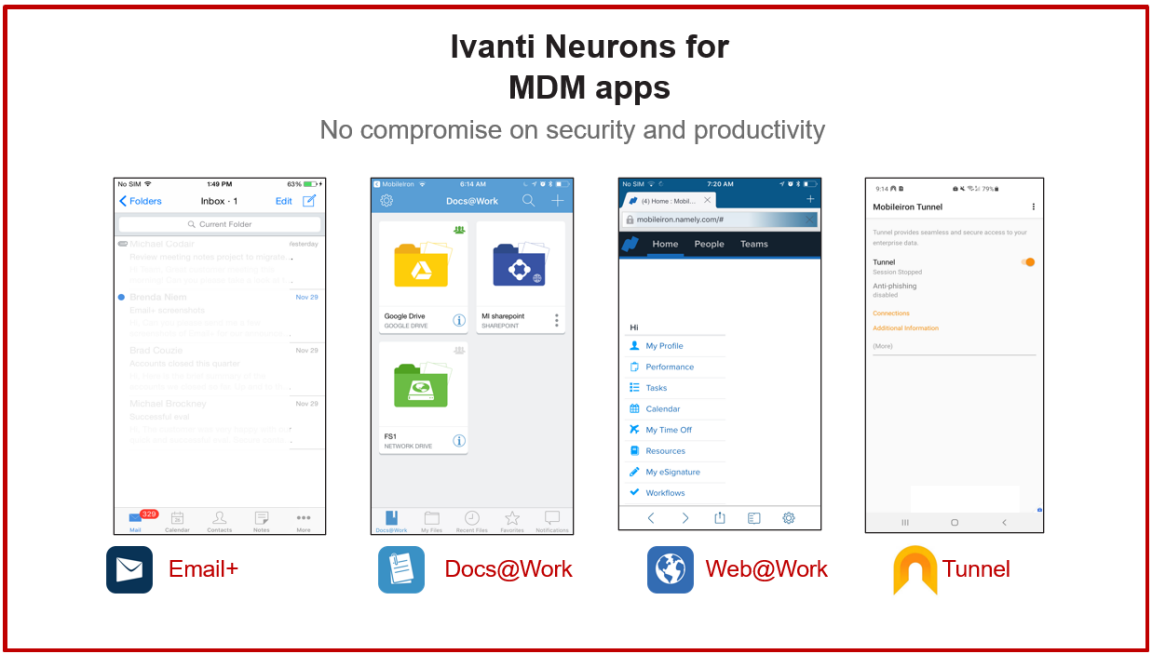
O diagrama a seguir mostra a visão geral da arquitetura da plataforma Ivanti Neurons for MDM UEM:



Ivanti Neurons for MDM aplicativos

- **App Catalog** – O App Catalog é uma vitrine de aplicativos corporativos personalizável. Os administradores de TI podem enviar diretamente aplicativos privados ou internos para os dispositivos de seus usuários finais. O App Catalog também pode ser combinado com o Apple Volume Purchase Program para facilitar uma distribuição segura de aplicativos móveis em dispositivos iOS. Futuramente, a Ivanti pode aproveitar os recursos encontrados nos aplicativos gerenciados do iOS e no Android Enterprise. Isso facilita, dentro da plataforma Ivanti Neurons for MDM UEM, a configuração de definições para aplicativos e políticas de segurança para ambas as funções avançadas de segurança do aplicativo.
- **Email+** – Uma plataforma cruzada para proteger o aplicativo PIM para iOS e Android. O Email+ oferece e-mail, calendário, contatos e tarefas protegidos em dispositivos pessoais e de propriedade de empresas ao se comunicar com um servidor ActiveSync em sua empresa.
- **Docs@Work** – Permite que os usuários acessem, criem, editem, façam marcações e compartilhem conteúdos de forma segura de repositórios, como o Microsoft SharePoint, e de serviços de nuvem, como o Box e o Dropbox. Isso é importante para que os usuários possam maximizar a produtividade durante as atividades.
- **Web@Work** – É um navegador seguro que permite que os usuários corporativos acessem com segurança o conteúdo da Web na intranet corporativa. Usando o Web@Work, você pode limitar o acesso a dados corporativos para usuários autorizados. Quando o Web@Work for implementado em conjunto com o AppTunnel, você terá protegido os dados corporativos em movimento. Com o Web@Work, os usuários podem acessar os recursos internos da Web de forma rápida e fácil.

A imagem a seguir mostra os aplicativos Ivanti Neurons for MDM:



Funções

Administrador – Como um Administrador corporativo, você é responsável pelas tarefas a seguir:

- Ofereça aos usuários da empresa um acesso contínuo e seguro aos e-mails do espaço de trabalho, aos aplicativos, às configurações e à conectividade, como Wi-Fi e VPN.
- Separe os dados pessoais dos dados corporativos nos dispositivos de funcionários para que os dados corporativos não sejam vazados em aplicativos pessoais e para que os dados pessoais não sejam acessados pela TI acidentalmente.

Usuário – Enquanto um usuário corporativo, você pode acessar continuamente os aplicativos comerciais e dados pessoais em dispositivos móveis, desktops e serviços de nuvem modernos e seguros. Para obter mais informações sobre todas as tarefas que você pode executar enquanto usuário, consulte a seção "Usuários" na página 86.

Introdução

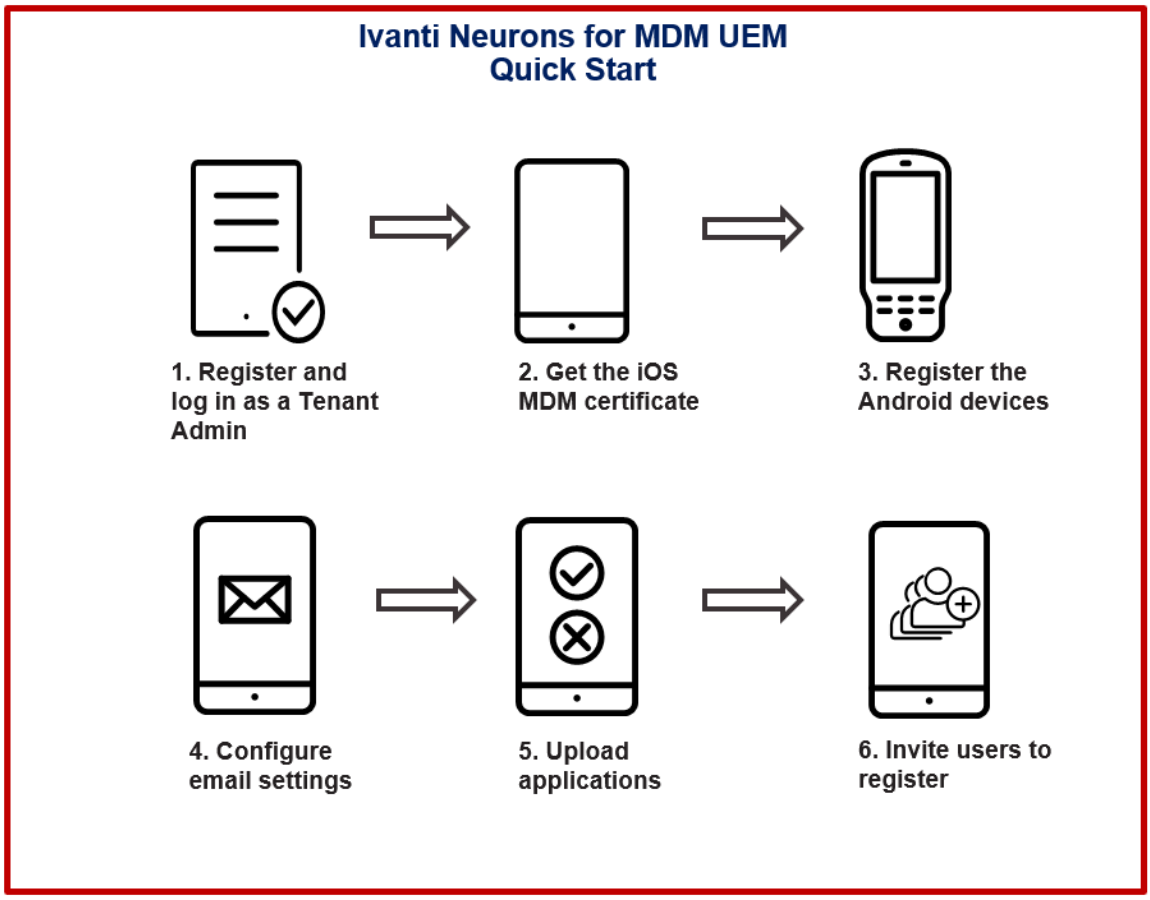
Se você for um novo usuário registrado, siga as etapas apresentadas nesta seção para ser integrado rapidamente aos serviços do Ivanti Neurons for MDM.

Assim que você se inscrever na plataforma Ivanti Neurons for MDM, a Ivanti criará um locatário do Ivanti Neurons for MDM para você. Você receberá um e-mail no endereço de e-mail registrado. Esse e-mail trará um PDF com as seguintes informações a respeito do locatário criado para sua empresa:

- Informações sobre o pacote de softwares que você adquiriu
- A URL e as credenciais de login de superadministrador do locatário
- Como acessar a Comunidade de Suporte e as Perguntas Frequentes do Ivanti Neurons for MDM
- Onde acessar a documentação técnica e fazer download do software

Ivanti, Inc não fornece chaves de software. Ao fazer login em seu locatário do Ivanti Neurons for MDM com as credenciais de Superadministrador e aceitar os termos de serviço, você ativa o produto Ivanti Neurons for MDM.

O digrama a seguir mostra as etapas para começar com o Ivanti Neurons for MDM:



Procedimento

1. Clique na URL fornecida no e-mail de registro de locatário. A solicitação de redefinição de senha aparece.
2. Altere sua senha.
3. Faça login na conta de locatário usando o ID e a senha. O assistente de boas-vindas aparece.
4. Preencha os detalhes no formulário **Boas-vindas**, aceite os termos e o acordo e clique em **Continuar**.
5. Para instalar o certificado de MDM do iOS, consulte "Instalar certificado de MDM" na página 1305.

   Se você quiser gerenciar seus dispositivos iOS em um momento posterior, pode pular a instalação do certificado de MDM do iOS. Em seguida, o assistente solicitará que você registre os dispositivos Android de sua empresa. Ignorar a instalação do certificado MDM do iOS significa que os dispositivos iOS não poderão ser registrados. Os usuários verão uma mensagem declarando que o registro do dispositivo iOS não foi habilitado.

6. Para registrar os dispositivos Android no modo Android Enterprise (AE), consulte "Contas gerenciadas do Google Play (Contas com Android Enterprise)" na página 1387. Em seguida, o assistente solicita que você configure as contas de e-mail.

   Se você quiser gerenciar seus dispositivos Android em um momento posterior, pode pular o registro da conta gerenciada do Google Play do Android. Ignorar o registro da conta do Google Play gerenciada não permitirá que você registre dispositivos Android Enterprise. Os dispositivos Android ainda podem ser registrados com o Administrador do dispositivo, mas os principais recursos, como o Google Play gerenciado e a Configuração do aplicativo, não estarão disponíveis para uso.

7. Para definir as configurações de e-mail e do ActiveSync, consulte " Configuração do Exchange" na página 814 e "Configuração de e-mail" na página 808.
8. Clique em **Continuar**. A solicitação de criação de senha aparece.
9. Selecione uma senha e clique em **Continuar**.
10. Selecione os aplicativos que você deseja carregar e clique em **Continuar**.

11. Especifique os endereços de e-mail dos usuários e clique em **Continuar**. Os usuários receberão um e-mail para registrar seus dispositivos móveis. Um resumo da configuração é exibido.
12. Clique em **Concluído**. A página Painel será exibida.
13. Para continuar explorando, faça o seguinte:
    - Acesse **Usuários** . Todos os usuários convidados são listados.
    - Acesse **Apps**. Todos os aplicativos que você carregou estão listados.
    - Vá até **Configurações**. Todas as configurações que você enviou durante o registro estão listadas.

Para obter mais informações sobre todas as tarefas que você pode executar enquanto administrador, consulte a seção "Administrador" na página 1162.

Como configurar o idioma preferido em um navegador

Se o usuário tiver definido um idioma do navegador sem suporte, ele poderá definir en_US (inglês, Estados Unidos) como o idioma padrão do portal.

Para definir a preferência de idioma em um navegador Safari executado em dispositivos macOS 10.15+, os usuários podem realizar a configuração da seguinte forma:

1. No dispositivo macOS, acesse **Preferências do sistema**.
2. Acesse **Idioma e Região > Geral**.
3. Defina **en_US** (ou qualquer outra opção de idioma) como o **Idioma preferido**.

Interface de navegação unificada para Ivanti Neurons for MDM e Access

Para novos clientes em alguns clusters, o Access está disponível como uma interface de navegação unificada com o Ivanti Neurons for MDM. Faça login com suas credenciais de administrador do Ivanti Neurons for MDM. As opções do Access estão disponíveis no painel de navegação esquerdo como uma guia separada. Acesse Documentação do produto e clique em Access para obter mais informações sobre o Access e como configurar o Access.

A interface de navegação unificada inclui os seguintes recursos:

- Login unificado para Ivanti Neurons for MDM e Access.
- Seletor de produtos no painel de navegação esquerdo para alternar entre Ivanti Neurons for MDM e Access.
- Memória de seleção de produto: após o primeiro login, o portal de administração do Ivanti Neurons for MDM é exibido. Nos logins subsequentes, aparece o Ivanti Neurons for MDM ou o Access, refletindo o produto selecionado no primeiro login.
- Painel de navegação esquerdo para Ivanti Neurons for MDM e Access.
- Painel de configurações unificadas da conta com links para opções, como Opções de atualização, Documentação, Portal de suporte, Alterar senha e Sair.

Modo de Administração de dispositivos (DA) de gerenciamento de dispositivos Android – descontinuado

O modo Administração de Dispositivos (DA) para gestão dispositivos Android está sendo descontinuado gradualmente do Ivanti Neurons for MDM 78 em diante.

Nenhum novo usuário com novo locatário criado no Ivanti Neurons for MDM 78 poderá registrar dispositivos (Android 6 e posteriores) no modo DA. Todos os novos locatários que precisam habilitar o registro de DA no Android 6 ao Android 9 devem entrar em contato com o Suporte Ivanti.

- Dispositivos Android 10 e posteriores continuarão bloqueados para registro no modo DA.
- Para usuários existentes (com ou sem implantações de DA), não há mudanças em termos de gerenciamento dos dispositivos DA existentes (Android 6 a Android 11). No entanto, ao atualizar para o Ivanti Neurons for MDM78, qualquer dispositivo recém-registrado executando o Android 10+ em locatários existentes também não terá permissão para rodar no modo DA. Esses locatários existentes só seriam capazes de registrar dispositivos das versões Android 6 a Android 9 no modo DA.
- Se algum usuário estiver planejando migrar dispositivos DA de uma instância do Core para o Ivanti Neurons for MDM R78, certifique-se de que o Android Enterprise esteja habilitado e pelo menos uma configuração do sistema seja distribuída para o conjunto de destino: PO, DO ou COPE antes de acionar a migração. Essa etapa é essencial para evitar a desativação de dispositivos após a migração.

Tipo de registro de DA	Locatário existente (atualizado para 78)	Novo locatário 78 (não atualizado)
Novo registro DA do dispositivo com SO >= 10	Não permitido	Não permitido
Novo registro DA do dispositivo com SO < 10	Permitido	Não permitido
Dispositivos DA existentes com SO >= 10	Permanecerá ativo	N/D
Dispositivos DA existentes com SO < 10	Permanecerá ativo	N/D
Dispositivos DA migrados com SO >= 10	Desativará	Desativará
Dispositivos DA migrados com SO < 10	Permanecerá ativo	Desativará

Configurar dispositivos macOS

Esse é um tópico de visão geral que fornece uma lista de procedimentos comuns e outros conteúdos relacionados à configuração de dispositivos macOS no Ivanti Neurons for MDM. Você pode acessar todos os tópicos de macOS no *Ivanti Neurons for MDMGuia do administrador*.

Conteúdo

Registrar dispositivos

A maioria dos usuários começa registrando um dispositivo. Você pode usar uma das seguintes abordagens para iniciar o processo de registro:

- Envie um convite para um ou mais usuários finais (registro iReg). Para mais informações, consulte o tópico *Registro de Dispositivo macOS* na seção Registro de dispositivo.
- Registro de dispositivos e Registro de usuários com Apple Business Manager

Para obter mais informações, consulte Registro do dispositivo.

Configurar modelo de convite de usuário

Você pode atribuir a marca ao convite de email do usuário final para deixá-lo com uma aparência mais familiar para seus usuários finais. Para obter mais informações, consulte Modelos de e-mail de identidade visual.

Você pode personalizar o processo de registro do dispositivo com nomes e logotipos que seus usuários reconhecerão. Para obter mais informações, consulte Identidade visual do usuário.

Para obter mais informações, consulte Como configurar e usar e-mails de confirmação de registro.

Configurar recursos do Zero Sign-on

Para documentação relacionada ao Zero Sign-On, consulte Zero Sign-On com acesso no *Guia de acesso*.

Para registro automatizado de toque zero, consulte o tópico Configurações do usuário, seção Configuração de definições para registros de novos dispositivos, Etapa 13.

Configurar Mobile@Work para cliente macOS

O aplicativo Mobile@Work para macOS fornece:

- Recursos de script em dispositivos macOS
- App Catalog para usuários finais
- Notificações por push
- Tela de integração do usuário (boas-vindas/status) para registros de dispositivos automatizados

Antes de enviar o Mobile@Work aos usuários finais, certifique-se de que a "Mobile@Work para macOS" na página 684 esteja criada e pronta para ser distribuída aos dispositivos macOS de destino.

Você pode ativar a integração do usuário para dispositivos macOS durante o processo automatizado de Registro de dispositivos. Assim que o Registro do dispositivo é concluído, o Mobile@Work para macOS é transferido para o dispositivo juntamente com os perfis, configurações e apps.

Configurar scripts shell macOS

O Ivanti Neurons for MDM permite criar seus próprios scripts shell do macOS, que podem então ser carregados no Ivanti Neurons for MDM e executados em dispositivos macOS gerenciados.É possível configurar os scripts usando a Configuração de scripts do Mobile@Work para macOS. O Mobile@Work para macOS retorna os resultados da execução do script para Ivanti Neurons for MDM, que são mostrados nos logs do dispositivo. Você pode consultar os logs do dispositivo na página de detalhes do dispositivo macOS na guia **Logs**. Para mais informações sobre a criação, upload e gerenciamento de repositório de scripts, consulte Todos os scripts.

Antes de executar scripts shell em dispositivos macOS, verifique se os usuários possuem o aplicativo Mobile@Work para macOS em execução em seus dispositivos e se possuem uma configuração do Mobile@Work para macOS transferida para seus dispositivos. Os scripts podem ser executados uma vez ou de maneira recorrente. O script no Ivanti Neurons for MDM também permite que os administradores coletem informações de um dispositivo para armazená-las no Ivanti Neurons for MDM como um atributo personalizado. Por exemplo, se você precisar saber a versão Java em um dispositivo macOS, é possível coletar essas informações e armazená-las por dispositivo em um atributo de dispositivo personalizado. Para obter mais informações, consulte *Como criar uma configuração Script do Mobile@Work para macOS* em Mobile@Work para macOS.

Definir configurações de macOS

As configurações são conjuntos de definições enviados aos dispositivos. Por exemplo, você pode usar configurações para instalar automaticamente configurações de VPN e requisitos de senha nesses dispositivos. Use a página **Configurações** para selecionar, definir e distribuir configurações. Existem vários tipos de configurações disponíveis.Na página, é possível visualizar uma lista de configurações macOS disponíveis, incluindo as seguintes configurações:

- Wi-Fi
- Senha
- VPN
- DNS criptografado
- FileVault 2
- Chave de recuperação do FileVault
- Firewall do macOS
- Restrições do macOS
- Restrições de macOS AppStore
- Configurações do Finder do macOS
- Política de extensão Kernel de macOS
- Active Directory (macOS)
- Criação de conta automática do Office 365 (macOS)

Você pode usar configurações personalizadas para importar e distribuir um arquivo de configuração predefinido.

Configurar políticas de macOS

As políticas definem requisitos para dispositivos e o que acontecerá se um dispositivo não cumprir os requisitos. Toda política é composta por uma regra e uma ação de conformidade (o que acontece se a regra for violada). Use a página **Políticas** para selecionar, configurar e distribuir as políticas. Proteção/criptografia de dados desabilitada e Apps permitidos são políticas relacionadas a macOS. Você pode usar Políticas personalizadas para criar uma política personalizada com base nos atributos de usuário e de dispositivo, critérios de seção, valores e ações de conformidade especificados por você.

Distribuir apps macOS

Ivanti Neurons for MDM dá suporte à distribuição de apps macOS por meio do protocolo MDM da Apple e usando o aplicativo Mobile@Work. Os administradores podem escolher usar uma ou ambas as seguintes abordagens:

- Protocolo MDM da Apple – Os administradores podem carregar apenas formatos PKG específicos (formato de distribuição) como apps internos e também podem distribuir a partir da Mac App Store (o suporte a licença de Apps e Books da Apple é incluído). No entanto, essa abordagem não permite que os administradores distribuam DMG e outros formatos PKG.
- Aplicativo Mobile@Work para macOS - como uma maneira de distribuir apps a usuários, os administradores podem usar o aplicativo MobileIron Packager (MIP) para converter qualquer arquivo PKG, DMG ou .app em um arquivo MIP. Carregue o arquivo MIP no Ivanti Neurons for MDM como um aplicativo interno.

É possível baixar o utilitário Mac Packager da Ivanti Neurons for MDM nos downloads de software da MobileIron.

Os administradores podem usar o Mobile@Work para distribuir apps internos que estejam no formato DMG, PKG ou .app. Para apps que estejam disponíveis apenas na Mac App Store, os administradores podem continuar usando recursos de MDM nativos da Apple, o que inclui recursos de licença de Apple Apps e Books.

Verificar relatórios e outras informações

O Painel exibe estatísticas importantes sobre dispositivos e usuários registrados. Cada seção no painel é chamada de widget.

Você pode verificar informações adicionais da seguinte maneira:

- Revisão de notificações - Vá até a página **Painel > Notificações** (ou clique no ícone de sino [canto superior direito]) para revisar as notificações e tomar medidas necessárias.
- Relatórios - Vá até a página **Painel > Relatórios** para acessar os dados em seu sistema de Gerenciamento de Terminal Unificado (UEM).
- Trilhas de auditoria – vá até a página **Painel > Trilhas de auditoria** para acessar o conjunto cronológico de registros que capturam atividades realizadas em todas as entidades dentro do Ivanti Neurons for MDM. Para ativar esse recurso, vá até a página **Administrador > Infraestrutura > Trilhas de auditoria** e clique em **Ativar trilhas de auditoria**.
- Insights de aplicativo – vá até a página **Painel > Insights de aplicativo** para exibir e analisar a distribuição do aplicativo e outros detalhes.

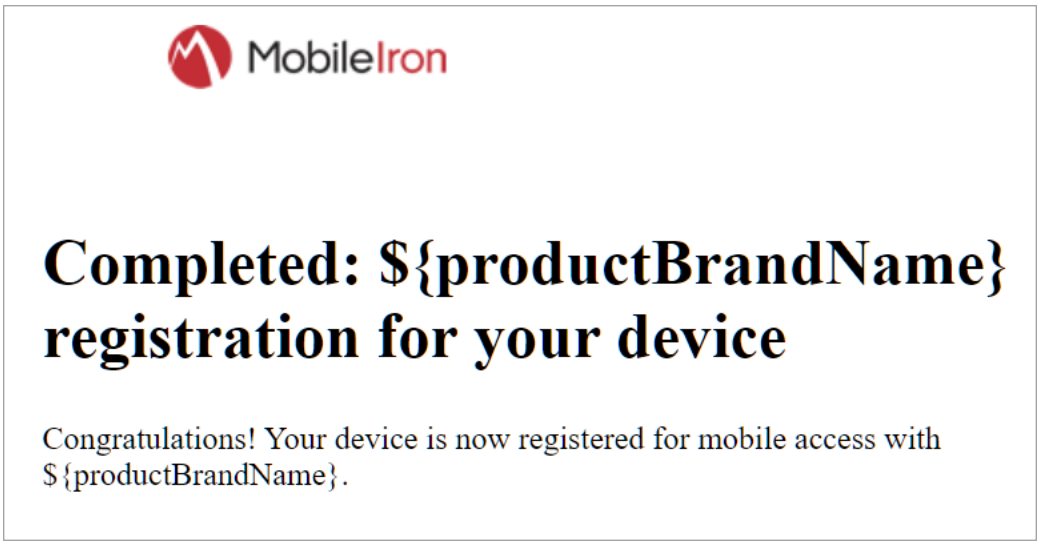
Como configurar e usar e-mails de confirmação de registro

Os administradores podem configurar e acionar e-mails para os usuários após a conclusão do registro. Esse e-mail pode conter, por exemplo, instruções adicionais para os usuários após o registro feito com sucesso. Os administradores podem ativar o envio desse e-mail durante o convite do usuário.

O processo:

- **Como configurar o recurso:**
  - Configure o modelo do e-mail.

    O modelo de e-mail em inglês se parece com isso por padrão, mas você pode revisá-lo para melhor atender às suas finalidades, seguindo as instruções em "Personalizando um modelo de e-mail" na página 1434 em "Colocar marca em modelos de email" na página 1432:

  - Ative o e-mail de confirmação do registro. Consulte "Como configurar e-mails de confirmação de registro do usuário" na página 113 em "Configurações do usuário" na página 98.

- **Como usar o recurso:**
  - Envie ao usuário o convite para se registrar, conforme descrito em "Como convidar usuários" na página 156. Quando o usuário se registrar com sucesso, a Ivanti Neurons for MDM enviará a esse usuário um e-mail de confirmação do registro.

Configurando e usando e-mails de notificação de conformidade com políticas

Os administradores podem agrupar em um modelo de e-mail de notificação de conformidade com políticas os e-mails enviados pelas políticas de Apps personalizados e permitidos, enviando ações por e-mail a usuários cujos dispositivos estão fora de conformidade. O processo a seguir descreve a configuração:

- **Como configurar o recurso:**
  - **Configure o modelo de e-mail**.

    O modelo de e-mail em inglês se parece com isso por padrão, mas você pode revisá-lo para melhor atender às suas finalidades, seguindo as instruções em "Personalizando um modelo de e-mail" na página 1434 em "Colocar marca em modelos de email" na página 1432:

  - **Ative o modelo de notificação de conformidade com as políticas**. Este modelo funciona em conjunto com a mensagem que você cria usando as ações de envio de e-mail das políticas de Aplicativos personalizados e permitidos. O Ivanti Neurons for MDM insere as informações especificadas nessas ações por e-mail no modelo de notificação de conformidade com políticas. Você pode ativar o modelo de e-mail de conformidade com políticas ao criar ou editar uma política de Aplicativos personalizados ou permitidos. Para obter mais instruções sobre a ativação do modelo de notificações de conformidade com políticas para uma política personalizada ou uma política de apps permitidos, consulte "Adicionando uma política personalizada" na página 1106 e "Criando uma política de aplicativos permitidos" na página 1146 respectivamente.
- **Como usar o recurso:**
  - Quando um dispositivo fica fora de conformidade com uma política de aplicativos Personalizados ou Permitidos com o modelo de notificação de política ativado, o Ivanti Neurons for MDM envia um e-mail ao proprietário do dispositivo, primeiro envolvendo o e-mail no modelo de notificação de política. Sua interação com o recurso é configurá-lo conforme resumido acima, já que o próprio Ivanti Neurons for MDM utiliza o recurso.

Recursos sob demanda

Ivanti Neurons for MDM inclui alguns recursos sob demanda que estão desabilitados por padrão. Tais recursos podem ter algum impacto no desempenho e podem ainda não estar totalmente prontos para implementação na produção.

Os administradores podem entrar em contato com o Suporte se quiserem ativar um ou mais recursos sob demanda que estejam desativados por padrão nos dispositivos do(s) locatário(s).

A tabela a seguir inclui a lista de recursos sob demanda documentados:

Recurso	Descrição	Plataforma(s)	Licença
Recursos do Windows 10	Recursos aplicáveis aos dispositivos Windows 10.	Windows 10	• Pacote legado: Gold • Pacote atual: UEM seguro Consulte a seção "Pacotes" na página 1449 para obter mais informações sobre ofertas legadas e atuais.
Copiar a URL do catálogo do aplicativo para a área de transferência	Fornece a habilidade para os administradores de copiar a URL do catálogo do aplicativo para a área de transferência para apps. Esta URL pode ser distribuída aos usuários via e-mail. Se o usuário clicar
no link a partir de um dispositivo registrado, o catálogo do aplicativo com o aplicativo será
aberto no navegador, onde o usuário poderá escolher instalar o
aplicativo. Os administradores são responsáveis por restringir a distribuição desta URL aos usuários destinados.	• iOS • macOS	NA (específico do locatário)

Recurso	Descrição	Plataforma(s)	Licença
Configurar um clipe da Web como um aplicativo	Configure um clipe da Web como um aplicativo no App Catalog para disponibilizar o aplicativo da Web no App Catalog para os usuários. O clipe da Web pode ser definido como uma configuração, mas uma configuração pode ser enviada somente pelo administrador. Os usuários podem optar por instalar o aplicativo da Web em seus dispositivos ou por não instalá-lo, mas os usuários não podem optar por não instalar uma configuração de clipe da Web.	iOS	NA (específico do locatário)
Ativar registro de dispositivos permitidos	Permite o registro de dispositivos com base nos números de série permitidos em Usuários > Configurações do usuário > Configuração padrão de registro de dispositivo.	• iOS • macOS	NA (específico do locatário)
Autenticação baseada em certificado	O recurso Autenticação baseada em certificado permite aos administradores fazer login usando certificados digitais e um nome de host especificado pelo locatário ou um nome de host personalizado.Essa autenticação pode ser definida usando a Configuração de host personalizado na guia **Admin**.	Este recurso não é específico da plataforma.	NA (específico do locatário) Este recurso está disponível apenas em ambientes de cluster NA3, e apenas se for ativado pelo suporte.

Recurso	Descrição	Plataforma(s)	Licença
Criar uma configuração de dispositivos dedicados (de uso único de propriedade da empresa ou COSU)	Os administradores podem configurar dispositivos dedicados que podem ser usados para uma finalidade específica com o Android Enterprise usando a configuração de dispositivos dedicados (uso único de propriedade da empresa, ou COSU). A configuração COSU é distribuída para dispositivos gerenciados de trabalho (modo Proprietário do dispositivo) para fornecer apenas um aplicativo disponível para os usuários no modo quiosque.	Android Enterprise	Licença
Período de inatividade do painel	Por padrão, o período de inatividade do painel está definido como 15 dias. Esse valor pode atualizado conforme as necessidades do locatário para, no máximo, 30 dias. Se você precisar de um período de inatividade mais longo, entre em contato com a equipe de Suporte.	Este recurso não é específico da plataforma.	

Preparando-se para suporte a dispositivos Android Enterprise

Esta seção descreve os requisitos mínimos de rede para dispositivos Android Enterprise. Os dispositivos Android normalmente não exigem a abertura de portas de entrada no firewall para funcionamento correto. No entanto, há várias conexões de saída às quais os administradores precisam estar atentos ao configurar os ambientes de rede para dispositivos com Android corporativo.

A lista de alterações de rede fornecida na tabela a seguir não é completa e pode variar. Ela abrange pontos de extremidade conhecidos para versões atuais e anteriores de apps GMS e API de gerenciamento corporativo.

Além das portas listadas na tabela a seguir, os dispositivos Android Enterprise exigem acesso ao Ivanti Neurons for MDM.

A tabela a seguir lista os requisitos para dispositivos Android Enterprise:

Host de destino	Portas	Finalidade
play.google.com android.com google-analytics.com googleusercontent.com gstatic.com *.gvt1.com *ggpht.com dl.google.com android.clients.google.com	TCP/443 TCP, UDP/5528-5230	Google Play e atualizações (APKs, logotipos de apps, etc.) gstatic.com, googleusercontent.com – Com Conteúdo gerado pelo usuário (por exemplo, ícones de aplicativo na loja) *.gvt.com, *.ggpht, dl.google.com, android.clients.google.com – Baixe apps e atualizações, APIs da PlayStore
*googleapis.com	TCP/443	UEM/APIs da Google/APIs da PlayStore
accounts.google.com	TCP/443	Autenticação

Host de destino	Portas	Finalidade
fcm.googleapis.com fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging (por exemplo, Localizar Meu Dispositivo, Console UEM <-> comunicação DPC, como configurações por push)
pki.google.com clients1.google.com	TCP/443	Revogação de certificado
clients[2...6]. google.com	TCP/443	Domínios compartilhados por vários serviços de back-end da Google, como relatórios de pane, sincronização de indicadores do Chrome, sincronização de horário (tlsdate) e muitos outros.

A Google não fornece IPs específicos. É necessário permitir que seu firewall aceite conexões de saída a todos os endereços IP contidos nos IPs bloqueados listados no ASN 15169 da Google http://bgp.he.net/AS15169#_prefixes.

Os IPs dos nós de bordas e pares do Google não estão listados nos blocos AS15169. Consulte ://peering.google.com/ para mais informações sobre a Rede de borda do Google.

Painel

O painel exibe estatísticas importantes sobre dispositivos e usuários registrados.Cada seção no painel é chamada de widget. Para cada widget, você define:

- a categoria de dados exibida (como dispositivos ou usuários)
- o modo de agrupamento dos dados (tal como o modelo ou a versão do SO)
- o modo de filtragem dos dados (tal como exibir somente dispositivos iOS ou por versão de compilação do SO)
- como os dados são exibidos (num gráfico circular ou de barras)

Esta seção contém os seguintes tópicos:

Trabalhando com widgets

Esta seção contém os seguintes tópicos:

O painel exibe estatísticas importantes sobre dispositivos e usuários registrados.Cada seção no painel é chamada de widget. Para cada widget, você define:

- a categoria de dados exibida (como dispositivos ou usuários)
- como os dados são agrupados (como o modelo ou a versão do SO)
- como os dados são filtrados (somente dispositivos iOS, por exemplo)
- como os dados são exibidos (num gráfico circular ou de barras)

Adicionando um widget

1. Clique em **Adicionar** (canto superior direito).
2. Atribua um nome ao widget.
3. Selecione uma categoria de dados.
4. Conclua as opções de filtragem, conforme elas são exibidas.
5. Selecione o tipo de exibição padrão (gráfico circular, de barras, com linhas).
6. Clique em **Concluído** .

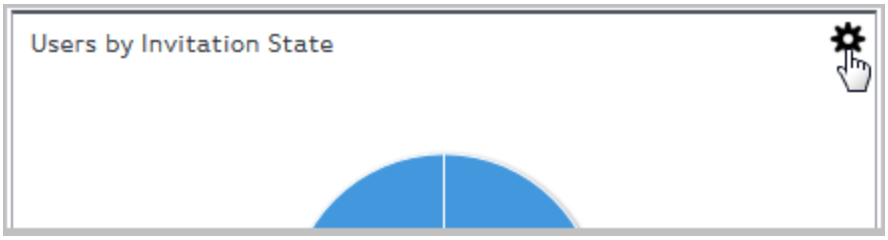
Organizando os widgets

São exibidos sempre três widgets por linha. Entretanto, você pode alterar a ordem em que os widgets são exibidos:

1. Clique em **Organizar** (canto superior direito).
2. Arraste as caixas na ordem em que os widgets devem ser exibidos.
3. Clique em **OK**.

Editando um widget

1. Clique no ícone de configurações para o widget (canto superior direito).



2. Selecione **Editar**.
3. Faça suas alterações.
4. Clique em **Concluído** .

Revisando notificações

Clique no ícone de sino (canto superior direito) ou acesse a página **Painel > Notificações** para revisar as notificações e realizar ações, quando necessário, com base nos seguintes critérios:

- Tipo de componente
  - Aplicativo
  - LDAP
  - AAD
  - Lista de dispositivos permitidos

    - Apps and Books
    - iOS
    - Android
    - Locatário
    - CA
    - Conector
    - Token do servidor do Registro de dispositivos
- Tipo de notificação
    - Expiração
    - Sincronização de dados
    - Limite de uso
    - Ação do administrador
    - Erro de autenticação do servidor
    - Erro de validação
    - Mudança de status
- Severidade
    - Excluído
    - Informações
    - Crítico
    - Perigo

Os administradores podem selecionar o componente Aplicativo para revisar rapidamente todas as notificações específicas do aplicativo na página Notificações e também na seção de notificação do sino. Se houver novas permissões para serem aceitas para apps do Google Play, os administradores poderão aceitá-las clicando nas notificações, em vez de acessar cada página de aplicativo para revisar e aceitar as permissões.

Ivanti Neurons for MDM os clientes/locatários receberão notificações de aprovação do aplicativo Android Go mesmo que o aplicativo Android Go não seja importado para o Catálogo de Aplicativos.

Repassar a expiração de senha de usuário e notificações de alteração de ID

Os administradores podem analisar as futuras expirações de senha na página **Notificações**. Eles também são notificados das expirações de senha com duas semanas até um dia de antecedência, incluindo links para arquivos de relatório em CSV que contêm a lista de usuários correspondentes. Após a senha expirar, as notificações não serão mais geradas.

Os Administradores também podem repassar uma notificação que alista os usuários com IDs (UIDs) que foram detectados com alterações durante a última sincronização LDAP.

Apagando uma notificação

É possível apagar manualmente essas notificações de qualquer severidade sempre que necessário na página **Notificações**.

1. Na página **Notificações**, clique no ícone na coluna **Ações** para ver a notificação que deseja apagar. A janela **Confirmar Apagar notificação** é exibida.
2. Clique em **Apagar notificação**. Quando apagada, o status da notificação é alterado para **Apagado** na coluna **Status**.

   A contagem total das notificações que são apagadas é exibida na página **Notificações**.

Relatórios

Na página **Painel > Relatórios**, é possível acessar os dados em seu sistema de Gerenciamento de Terminal Unificado (UEM). Por exemplo, os administradores podem adicionar informações como Nome do espaço do dispositivo e Atributos personalizados do dispositivo aos relatórios usando a opção de filtro correspondente ao criar relatórios de Dispositivos e Dispositivos bloqueados. Desta forma, esses relatórios têm colunas para Nome do espaço do dispositivo e Atributos personalizados do dispositivo, respectivamente. Os Atributos personalizados do dispositivo estão disponíveis nas opções de filtro ao criar um relatório. Os administradores podem escolher na lista de chaves de atributo de dispositivo personalizadas usadas para dispositivos e selecionar os operadores disponíveis.

A partir do Ivanti Neurons for MDM 76, os operadores para todos os modelos de relatório possuem operadores padrão. Os operadores dos seguintes modelos são padronizados nesta versão:

- Painel > Relatórios > Criar relatório

Este é o fluxo de trabalho de um relatório:

1. Escolher – Selecione em um modelo predefinido de relatório.
2. Definir escopo – Defina o período dos dados de relatório.
3. Definir detalhes – Dê um nome e personalize seu relatório.
4. Executar ou agendar – Execute o relatório imediatamente ou crie um agendamento.
5. Compartilhar – Especifique quem receberá o relatório.

Tópicos relacionados:

- Painel > Relatórios (Agendados)
- Painel > Relatórios (Personalizados)

Pesquisa rápida: navegue até a guia Relatórios. O campo de pesquisa rápida permite pesquisar nas seguintes colunas, mesmo se você incluir espaço ou caracteres especiais:

- NOME
- DESCRIÇÃO
- NOME DO MODELO

Trilhas de auditoria

Trilhas de auditoria são um conjunto cronológico de registros que captura as atividades realizadas em todas as entidades dentro do Ivanti Neurons for MDM por qualquer participante, incluindo administradores e usuários finais, e por diversos componentes do próprio sistema. A partir do Ivanti Neurons for MDM versão 80, as Trilhas de Auditoria estão ativadas por padrão para todos os locatários. O locatário pode optar por ativar ou desativar as Trilhas de auditoria de registro de dispositivos. Para os locatários que estavam ativados com Trilhas de auditoria antes da R80, os eventos de registro permanecem ativados. Para os dispositivos de todos os outros locatários, as trilhas de registro estão desativadas. Quando você registra novamente um dispositivo Android, a página Trilhas de Auditoria exibe o status do dispositivo atualmente registrado como Ação Novo Registro de Dispositivo executada e a entrada anterior como Ação Desativar Dispositivo executada. Para mais informações, consulte "Registro de dispositivo (iOS, macOS e Android)" na página 222.

As atividades a seguir são rastreadas:

- Adicionar, retirar, excluir e atualizar dispositivos
- Forçar registro nos dispositivos
- Alterar propriedade do dispositivo
- Criar, atualizar e excluir configurações do usuário (configurações de Registro do dispositivo, Limite do dispositivo e Termos de serviço)
- Bloquear e desbloquear dispositivos
- Criar, editar, excluir e priorizar configurações
- Criar, editar e excluir políticas
- Alterações no grupo de distribuição das configurações.
- Criação, edição e exclusão de usuários (não inclui a criação de usuários LDAP).
- Criação, edição e exclusão de grupos de usuários.
- Criação, edição e exclusão de filtros de distribuição.
- Criação, edição e exclusão de servidor LDAP.

- Sincronização com o servidor LDAP nos seguintes cenários:
  - Início da sincronização do LDAP
  - Sucesso na sincronização do LDAP
  - Descarte da sincronização do LDAP (ocorre quando a exclusão do número de usuários excede o valor de limite configurado).
  - Descarte parcial de sincronização do LDAP (ocorre quando há entradas com falha durante a sincronização)
  - Servidor LDAP adicionado
  - Servidor LDAP editado
  - Servidor LDAP excluído
  - Sincronização do servidor LDAP iniciada
  - Sincronização do servidor LDAP falhou
  - Sincronização do servidor LDAP concluída
- Criação, edição e exclusão de apps.
- Criação, edição e exclusão de configurações de aplicativo.
- Criar, editar e excluir scripts.
- Excluindo a entidade LDAP de administrador.
- Modificando preferências de LDAP.
- Carregando certificado LDAP.
- Alteração do ícone do aplicativo.

Ativando Trilhas de auditoria

Você precisa ativar o recurso Trilhas de Auditoria para capturar as atividades executadas no Ivanti Neurons for MDM.

1. Selecione **Administrador > Infraestrutura > Trilhas de auditoria**. A página **Trilhas de auditoria** é exibida.
2. Clique em **Ativar trilhas de auditoria**. A janela **Ativar trilhas de auditoria?** é exibida para confirmar sua ação de ativar as trilhas de auditoria.
3. Na janela **Ativar trilhas de auditoria?**, clique em **Ativar trilhas de auditoria**.

   Você não poderá desativar o recurso Trilhas de auditoria após ativá-lo. Para desativá-lo, entre em contato com o suporte.

4. No campo **Exportar Trilhas de auditoria**, deslize a barra de alternância para **ATIVADO** para configurar a exportação das Trilhas de auditoria. A exportação das Trilhas de auditoria é usada para exportar e carregar todas as informações das Trilhas de auditoria em um local específico do servidor. A exportação das Trilhas de auditoria é executada pelo SSH File Transfer Protocol (SFTP). O servidor deve estar acessível a partir da porta padrão. Os usuários podem definir configurações da exportação de trilhas de auditoria para carregar arquivos das trilhas de auditoria automaticamente em um local específico diariamente. Para mais informações, veja Exportando trilhas de auditoria.

Visualização das atividades da Trilha de auditoria

Você pode visualizar as atividades rastreadas na página **Trilhas de auditoria** em **Painel**. Se um item de linha se estender além da largura padrão da coluna e estiver oculto devido à borda da coluna, reticências são exibidas e, ao passar o mouse sobre as reticências, o item de linha completo é exibido como uma dica de ferramenta.

Os seguintes detalhes são exibidos nessa visualização:

Nome da coluna	Descrição
Nome	Nome do dispositivo ou nome da configuração do usuário. Por exemplo, para atividades do dispositivo, ela exibe o nome do dispositivo. Você pode clicar no hiperlink para acessar a página de detalhes da atividade. Se houver um usuário associado ao dispositivo, o nome de usuário do proprietário do dispositivo também será exibido no nome do dispositivo. Clique no ícone do link **Ir para dispositivo** ao lado do nome do dispositivo para navegar até a página de detalhes do dispositivo. Na página Detalhes do dispositivo, você pode clicar no hiperlink **Ir para Trilhas de auditoria** para visualizar a página de detalhes de atividade de Trilhas de auditoria.
Tipo	Tipo de atividade que é acionada. Exemplo: 'conta' para uma atividade de login.
Categoria	Os categoria da atividade. Exemplo: Configuração, Política.
Última atividade	A última atividade realizada. Exemplo: Criar, Excluir.
Último usuário	Os usuário que executou a atividade.
Realizado em	A data e a hora da atividade realizada ficam visíveis apenas no formato de 24 horas.

Visualização dos detalhes da atividade

A Exibição de Detalhes da Atividade (camada interna) é acessada clicando-se no link sob a coluna **Nome** na Exibição de Entidades e lista todas as trilhas de atividades históricas relativas a essa entidade. Os seguintes detalhes são exibidos nessa visualização: Se um item de linha se estender além da largura padrão da coluna e estiver oculto devido à borda da coluna, reticências são exibidas e, ao passar o mouse sobre as reticências, o item de linha completo é exibido como uma dica de ferramenta.

Nome da coluna	Descrição
Horário da ação	Os tempo que passou desde que a ação foi executada.
Atividade	Descreve a ação específica executada. Exemplo: aplicativo adicionado ao App Catalog.
Realizado por	Os usuário que executou a atividade.
Alterações - antes e depois	Clique no ícone para visualizar os detalhes de comparação de trilha de auditoria na janela **Alterações nas trilhas de auditoria – Antes e depois**.

Os seguintes detalhes são exibidos na janela **Alterações nas trilhas de auditoria - antes e depois**.

Nome da coluna	Descrição
Atributo	Exibe o nome do atributo modificado. Exemplo: **createdAt**.
Antes	Valores do atributo antes de a ação ser realizada.
Depois de	Valores do atributo depois de a ação ser realizada.

Com o ícone de configuração **Personalizar colunas** exibido no canto superior direito do cabeçalho da coluna, é possível selecionar ou desmarcar a caixa de seleção do nome da coluna relevante para exibir/ocultar as colunas na visualização de lista.

Filtragem das atividades da Trilha de auditoria

Usando a opção **Filtros** você pode filtrar e visualizar a lista de atividades da Trilha de Auditoria. Estas são as opções de filtragem disponíveis:

Opções de filtragem	Descrição
Filtrar por intervalo de datas	Selecione o período nos campos Data de início e Data de término. Quando o intervalo é selecionado, a lista de atividades da Trilha de auditoria executadas no período selecionado é listada. Esta opção de filtro está disponível em qualquer uma das opções de exibição (agrupadas ou expandidas). Somente um máximo de 15 dias pode ser selecionado como intervalo tendo a data final como a data atual.
Categoria (Aplicável somente na Visualização expandida)	Selecione a categoria entre as seguintes opções: • **Política** • **Gerenciamento de dispositivos** • **Gerenciamento de usuários** • **Gerenciamento da configuração do usuário** • **LDAP** • **Configuração** • **Acesso ao portal do administrador** • **Aplicativo Gerenciamento** • **Conformidade do dispositivo do Azure** A coluna Categoria é ocultada por padrão na visualização expandida.

Opções de filtragem	Descrição
Tipo (Aplicável somente na Visualização expandida)	Selecione as seguintes opções de **Tipo de entidade**: • **Conta** • **Dispositivo** • **Autenticação de registro** • **Limite de dispositivos** • **Termos de serviço** • **Relatório de conformidade** A coluna Tipo é ocultada por padrão na visualização expandida.
Atividade (Aplicável somente na Visualização expandida)	Selecione as atividades específicas que deseja visualizar. As opções são as seguintes: • **Excluir** • **Atualização da distribuição** • **Forçar check-in** • **Limpar erro de configuração** • **Desativar** • **Login** • **Atualizar** • **Atualizar proprietário** • **Apagar** • **Bloquear** • **Atualizar conformidade do Intune**

Opções de filtragem	Descrição
Nome (Aplicável somente na Visualização expandida)	Filtra por nome do dispositivo ou nome da configuração do usuário.
Realizado por	Filtra pelos usuários que executaram a ação.
Status	Filtra pelo status de login. As opções são: • **Bem-sucedido** • **Falha**

A ordem da exibição é baseada no horário que a atividade foi executada.

Com o ícone de configuração **Personalizar colunas** exibido no canto superior direito do cabeçalho da coluna, é possível selecionar ou desmarcar a caixa de seleção do nome da coluna relevante para exibir/ocultar as colunas na visualização de lista.

Por padrão, as páginas listam 50 atividades. Se houver mais de 50 atividades, clique no botão **Avançar** na parte inferior da página para exibir mais atividades. Como alternativa, você também pode clicar na opção de exibição relevante no campo **Mostrar**, localizado na parte inferior da página. Por exemplo, clique em **100** para exibir a lista das 100 atividades mais recentes.

Procurando atividades de Trilha de auditoria

Usando o campo Pesquisar, você pode encontrar e visualizar a lista de atividades da Trilha de auditoria com base na palavra-chave inserida. Atualmente, quando você realiza uma pesquisa rápida, toda a string é indexada incluindo os nomes de propriedade. A partir do Ivanti Neurons for MDM 76, somente os valores de propriedade são indexados. Os usuários não precisam fornecer as chaves de detalhes presentes na coluna de detalhes ao realizar uma pesquisa rápida. A palavra-chave inserida pode ser o valor aplicável a qualquer uma das seguintes colunas:

- **Nome** (nome do dispositivo ou nome do usuário)
- **Tipo**
- **Categoria**

- **Realizado por**
- **Detalhes**

Não é possível pesquisar os valores na coluna Atividade.

O resultado exibido também incluirá as atividades da Trilha de auditoria que tiverem correspondência entre qualquer parte dos valores da coluna e a palavra-chave inserida. Por exemplo, as atividades de Trilha de auditoria que tiverem o valor "Fulano" na coluna Nome serão exibidas quando a palavra-chave inserida no campo Pesquisar for "ano".

Exportar trilhas de auditoria para um arquivo CSV

Você pode exportar os registros de trilha de auditoria usando a opção Exportar para CSV na página Trilhas de Auditoria.

Procedimento

1. Vá até **Painel** > **Trilhas de auditoria**.
2. Clique no menu suspenso **Ações** e selecione a opção **Exportar para CSV** . Como alternativa, você pode filtrar por intervalo de datas antes de selecionar a opção Exportar para CSV.
   Uma mensagem pop-up aparece informando que o relatório de exportação pode levar algum tempo para ser processado. Aguarde a conclusão da solicitação antes de enviar outra.
3. Clique em **Baixar**. Você receberá um e-mail contendo um link para baixar o relatório.
4. (Opcional) Clique em **Excluir** para excluir o relatório.

Se você não conseguir visualizar a página **Painel**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Percepção de aplicativo

Esta seção contém os seguintes tópicos:

O Percepção de aplicativo é um recurso no Painel que o ajuda a visualizar e analisar a seguinte distribuição de aplicativo:

- Distribuições de aplicativo interno que precisam de instalação
- Distribuições de aplicativo público que precisam de instalação
- Apps do iOS não gerenciados
- Os 10 principais apps gerenciados instalados
- 5 apps internos com melhor classificação

Análise dos cinco principais apps que precisam ser instalados: esses são apps públicos ou internos distribuídos a um grande número de usuários, mas que têm taxas de instalação proporcionalmente baixas. O gráfico de apps do iOS não gerenciados apresenta informações sobre os apps não gerenciados nos dispositivos. Você pode ver a lista de apps não gerenciados e os dispositivos onde eles estão instalados, e tomar medidas para converter o aplicativo em um aplicativo gerenciado. Essas são as distribuições de aplicativo que exigem a atenção do administrador ou alguma ação para melhorá-las. Esses gráficos representam os dispositivos que já têm o aplicativo instalado. O gráfico de rosca apresenta uma visão geral de alto nível da distribuição de apps públicos e internos que não apenas ajuda a analisar o número de dispositivos que exigem a instalação de aplicativo, como também permite examinar em mais detalhes para obter mais informações específicas do aplicativo clicando em uma região específica do gráfico. Além disso, você também pode incluir um único gráfico de distribuição que represente a distribuição específica para a versão de um único aplicativo.

 O painel mostra somente informações sobre dispositivos verificados nos últimos 15 dias.

Visualizando a distribuição do aplicativo

Na página **Apps** em **Painel**, você pode ver os seguintes gráficos:

- Distribuição de aplicativo interna que requer instalação
- Distribuição de aplicativo pública que requer instalação
- Apps do iOS não gerenciados

Os gráficos de 5 apps internos, 5 apps públicos e apps iOS não gerenciados são exibidos por padrão. Os gráficos são ordenados da esquerda para a direita começando com o aplicativo com a taxa mais alta de não instalação.

Os gráficos de rosca exibem duas cores para representar o status de instalação. A cor azul representa o número de dispositivos em que o aplicativo está instalado. A cor vermelha representa o número de dispositivos que exigem instalação. A contagem de dispositivos será exibida se você passar o cursor do mouse sobre cada região de cor.

Você pode excluir um gráfico clicando na opção excluir no canto superior direito do gráfico.

Visualizando detalhes do aplicativo

O centro do gráfico de rosca também exibe o número de dispositivos que exigem instalação. Exemplo: 750/1.000, o que significa que 750 de 1.000 dispositivos exigem instalação.

Os gráficos de rosca exibem três cores para representar a distribuição do aplicativo.

- A cor azul representa o número de dispositivos em que o aplicativo está instalado. Clicar na região azul no gráfico o leva para a página **Dispositivos**. Na página **Dispositivos**, a coluna **Versão do aplicativo** exibe a versão do aplicativo instalado e a data em que ele foi instalado.

  > Você também pode visualizar dispositivos pelas versões de aplicativo instaladas selecionando as opções na seção **Versões**, no painel esquerdo.

- A cor vermelha representa o número de dispositivos que exigem instalação do aplicativo. Clicar na região vermelha no gráfico o leva para a página **Dispositivos**. Na página **Dispositivos**, você pode ver os dispositivos que exigem a instalação do aplicativo.

Um ícone de aplicativo é exibido no centro do gráfico. Clicar no ícone o leva para a página de detalhes do aplicativo em **Apps > App Catalog**.

Nessa página, clique na guia **Dispositivos com aplicativo instalado** para ver a lista de dispositivos para o aplicativo selecionado.

Clique na guia **Dispositivos sem aplicativo instalado** para visualizar a lista de dispositivos não instalados para o aplicativo selecionado.

Adicionando gráficos de distribuição de aplicativo único

Você pode adicionar gráficos de rosca de distribuição únicos para uma versão específica de um aplicativo na página Apps. A cor vermelha representa a lista de dispositivos elegíveis que devem ter o aplicativo instalado. Esses gráficos representam os seguintes detalhes da distribuição dos apps:

- Dispositivos instalados com uma versão específica do aplicativo
- Dispositivos com outras versões do aplicativo
- Dispositivos não instalados com o aplicativo

Procedimento

1. Clique em **+Adicionar** na página **Apps**. A janela **Adicionar gráfico de aplicativo** é exibida.
2. Na lista suspensa **Tipo de gráfico**, selecione **Distribuição de aplicativo único**.

3. Marque a caixa de seleção para a lista de apps para os quais você deseja visualizar o gráfico de distribuição de aplicativo único.

   > Como alternativa, você pode pesquisar um aplicativo específico digitando o nome do aplicativo no campo Pesquisar aplicativos.

4. Clique em **Adicionar gráfico**. Os gráficos de distribuição de aplicativo único são exibidos na página Apps.

   > Você pode selecionar um máximo de nove aplicativos na lista.

O centro do gráfico exibe o número de dispositivos que estão instalados com a versão do aplicativo especificada.

Exemplo: 5/10, que indica que cinco de 10 dispositivos estão instalados com a versão do aplicativo especificada.

Os gráficos de rosca exibem três cores para representar a distribuição do aplicativo.

- A cor verde representa o número de dispositivos em que a versão específica do aplicativo está instalada. Clique na região verde no gráfico para acessar a página **Dispositivos**, que exibe a lista de dispositivos instalados com a versão especificada do aplicativo. Você também pode visualizar dispositivos com base em outras versões do aplicativo instaladas selecionando as opções na seção **AppVersion** no painel esquerdo.
- A cor verde-clara representa o número de dispositivos em que outra versão do aplicativo está instalada. Clique na região verde-claro no gráfico para acessar a página **Dispositivos**, que exibe a lista de dispositivos instalados com outras versões do aplicativo. Você também pode visualizar dispositivos em outras versões do aplicativo instaladas selecionando as opções de versão na seção **AppVersion** no painel esquerdo.
- A cor vermelha representa o número de dispositivos em que o aplicativo não está instalado. A contagem de dispositivos será exibida se você passar o cursor do mouse sobre cada região de cor. Clicar na região vermelha no gráfico o leva para a página **Dispositivos**, na qual você pode visualizar os dispositivos instalados no aplicativo. O painel esquerdo mostra também a data a partir da qual o aplicativo está disponível no App Catalog.

Um ícone de aplicativo é exibido no centro do gráfico. Clicar no ícone o leva para a página de detalhes do aplicativo em **Apps > App Catalog**. Nessa página, clique na guia **Dispositivos com aplicativo instalado** para ver a lista de dispositivos para o aplicativo selecionado. Clique na guia **Dispositivos sem aplicativo instalado** para visualizar a lista de dispositivos não instalados para o aplicativo selecionado.

Você pode excluir um gráfico clicando na opção excluir no canto superior direito do gráfico.

Adicionando um gráfico de apps do iOS não gerenciados

Você pode identificar e visualizar a lista de aplicativos não gerenciados adicionando o gráfico de aplicativos iOS não gerenciados à página Apps. Este gráfico aparece automaticamente quando um administrador adiciona um aplicativo iOS não gerenciado ao catálogo. O administrador pode excluir ou adicionar esse gráfico conforme necessário.

Procedimento

1. Clique em **+Adicionar** na página **Apps**. A janela **Adicionar gráfico de aplicativo** é exibida.
2. Na lista suspensa **Tipo de gráfico**, selecione **Apps iOS não gerenciados exclusivos**.
3. Clique em **Adicionar gráfico**. O gráfico de apps iOS não gerenciados é exibido na página **Apps**.

O gráfico exibe o número de apps do App Catalog que não são gerenciados. A parte inferior do gráfico exibe três colunas com os seguintes detalhes:

- **Dispositivos com apps do iOS não gerenciados** – Indica o número de apps do iOS não gerenciados. Clique no link para exibir a lista de dispositivos com apps não gerenciados na janela Dispositivos com apps do iOS não gerenciados.
- **Total de apps no App Catalog** – Exibe o número total de apps disponível no App Catalog.
- **Apps iOS não gerenciados (%)** – indica a porcentagem de apps iOS não gerenciados.

Quando um aplicativo já foi instalado por meio da iTunes App Store, você pode converter o aplicativo e seus dados em um aplicativo gerenciado. Para isso:

1. Clique no link de número na **coluna Dispositivos com apps do iOS não gerenciados**. A janela **Apps do iOS não gerenciados exclusivos** é exibida.
2. Selecione um ou mais apps não gerenciados na lista e clique no link de número em apps iOS não gerenciados. Os apps selecionados serão convertidos em gerenciados e o status será atualizado no próximo registro do dispositivo.

> Para exportar os dados sobre aplicativos não gerenciados em formato CSV, clique no link **Exportar para CSV**.

Adicionando dez principais apps gerenciados instalados

Você pode identificar e visualizar a lista dos 10 principais aplicativos gerenciados instalados usando um gráfico de Principais 10 aplicativos gerenciados instalados na página Apps. O administrador pode excluir ou adicionar este gráfico conforme necessário.

Por padrão, o gráfico Principais 10 apps gerenciados instalados está disponível na página **Apps**. Se o gráfico for excluído, o administrador poderá adicioná-lo da página **Apps**.

Procedimento

1. Clique em **+Adicionar** na página **Apps**. A janela **Adicionar gráfico de aplicativo** é exibida.
2. Na lista suspensa **Tipo de gráfico**, selecione **Principais 10 apps gerenciados instalados**.
3. Clique em **Adicionar gráfico**. O gráfico dos dez principais apps gerenciados instalados é exibido na página **Apps**.

Você pode ver os principais 10 apps gerenciados instalados com base na categoria selecionada na lista suspensa **Mostrar**. As categorias disponíveis são:

- **Todos os apps** (selecionado por padrão)
- **Apps internos**
- **Apps públicos**

Cada barra no gráfico é exibida para representar cada aplicativo específico; o nome do aplicativo também é exibido. Focalize cada barra para ver a plataforma (Android, iOS ou Windows) e o número de dispositivos instalados com o aplicativo.

Clicar na barra de um aplicativo específico navega para a página **Dispositivos** que exibe os detalhes dos dispositivos instalados com o aplicativo. O painel esquerdo na página Dispositivos indica o número de dispositivos instalados com o aplicativo. Clicar no botão X no painel esquerdo navega de volta à página **Apps** no Painel.

Você pode excluir o gráfico clicando na opção excluir no canto superior direito do gráfico.

Adicionando cinco apps internos com melhor classificação

Você pode identificar e visualizar a lista dos 5 apps internos com melhor avaliação usando o gráfico 5 apps internos com melhor avaliação na página Apps. O administrador pode excluir ou adicionar este gráfico conforme necessário.

Por padrão, o gráfico 5 apps internos com melhor avaliação está disponível na página **Apps**. Se o gráfico for excluído, o administrador poderá adicioná-lo da página **Apps**.

Procedimento

1. Clique em **+Adicionar** na página **Apps**. A janela **Adicionar gráfico de aplicativo** é exibida.
2. Na lista suspensa **Tipo de gráfico**, selecione **5 apps internos com melhor avaliação**.
3. Clique em **Adicionar gráfico**. O gráfico dos cinco apps internos com melhor classificação é exibido na página **Apps**.

Este gráfico representa os dados por meio de um logotipo do aplicativo e uma classificação por estrelas. A classificação por estrelas é representada por imagens de estrelas e uma representação em um número inteiro (sendo 5 a classificação máxima). Também é exibido o número de usuários que classificaram o aplicativo.

O número de classificações de um aplicativo não corresponde apenas aos dispositivos restritos ao administrador e espaço em questão, mas sim a todos os usuários do aplicativo. A classificação é a média de todas as classificações dadas ao aplicativo pelos usuários que o visualizaram no Apps@Work em seus dispositivos registrados.

Clique no aplicativo específico para acessar a página **Detalhes do aplicativo**, que exibe os respectivos detalhes.

Você pode excluir o gráfico clicando na opção excluir no canto superior direito do gráfico.

Usando relatórios agendados

Licença: Silver

O recurso Relatórios Agendados permite agendar e gerar relatórios sobre várias métricas com modelos prontos para uso. Você deve ter a função de Administrador de sistema ou de Somente leitura do sistema para acessar este recurso. Atualmente, você pode criar no máximo 40 relatórios.

O relatório de Violações de política pode ter diversos registros para um mesmo dispositivo se este tiver diversas instâncias do Tunnel criadas para ele. Isso se aplica tanto para os relatórios padrão quanto para os relatórios personalizados.

Gerando um relatório

Você pode agendar e gerar um relatório.

Procedimento

1. Acesse **Painel** > **Relatórios**.
2. Clique em **Criar um relatório** para exibir a página Escolher um modelo de relatório.

3. Escolha um modelo para o relatório a partir das opções configuradas.

    - **Dispositivos bloqueados** - relatório sobre dispositivos com acesso atualmente bloqueado pelo Sentry.
    - **Dispositivos** - relatório sobre os dispositivos de todas as partições no seu sistema.
    - **Violações de política** - relatório sobre violações de política em seu sistema.
    - **Usuários** - relatório sobre os usuários em seu sistema
    - **Status de expiração de senha de usuário** - relatório sobre o status de expiração de senha dos usuários em seu sistema.
    - **Aplicativos mais usados** - relatório sobre todos os aplicativos no seu sistema, classificados pelo número de vezes que cada um foi instalado.
    - **Aplicativos não gerenciados** - relatório sobre os aplicativos não gerenciados no seu sistema.
    - **Todos os aplicativos** - reportar todos os aplicativos em dispositivos gerenciados por você.

4. Clique em **Avançar**.

    A página **Detalhes do Relatório** é exibida.

    - Insira um **Nome de relatório**.
    - (Opcional) Insira uma **Descrição** para o relatório.

    Selecione o **Intervalo de Eventos** entre as seguintes opções:
    Para relatórios existentes:

    - **Todos os eventos**
    - **Dia anterior**
    - **Semana anterior**
    - **Mês anterior**

- **Intervalo anterior** - exibe o relatório que foi criado usando o controle deslizante de intervalo na versão anterior do portal administrativo do Ivanti Neurons for MDM. Se o administrador selecionar e salvar alguma das opções acima para o relatório, a opção Intervalo Anterior não será exibida. O valor do intervalo fica visível na página Resumo do Relatório.

Para novos relatórios:

- **Todos os eventos**
- **Dia anterior**
- **Semana anterior**
- **Mês anterior**

5. Clique em **Avançar**. A página Dados do Relatório é exibida.
6. Clique em **Personalizar colunas** para adicionar, remover ou reordenar colunas na seção **Colunas do Relatório**. Como alternativa, clique no nome da coluna para remover a coluna adicionada.
7. (Opcional) Use a caixa de seleção **Selecionar todas as colunas** para selecionar todas as colunas exibidas na lista.
8. Clique em **Restaurar padrões** para reverter para as colunas anteriormente geradas. Para reverter para as colunas sem quaisquer personalizações, você pode escolher um dos modelos na página **Escolher um modelo de relatório**.
9. Crie filtros com base em regras específicas na seção **Filtro Avançado** .

Todas as opções de filtro não estão disponíveis para todos os relatórios. Para mais informações sobre a lista de filtros disponíveis, consulte o tópico "Filtros" na página 64 abaixo deste procedimento.

Os novos atributos de hardware a seguir estão disponíveis para dispositivos Windows ao criar relatórios: Criptografia BitLocker, Edição do SO, Versão do Sistema, Fabricante da Placa-Mãe, Produto da Placa-Mãe, Status da Placa-Mãe, Fabricante do BIOS, Versão do BIOS, Partições do Disco Rígido, Tipo de Unidade Óptica, Nome da CPU e Status da CPU.

10. (Opcional) Você também pode clicar no ícone **+** para adicionar outra regra ou clicar no ícone **Adicionar grupo** para adicionar outro grupo de regras.
11. Clique em **Avançar**. A página Agendamento do Relatório é exibida.
12. Selecione *um* dos seguintes formatos para fazer o download do relatório:
    - CSV
    - PDF
    - **CSV e PDF**

      Para arquivos de relatório em PDF, são permitidas até 10 colunas. Na seção Gráficos de Relatório, são exibidos dois tipos de gráficos a serem incluídos nos relatórios em PDF.

      O relatório **Todos os Aplicativos** aceita apenas formato CSV.
13. Clique em **Agendamento Automático** para definir a recorrência com que o relatório será executado automaticamente. Como alternativa, clique em **Manual** para executar o relatório uma vez, e ele será enviado por e-mail.
    - Selecione *uma* opção de **Relatório Recorrente**:
      - **Diariamente**
      - **Semanalmente**
      - **Mensalmente**
      - **Agendamento anterior** - para relatórios existentes
    - Selecione a **Data inicial** e a **Data final** (opcional).
14. Clique em **Avançar**. A página Distribuição de Relatório é exibida. Selecione os destinatários do relatório.
15. (Opcional) Adicione IDs de e-mail externo clicando no link **Adicionar e-mail externo**.
16. Clique em **Concluído** . O **Resumo de Distribuiçãodo Relatório** aparece.
17. (Opcional) Clique em **Editar** para modificar o relatório.

18. Clique em **Salvar**.

19. Clique no ícone de download para selecionar o formato do relatório. Um e-mail contendo o botão **Baixar relatório** é enviado aos destinatários do relatório.

Filtros

Opções de regra	Descrição
Trava de ativação ativada	Regras baseadas na trava de ativação habilitada como **Sim** ou **Não**. Exemplo de regra: 'Trava de ativação ativada é igual a Sim'.
Status do AppTunnel	Regra para status do AppTunnel como **BLOQUEAR** ou **PERMITIR**. Exemplo de regra: 'O Status do AppTunnel é igual a Bloquear'.
Nível da bateria	Valor do nível de bateria do dispositivo. Exemplo de regra: "O nível da bateria é igual a 1080" O valor inserido para o nível da bateria deve estar em segundos.
Último check-in do cliente	Regra baseada no último check-in do cliente dentro do intervalo de datas. Exemplo de regra: "O último check-in do cliente está no intervalo 02/04/2019 06:00:00,05/04/2019 17:00:00".
Estado de conformidade	Regra baseada no estado de conformidade como **Sim** ou **Não**. Exemplo de função: 'Estado de conformidade igual a Sim'.
Nome do país atual	Digite o nome do país atual. Exemplo de regra: "Estado de conformidade é igual a França".

Opções de regra	Descrição
MCC atual	Regra baseada no código móvel do país atual. Exemplo de regra: 'O MCC atual é igual a 410'.
MNC atual	Regra baseada no código de rede móvel atual. Exemplo de regra: 'O MNC atual é igual a 06'.
Registro de dispositivos ativado	Regra baseada no registro do dispositivo ativado como **Sim** ou **Não**. Exemplo de regra: "Registro do dispositivo ativado é igual a Sim"
Inscrito no Registro de dispositivos	Regra baseada em Registrado no registro de dispositivos como **Sim** ou **Não**. Exemplo de regra: "Registrado no registro do dispositivo é igual a Sim"
Proteção de dados	Indica se a proteção de dados está ativada no dispositivo. Os possíveis valores são **Sim** ou **Não**. Exemplo de regra: "Proteção de dados é igual a Sim".
Roaming de dados ativado	Regra baseada em roaming de dados ativado como **Sim** ou **Não**. Exemplo de regra: 'Roaming de dados ativado é igual a Sim'.

Opções de regra	Descrição
Status de bloqueio do dispositivo	Regra baseada no status de bloqueio do dispositivo. Exemplo de regra: 'O Status de bloqueio do dispositivo é igual a Bloquear'
ID do dispositivo	Função para um ID do dispositivo específico ou em um intervalo de IDs do dispositivo. Exemplo de função: 'ID do dispositivo superior a 45'. x
MCC inicial	Regra baseada no código móvel do país inicial. Exemplo de regra: 'O MCC inicial é igual a 310'.
MNC inicial	Regra baseada no código de rede móvel inicial. Exemplo de regra: 'O MNC inicial é igual a 510'.
IMEI	Função para um valor de IMEI específico. Exemplo de função: 'IMEI começa com 9900'

Opções de regra	Descrição
Estado de convite	Selecione qualquer uma das opções do Estado de convite a seguir: • **Nenhum** • **Pendente** • **Expirado** • **Concluído** Exemplo de função: 'Estado de conformidade igual a Pendente'.
Serviço de localizador ativado	Regra baseada no serviço de localizador ativado como **Sim** ou **Não**. Exemplo de regra: 'Serviço do localizador ativado é igual a Sim'.
Status de quarentena	Regra baseada no serviço de localizador ativado como **Sim** ou **Não**. Exemplo da regra: "Estado de quarentena é igual a Sim".
Registrado em	Função para selecionar o intervalo de data e hora de quando o dispositivo foi registrado. Exemplo de função: 'Registrado em no intervalo de 10/03/2017 09:00:00,10/20/2017 17:00:00'.
Roaming	Regra baseada no roaming como **Sim** ou **Não**. Exemplo da regra: 'Roaming é igual a Sim'

Opções de regra	Descrição
Status	Selecione qualquer uma das seguintes opções de Status de convite: • **Ativo** • **Desativação pendente** • **Desativação enviada** • **Retirado** • **Desativação cancelada** • **Apagamento pendente** • **Apagamento enviado** • **Exterminado** • **Apagamento cancelado** Exemplo da regra: "Status é igual a Desativação pendente".
Roaming de voz ativado	Regra baseada no roaming de voz ativado como **Sim** ou **Não**. Exemplo da regra: 'Roaming de voz ativado é igual a Sim'
Endereço Wi-Fi MAC	Insira um valor de endereço Mac específico. Exemplo de função: 'Endereço Wi-Fi Mac diferente de 00-14-22-01-23-45'.
Backup do iCloud ativado	Regra baseada no Backup do iCloud ativado como **Sim** ou **Não**. Exemplo de regra: "Backup do iCloud ativado é igual a Sim"

Opções de regra	Descrição
Status de ativação da conta na iTunes Store	Regra baseada no Status de ativação da conta da iTunes Store como **Sim** ou **Não**. Exemplo de regra: 'Status de ativação da conta da iTunes Store não é igual a Não'.
Tipo de plataforma	Aplicável ao relatório Todos os Aplicativos.
Origem	Aplicável ao relatório Todos os Aplicativos.
Atributos personalizados	Aplicável ao relatório Todos os Aplicativos.
Gerenciado	Aplicável aos relatórios Todos os Aplicativos e Aplicativos Mais Usados.
Identificador de aplicativo	É o padrão para o relatório Todos os Aplicativos.
Meid	Aplicável ao relatório Aplicativos Não Gerenciados.

Executar ações em um relatório na página Relatórios Agendados

Você pode executar várias ações na página Relatórios Agendados.

Procedimento

1. Acesse **Painel** > **Relatórios**.
2. Na página **Meus Relatórios Agendados**, clique no menu suspenso **Ações** e selecione uma destas opções:

Opções de ações	Ação realizada
Exibir	Permite visualizar o relatório.
Editar	Permite editar o relatório. O relatório também permite visualizar o intervalo que foi selecionado na última versão como Intervalo Anterior.
Executar agora	Executa o relatório.
Baixar CSV	Faz o download do relatório no formato CSV.
Baixar PDF	Baixa o relatório em formato PDF.
Excluir	Exclui o relatório.

Exibir detalhes do relatório

Você pode visualizar os detalhes do relatório e realizar algumas ações no relatório criado.

Procedimento

1. Acesse **Painel** > **Relatórios**.
2. Na página **Meus Relatórios Agendados**, clique no nome do relatório para ver os detalhes dele. A página do relatório é aberta.
3. Você pode visualizar o Resumo do Relatório e o Histórico de Relatórios nesta página.

Para obter mais informações, consulte Usando relatórios personalizados.

Usando relatórios personalizados

Licença: Gold

O recurso de relatórios personalizados permite que você personalize e gere relatórios em várias métricas com modelos prontos para uso. Você deve ter a função de Administrador de sistema ou de Somente leitura do sistema para acessar este recurso. Atualmente, você pode criar no máximo 40 relatórios.

Esta seção contém os seguintes tópicos:

"Gerando um relatório" abaixo

"Executar ações em um relatório" na página 83

"Exibir detalhes do relatório" na página 84

Gerando um relatório

Você pode agendar e gerar um relatório no portal administrativo do Ivanti Neurons for MDM.

Procedimento

1. Acesse **Painel** > **Relatórios**.
2. Clique em **Criar um relatório** para exibir a página Escolher um modelo de relatório.

3. Escolha um modelo para o relatório a partir das opções configuradas.

    - **Dispositivos bloqueados** - relatório sobre dispositivos com acesso atualmente bloqueado pelo Sentry.
    - **Dispositivos** - relatório sobre os dispositivos de todas as partições no seu sistema.
    - **Violações de política** - relatório sobre violações de política em seu sistema.
    - **Usuários** - relatório sobre os usuários em seu sistema
    - **Status de expiração de senha de usuário** - relatório sobre o status de expiração de senha dos usuários em seu sistema.
    - **Aplicativos mais usados** - relatório sobre todos os aplicativos no seu sistema, classificados pelo número de vezes que cada um foi instalado.
    - **Aplicativos não gerenciados** - relatório sobre os aplicativos não gerenciados no seu sistema.
    - **Todos os aplicativos** - reportar todos os aplicativos em dispositivos gerenciados por você.

4. Clique em **Avançar**. A página Detalhes do Relatório é exibida.
5. Insira um **Nome de relatório**.
6. (Opcional) Insira uma **Descrição** para o relatório.
7. Selecione o **Intervalo de Eventos** entre as seguintes opções:
   Para relatórios existentes:

    - **Todos os eventos**
    - **Dia anterior**
    - **Semana anterior**
    - **Mês anterior**
    - **Intervalo anterior** - exibe o relatório que foi criado usando o controle deslizante de intervalo na versão anterior do portal administrativo do Ivanti Neurons for MDM. Se o administrador selecionar e salvar alguma das opções acima para o relatório, a opção Intervalo Anterior não será exibida. O valor do intervalo fica visível na página Resumo do Relatório.

   Para novos relatórios:

- **Todos os eventos**
- **Dia anterior**
- **Semana anterior**
- **Mês anterior**

8. Clique em **Avançar**. A página Dados do Relatório é exibida.
9. Clique em **Personalizar** para gerar um relatório personalizado:

> Na página **Painel > Relatórios**, a coluna Nome do Modelo exibirá "personalizado" entre colchetes para indicar que o relatório foi personalizado.

10. Clique em **Personalizar colunas** para adicionar, remover ou reordenar colunas na seção **Colunas do Relatório**. Como alternativa, clique no nome da coluna para remover a coluna adicionada.
11. (Opcional) Use a caixa de seleção **Selecionar todas as colunas** para selecionar todas as colunas exibidas na lista.
12. Clique em **Restaurar padrões** para reverter para as colunas anteriormente geradas. Para reverter para as colunas sem quaisquer personalizações, você pode escolher um dos modelos na página **Escolha um modelo de relatório**. As colunas padrão são indicadas com um ícone de cadeado.
13. Crie filtros com base em regras específicas na seção **Filtro Avançado** .

> Todas as opções de filtro não estão disponíveis para todos os relatórios. Para mais informações sobre a lista de filtros disponíveis, consulte o tópico "Filtros" na página 77 abaixo deste procedimento.

> Os novos atributos de hardware a seguir estão disponíveis para dispositivos Windows ao criar relatórios: Criptografia BitLocker, Edição do SO, Versão do Sistema, Fabricante da Placa-Mãe, Produto da Placa-Mãe, Status da Placa-Mãe, Fabricante do BIOS, Versão do BIOS, Partições do Disco Rígido, Tipo de Unidade Óptica, Nome da CPU e Status da CPU.

14. (Opcional) Você também pode clicar no ícone **+** para adicionar outra regra ou clicar no ícone **Adicionar grupo** para adicionar outro grupo de regras.
15. Clique em **Avançar**. A página Agendamento do Relatório é exibida.

16. Selecione *um* dos seguintes formatos para fazer o download do relatório:

    - **CSV**
    - **PDF**
    - **CSV e PDF**

      Para arquivos de relatório em PDF, são permitidas até 10 colunas. Na seção Gráficos de relatório, os dois tipos de gráficos que serão incluídos nos relatórios em PDF serão exibidos.

      Todos os relatórios de Aplicativos oferecem suporte apenas ao formato CSV.

17. Clique em **Agendamento Automático** para definir a recorrência com que o relatório será executado automaticamente. Como alternativa, clique em **Manual** para executar o relatório uma vez, e ele será enviado por e-mail.

    - Selecione *uma* opção de **Relatório Recorrente**:
      - **Diariamente**
      - **Semanalmente**
      - **Mensalmente**
      - **Agendamento anterior** - para relatórios existentes
    - Selecione a **Data inicial** e a **Data final** (opcional).

    A opção Executar agora irá gerar um relatório único. Você pode usar o mesmo modelo para gerar relatórios agendados. Na página **Painel > Relatórios**, as colunas Frequência e Próximo agendado exibirão o status Não agendado para esses relatórios.

18. Clique em **Avançar**. A página Distribuição de Relatório é exibida. Selecione os destinatários do relatório.
19. (Opcional) Adicione IDs de e-mail externo clicando no link **Adicionar e-mail externo**.
20. Clique em **Concluído** . O **Resumo de Distribuiçãodo Relatório** aparece.
21. (Opcional) Clique em **Editar** para modificar o relatório.

22. Clique em **Salvar**.

23. Clique no ícone de download para selecionar o formato do relatório. Um e-mail contendo o botão **Baixar relatório** é enviado aos destinatários do relatório.

Filtros

Opções de funções	Descrição
Trava de ativação ativada	Regras baseadas na trava de ativação habilitada como **Sim** ou **Não**. Exemplo de regra: 'Trava de ativação ativada é igual a Sim'.
Status do AppTunnel	Regra para status do AppTunnel como **BLOQUEAR** ou **PERMITIR**. Exemplo de regra: 'O Status do AppTunnel é igual a Bloquear'.
Nível da bateria	Valor do nível de bateria do dispositivo. Exemplo de regra: "O nível da bateria é igual a 1080" O valor inserido para o nível da bateria deve estar em segundos.
Último check-in do cliente	Regra baseada no último check-in do cliente dentro do intervalo de datas. Exemplo de regra: "O último check-in do cliente está no intervalo 02/04/2019 06:00:00,05/04/2019 17:00:00".
Estado de conformidade	Regra baseada no estado de conformidade como **Sim** ou **Não**. Exemplo de função: 'Estado de conformidade igual a Sim'.
Nome do país atual	Digite o nome do país atual. Exemplo de regra: "Estado de conformidade é igual a França".

Opções de funções	Descrição
MCC atual	Regra baseada no código móvel do país atual. Exemplo de regra: 'O MCC atual é igual a 410'.
MNC atual	Regra baseada no código de rede móvel atual. Exemplo de regra: 'O MNC atual é igual a 06'.
Registro de dispositivos ativado	Regra baseada no registro do dispositivo ativado como **Sim** ou **Não**. Exemplo de regra: "Registro do dispositivo ativado é igual a Sim"
Inscrito no Registro de dispositivos	Regra baseada em Registrado no registro de dispositivos como **Sim** ou **Não**. Exemplo de regra: "Registrado no registro do dispositivo é igual a Sim"
Proteção de dados	Indica se a proteção de dados está ativada no dispositivo. Os possíveis valores são **Sim** ou **Não**. Exemplo de regra: "Proteção de dados é igual a Sim".
Roaming de dados ativado	Regra baseada em roaming de dados ativado como **Sim** ou **Não**. Exemplo de regra: 'Roaming de dados ativado é igual a Sim'.

Opções de funções	Descrição
Status de bloqueio do dispositivo	Regra baseada no status de bloqueio do dispositivo. Exemplo de regra: 'O Status de bloqueio do dispositivo é igual a Bloquear'
ID do dispositivo	Função para um ID do dispositivo específico ou em um intervalo de IDs do dispositivo. Exemplo de função: 'ID do dispositivo superior a 45'. x
MCC inicial	Regra baseada no código móvel do país inicial. Exemplo de regra: 'O MCC inicial é igual a 310'.
MNC inicial	Regra baseada no código de rede móvel inicial. Exemplo de regra: 'O MNC inicial é igual a 510'.
IMEI	Função para um valor de IMEI específico. Exemplo de função: 'IMEI começa com 9900'

Opções de funções	Descrição
Estado de convite	Selecione qualquer uma das opções do Estado de convite a seguir: • **Nenhum** • **Pendente** • **Expirado** • **Concluído** Exemplo de função: 'Estado de conformidade igual a Pendente'.
Serviço de localizador ativado	Regra baseada no serviço de localizador ativado como **Sim** ou **Não**. Exemplo de regra: 'Serviço do localizador ativado é igual a Sim'.
Status de quarentena	Regra baseada no serviço de localizador ativado como **Sim** ou **Não**. Exemplo da regra: "Estado de quarentena é igual a Sim".
Registrado em	Função para selecionar o intervalo de data e hora de quando o dispositivo foi registrado. Exemplo de função: 'Registrado em no intervalo de 10/03/2017 09:00:00,10/20/2017 17:00:00'.
Roaming	Regra baseada no roaming como **Sim** ou **Não**. Exemplo da regra: 'Roaming é igual a Sim'

Opções de funções	Descrição
Status	Selecione qualquer uma das seguintes opções de Status de convite: • **Ativo** • **Desativação pendente** • **Desativação enviada** • **Retirado** • **Desativação cancelada** • **Apagamento pendente** • **Apagamento enviado** • **Exterminado** • **Apagamento cancelado** Exemplo da regra: "Status é igual a Desativação pendente".
Roaming de voz ativado	Regra baseada no roaming de voz ativado como **Sim** ou **Não**. Exemplo da regra: 'Roaming de voz ativado é igual a Sim'
Endereço Wi-Fi MAC	Insira um valor de endereço Mac específico. Exemplo de função: 'Endereço Wi-Fi Mac diferente de 00-14-22-01-23-45'.
Backup do iCloud ativado	Regra baseada no Backup do iCloud ativado como **Sim** ou **Não**. Exemplo de regra: "Backup do iCloud ativado é igual a Sim"

Opções de funções	Descrição
Status de ativação da conta na iTunes Store	Regra baseada no Status de ativação da conta da iTunes Store como **Sim** ou **Não**. Exemplo de regra: 'Status de ativação da conta da iTunes Store não é igual a Não'.
Tipo de plataforma	Aplicável ao relatório Todos os Aplicativos.
Origem	Aplicável ao relatório Todos os Aplicativos.
Atributos personalizados	Aplicável ao relatório Todos os Aplicativos.
Gerenciado	Aplicável aos relatórios Todos os Aplicativos e Aplicativos Mais Usados.
Identificador de aplicativo	É o padrão para o relatório Todos os Aplicativos.
Meid	Aplicável ao relatório Aplicativos Não Gerenciados.

Executar ações em um relatório

Você pode executar várias ações na página Relatórios Agendados.

Procedimento

1. Acesse **Painel** > **Relatórios**.
2. Na página **Meus Relatórios Agendados**, clique no menu suspenso **Ações** e selecione uma destas opções:

Opções de ações	Ação realizada
Exibir	Permite visualizar o relatório.
Editar	Permite editar o relatório.
Executar agora	Executa o relatório.
Baixar CSV	Faz o download do relatório no formato CSV.
Baixar PDF	Baixa o relatório em formato PDF.
Excluir	Exclui o relatório.

Exibir detalhes do relatório

Você pode visualizar os detalhes do relatório e realizar algumas ações no relatório criado.

Procedimento

1. Acesse **Painel** > **Relatórios**.
2. Na página **Meus Relatórios Agendados**, clique no nome do relatório para ver os detalhes dele. A

página do relatório é aberta.

3. Selecione uma das opções a seguir

Opções de ações	Ação realizada
Ativar/desativar	Permite habilitar ou desabilitar o relatório.
Executar agora	Executa o relatório.
Exibir	Permite exibir os detalhes do relatório. Use o menu suspenso Ações para executar qualquer uma das seguintes tarefas: • **Desabilitar** • **Baixar CSV/PDF mais recente** (conforme o tipo de relatório selecionado, seja CSV, PDF ou CSV e PDF, mostra a opção Baixar) • **Histórico** • **Excluir**
Excluir	Exclui o relatório.

Usuários

Antes de convidar alguém para registrar dispositivos móveis, crie uma entrada de usuário para essa pessoa. Também é necessário criar um usuário para qualquer pessoa que vá usar o Ivanti Neurons for MDM para ajudar a gerenciar dispositivos ou publicar conteúdo (administradores).

Esta seção contém os seguintes tópicos

Como adicionar usuários

Esta seção contém os seguintes tópicos:

Você pode adicionar um único usuário ou vários usuários de uma vez. Após adicionar vários usuários, talvez você queira filtrar a exibição para mostrar somente aqueles que lhe interessam.

Outras coisas que você pode fazer com os usuários nesta página:

- atribuir a/remover de um grupo de usuários
- enviar uma mensagem
- convidar para registrar
- atribuir funções
- alterar uma senha
- excluir

Todos os perfis de proprietário de dispositivo são atribuídos a uma conta de dispositivo. As contas de dispositivo não têm restrições quanto ao número de dispositivos atribuídos a si. Os perfis de trabalho (de propriedade do funcionário) são contas de usuário atribuídas.

Como adicionar um usuário

Procedimento

1. Acesse **Usuários**.
2. Clique em **+ Adicionar** (canto superior direito).
3. Selecione **Usuário único**.
4. Preencha o formulário com as informações do usuário:
   - Endereço de e-mail
   - Nome
   - Sobrenome

   > O campo Nome de Usuário exibe o endereço de e-mail inserido. Na maioria dos casos, você não deve editar esse padrão. Para obter mais informações, consulte Quando editar um nome de usuário
5.

   > Se quiser alterar o nome de exibição desse usuário, edite o texto predefinido no campo **Nome de exibição**.
6. Se quiser atribuir uma senha, digite-a nos campos **Senha** e **Confirmar senha**.
   - Ao atribuir uma senha, comunique-a ao usuário para o registro do dispositivo.
   - Se você não atribuir uma senha, o usuário precisará criar uma senha durante o registro do dispositivo.
7. Selecione o **Local** na lista suspensa.
8. Digite **Apple ID gerenciado**. Você pode incluir "appleid" como um subdomínio do Apple ID gerenciado para evitar conflitos com os Apple IDs existentes. Por exemplo, usuário@appleid.seudomínio.com. O subdomínio deve ser um subdomínio confirmado e válido no Apple Business Manager.

   > A conta não poderá ser atualizada com um Apple ID gerenciado diferente se houver um dispositivo registrado pelo usuário ativo com o Apple ID gerenciado da conta atual.
9. (Opcional) Atribua um ou mais grupos de usuários. O Apple ID gerenciado não pode ser atualizado quando houver um dispositivo com o status "Ativo" e "Remoção pendente".

10. Se quiser configurar outros recursos antes de convidar o usuário, desmarque a opção **Enviar este convite agora**. Caso contrário, o e-mail de convite será enviado quando você clicar em **Concluído**.
11. Clique em **Concluído** para adicionar o usuário.

Para dispositivos Android, as contas de dispositivo são projetadas para dispositivos gerenciados de uso único, nos quais uma única conta de serviço local pode ser usada para registrar um grande número de dispositivos. Ao criar um novo usuário, você pode ativar as Contas de dispositivo (em vez das Contas de usuário padrão) para os registros de Conta do Google Play gerenciada pelo proprietário do dispositivo.

Marque a caixa de seleção **Conta do dispositivo Android Enterprise** para permitir que os registros de dispositivos gerenciados de trabalho Android Enterprise anexados a esta conta sejam automaticamente atribuídos a uma Conta de dispositivo do Google.

Ao editar um usuário local ou LDAP para dispositivos Android, os dispositivos da conta Google Play gerenciada pelo proprietário do dispositivo com Android corporativo associados ao usuário serão atribuídos a Contas de dispositivo na próxima vez que o dispositivo for registrado, contanto que as seguintes condições sejam atendidas:

- O recurso é ativado ao marcar a caixa de seleção **Conta de dispositivo Android corporativo**.
- A versão do aplicativo Go no dispositivo Android é a 47 ou mais recente.

Adicionando diversos usuários

Procedimento :

1. Acesse **Usuários** .
2. Clique em **+ Adicionar** (canto superior direito).
3. Selecione **Vários usuários**.
4. Por padrão, você pode inserir endereços de e-mail **Manualmente**. Digite ou cole os endereços de e-mail dos usuários, separados por vírgulas.

   Por exemplo: jdoe@minhaempresa.com, jsmith@minhaempresa.com, tjones@minhaempresa.com
5. Se quiser configurar outros recursos antes de convidar o usuário, desmarque a opção **Enviar este convite agora**.

Caso contrário, o e-mail de convite será enviado quando você clicar em **Concluído**.

6. Clique em **Concluído** para adicionar os usuários.

Adicionando vários usuários fazendo upload de um arquivo

Procedimento:

1. Acesse **Usuários** .
2. Clique em **+ Adicionar** (canto superior direito).
3. Selecione **Vários usuários**.
4. Selecione **Carregar CSV**.
5. Clique em **Baixar modelo de CSV**.
6. Edite o modelo com as informações a seguir referentes a cada usuário:
   - usuário ID (obrigatório)
   - endereço de e-mail (obrigatório)
   - senha
   - nome
   - sobrenome
   - nome de exibição
   - grupos de usuários
   - atributos personalizados

   São as mesmas informações que você insere ao adicionar um usuário individual. Não ultrapasse a quantidade de 10.000 entradas no arquivo.
7. Salve o arquivo.
8. Arraste-o para a área de upload ou selecione **Carregar CSV** para selecionar o arquivo.

9. Depois que as informações do usuário que foram carregadas forem exibidas, faça as edições necessárias.
10. Clique em **Avançar** (inferior direito).
11. Se não quiser enviar convites imediatamente, selecione **Não enviar convites**.
12. Clique em **Concluído** .

Adicionando um administrador

Procedimento :

1. Clique em **Adicionar** (canto superior direito).
2. Selecione **Usuário único**.
3. Preencha o formulário com as informações do usuário:
   - Endereço de e-mail
   - Nome
   - Sobrenome

   O campo **Nome de usuário** exibe o endereço de e-mail que você inseriu.
4. Se quiser alterar o nome de exibição desse usuário, edite o texto predefinido no campo **Nome de exibição**.
5. Atribua uma senha no campo **Senha**.
6. Digite a senha novamente no campo **Confirmar senha**.
7. Clique em **Concluído** para adicionar o usuário.
8. Comunique a senha à pessoa que irá ajudar no gerenciamento dos dispositivos.

Usuário Ninguém

O usuário ninguém é um usuário padrão que não pode ser excluído. O serviço aplica esse usuário a dispositivos que não possuem usuários associados, como dispositivos desativados.

Exibição das informações do PIN de registro do dispositivo

Ao adicionar novos usuários, a informação do PIN de registro gerado será exibida aos administradores se o Tipo de autenticação do registro do dispositivo for definido como Somente PIN. Estas informações podem ser úteis para ajudar os usuários com as inscrições do dispositivo.

- Para usuários individuais, o PIN é exibido pela ação **Usuários > Convidar usuário para se registrar** e também na seção Informações do PIN da página Detalhes do usuário.
- Para vários usuários, os PINs são exibidos como uma coluna na página Lista de usuários, além das colunas Status do PIN (válido ou expirado), PIN emitido e PIN expira em.

Se você não conseguir executar tarefas na página **Usuários**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Gerenciamento de usuários

Grupos de usuários

Esta seção contém os seguintes tópicos:

Crie um grupo de usuários para que você possa atribuir apps e funções a vários usuários.Por exemplo, você poderá criar um grupo Gerentes se desejar que todos os gerentes do departamento sejam administradores de apps e conteúdos.

É possível criar um grupo de usuários a serem gerenciados de acordo com um dos seguintes métodos:

- **Gerenciados dinamicamente (o mais comum):** usuários locais e de LDAP são adicionados/removidos de/para um grupo de maneira dinâmica com base em determinadas regras e/ou atributos.
- **Gerenciados manualmente (propósito limitado):** adicionar/remover usuários de/para um grupo manualmente. Os grupos gerenciados manualmente são recomendados somente para fins de teste que exijam menos permissões.

É possível inserir o texto no campo **Pesquisar** para exibir uma lista de todos os grupos de usuário cujos nomes comecem com o texto inserido.

- Os resultados de pesquisa são exibidos como uma lista de possíveis correspondências em tempo real enquanto o texto está sendo digitado.
- Selecione o nome do grupo de usuários desejado na lista de possíveis correspondências para a ação subsequente.
- A correspondência da pesquisa não faz distinção entre letras maiúsculas e minúsculas.

Criar um grupo de usuários com gerenciamento dinâmico

Procedimento

1. Clique em **+Adicionar**.
2. Insira um nome de grupo de usuários no campo **Nome**.
3. (Opcional) Clique em **Adicionar descrição** para adicionar uma descrição para o grupo de usuários.
4. Clique na opção **Gerenciados dinamicamente (o mais comum)**.

5. Configure regras e/ou atributos de acordo com seus requisitos. A seguir estão as opções de regra disponíveis:
    - Atributo LDAP personalizado
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname
    - Atributo de LDAP padrão
        - samAccountName
        - userPrincipalName
    - Atributo de usuário padrão
        - email_address
        - distinguished_name
        - last_name
        - display_name
        - first_name
        - Grupo de usuários
        - Atributo de usuário personalizado
    - Grupo de usuário DN
    - Grupo de usuários GUID
    - Nome do grupo de usuários
6. Para cada regra, selecione entre usuários locais e de LDAP. É possível incluir ou excluir um subgrupo usando os critérios de filtro **Grupo de usuários**.
7. Adicione mais regras clicando no ícone mais.
   Você pode configurar **QUALQUER** ou **TODOS** os filtros condicionais para as regras adicionadas.
8. Crie um grupo de regras clicando no ícone hierárquico ao lado do ícone mais.

9. Revise as regras e os atributos do grupo de usuários na consulta de texto abaixo da criação de regras.
10. Na seção **Resultados**, revise os detalhes dos usuários que correspondem aos critérios configurados. Ao adicionar ou modificar uma regra ou um atributo, é possível observar que os usuários correspondentes são exibidos, se eles existirem.
11. Clique em **Salvar** para salvar o grupo de usuários configurados.

Criar um grupo de usuários com gerenciamento manual

1. Clique em **+Adicionar**.
2. Insira um nome para o grupo.
3. (Opcional) Clique em **Adicionar descrição** para adicionar uma descrição.
4. Selecione a opção **Gerenciado manualmente (propósito limitado)**.
5. No campo **Pesquisar usuários**, digite o endereço de e-mail de cada usuário a ser incluído no grupo. Conforme você digita, os usuários correspondentes são localizados e exibidos, caso existam.
6. Selecione os usuários que deseja adicionar ao grupo. Você pode pesquisar e adicionar mais usuários, conforme necessário.
7. Clique em **Salvar**.

> Você pode criar um grupo de usuários gerenciado manualmente e adicionar esse grupo a um grupo de usuários gerenciado dinamicamente. Nesse cenário, a edição do grupo de usuários com gerenciamento manual não viola a regra de grupo de usuários com gerenciamento dinâmico. Você não será capaz de excluir um grupo de usuários com gerenciamento manual se ele for adicionado a um grupo de usuários com gerenciamento dinâmico.

Criação de um grupo de usuários a partir de um dos grupos de usuários duplicados

A partir do Ivanti Neurons for MDM 91, o portal do administrador exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo "Nome do grupo de usuários" é selecionado no construtor de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Usuários**, **Grupos de usuários**.
3. Clique em **+Adicionar**. O assistente Criar grupo de usuários é aberto.
    a. Especifique o nome no campo **Nome**.
    b. Selecione **Nome do grupo de usuários** no Criador de regras, selecione **é igual a**, selecione *um* dos nomes de grupos duplicados.
    c. Clique no ícone **+** para adicionar mais regras.
    d. Selecione **Grupo de usuários GUID**, **é igual a**.
    e. Copie e cole o GUID da tabela que exibe a lista de nomes de grupos de usuários duplicados e GUIDs. O resultado exibe os usuários associados que serão adicionados ao novo grupo.
    f. Clique em **Salvar**. Os usuários listados são adicionados ao novo grupo de usuários que você criou.

Se você não conseguir executar tarefas na página **Grupos de usuários,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Gerenciamento de usuários

Configurações do usuário

Esta seção contém os seguintes tópicos:

As configurações do usuário definem as opções de registro do dispositivo. Existem vários tipos:

- **Configuração de registro do dispositivo**: define a autenticação por senha, PIN ou ambos; tipo de registro da Apple e propriedade do dispositivo.

- Anteriormente, se você configurasse, a autenticação SAML/IdP, a autenticação SAML era utilizada tanto para o registro de dispositivos quanto para a autenticação do portal. A partir da versão 79.1 em diante, um botão de alternância é fornecido para escolher diferentes métodos de autenticação para o acesso ao portal do administrador e ao registro de dispositivos. A alternância de bypass é aplicável apenas ao registro de dispositivos.

  Este recurso não oferece suporte para o tipo de autenticação Somente PIN.

- **Configuração de limite de dispositivos**: define quantos dispositivos um usuário pode registrar.
- **Configuração do limite de apagamento**: limita o número máximo de dispositivos que podem ser apagados por vez.
- **Configuração de autenticação do portal de autosserviço:** define o tipo de autenticação de senha para o portal de autosserviço.
- **Configuração de complexidade da senha**: configure a complexidade da senha e parâmetros de política para contas locais usadas para registro de dispositivo e acesse o portal do administrador e os portais de autosserviço.
- **Configuração dos termos de serviço:** define os termos de serviço exibidos ao usuário em cada registro de dispositivo.
- **Configuração de lembrete de convite do usuário:** define as datas e a frequência para o envio de emails de lembrete de convite do usuário.
- **Configuração de confirmação do registro do usuário:** controla a capacidade de enviar o e-mail de confirmação do registro do usuário. Consulte "Como configurar e usar e-mails de confirmação de registro" na página 25 para obter uma visão geral da solução e "Como configurar e-mails de confirmação de registro do usuário" na página 113 abaixo para obter instruções de configuração específicas do usuário.
- **Configuração de programação de trabalho do usuário:** controla a capacidade de configurar a programação de trabalho de um usuário que bloqueia todas as comunicações do Sentry com dispositivos gerenciados fora do horário de trabalho prescrito. Útil para localidades com leis de Direito à desconexão.
- **Configuração de autenticação do portal do administrador:** controla se o solicita ao administrador apenas a senha ou a senha e o PIN.

Você pode editar as configurações padrão para o grupo **Todos os usuários** ou adicionar configurações personalizadas e atribuí-las aos outros grupos de usuários.

Edição da configuração padrão

Clique no link **Editar** da configuração que possui o ícone de bloqueio. Não é possível excluir a configuração padrão.

Adicionando uma configuração personalizada

Clique no link **Adicionar configuração para grupos de usuários específicos**.

Remoção de uma configuração personalizada

Clique no ícone X.

Configuração de definições para registros de novos dispositivos

Você pode configurar a versão mínima do SO, o tipo de autenticação e a propriedade do dispositivo para registros de novos dispositivos. A URL de inscrição do dispositivo gerada nas versões anteriores do Ivanti Neurons for MDM deixará de funcionar com a versão atual. O administrador precisará gerar novamente a URL de inscrição do dispositivo para registrar o dispositivo.

A opção para inserir o registro do dispositivo na lista de permitidos está disponível apenas nas configurações de usuário padrão e não está disponível para configurações de usuário personalizadas. É possível carregar um arquivo CSV usando o modelo que contém os números de série e os atributos do dispositivo personalizados que são usados para inserir alguns dispositivos na lista de permitidos. É possível incluir um ou mais atributos de dispositivo personalizados existentes para criar a lista de permitidos. Isso permitirá que você designe atributos aos grupos de dispositivos ou espaços após o registro. Para criar atributos personalizados, acesse **Administrador > Atributos**. Os dispositivos iOS e macOS não são permitidos para registro via iReg se o recurso Lista de permitidos estiver habilitado e o número de série do dispositivo não for mencionado no arquivo CSV. Se o arquivo CSV contiver um número de série duplicado, a última entrada no arquivo CSV será considerada e os atributos de dispositivo personalizados associados à entrada serão considerados para a atribuição de dispositivo durante o registro. Se a opção **Lista de dispositivos permitidos** estiver ativada, somente os dispositivos permitidos poderão ser registrados no . Esse recurso é aplicável apenas a dispositivos que se registram por meio do processo de registro baseado na web. Isso não afetará os dispositivos já registrados no Ivanti Neurons for MDM. Após o registro, se o número de série do dispositivo for removido do arquivo CSV, o dispositivo não será desativado. O usuário mencionado no arquivo CSV é opcional e será atribuído apenas se o usuário for mencionado no arquivo CSV e for um usuário válido. Se deseja carregar um novo arquivo CSV, é possível excluir o arquivo CSV existente e carregar o novo arquivo. A inserção na lista de permitidos tem suporte apenas no iReg e se o Go client for necessário, então escolha o registro automático. Para recursos como AppConnect, Threat Defense etc. funcionarem, o Go client deve estar instalado no sistema. Como não fornecemos suporte ao registro no aplicativo, o usuário pode registrar o dispositivo pelo iReg e, depois, o aplicativo Go poderá ser enviado aos dispositivos do App Catalog. Quando o usuário aceita a instalação do aplicativo, o dispositivo se torna um dispositivo gerenciado e todos os recursos continuam a funcionar após o registro. A configuração de toque zero não pode ser usada em dispositivos nos quais o status do AppConnect é Ativo ou Inativo. Pode ser usado apenas quando o status do AppConnect for Nenhum. O status do AppConnect permanece como Nenhum até que o cliente Go seja iniciado no dispositivo após o registro pelo iReg.

Procedimento

1. Faça login em Ivanti Neurons for MDM.
2. Acesse **Usuários** > **Configurações do usuário**.
3. Em **Configurações de registro de dispositivo**, clique em **+Adicionar configuração para grupo de usuários específico**.
4. Edite a configuração **Tipo de autenticação do registro do dispositivo** ou adicione uma nova.
5. Digite um nome no campo **Nome**.
6. (Opcional) Insira a descrição da configuração.

7. Na seção **Configurações do SO**, defina a versão mínima do sistema operacional para iOS, macOS e Windows:

   Selecione o botão de alternância **Habilitar Versão Mínima** e selecione uma versão do sistema operacional na lista suspensa.

   > A configuração Habilitar Versão Mínima não se aplica a registros de dispositivos DEP.

8. Para **Android**:

   - Ative a opção **Correção de segurança mínima** (somente Android) e selecione uma das seguintes opções na lista suspensa para definir o período:
     - **dia(s)**
     - **mês(es)**
     - **ano(s)**
   - Habilite a opção **Lista de permitidos/bloqueados do fabricante** e selecione qualquer uma das opções a seguir:
     - **Criar uma lista de permitidos** – Para permitir o registro apenas de dispositivos destes fabricantes.
     - **Criar uma lista de bloqueados** – Para impedir o registro de dispositivos destes fabricantes.

       Para adicionar um fabricante:

       a. Clique em **Adicionar fabricante**.

       b. Digite o nome do fabricante no campo **Nome do fabricante**.

       c. Clique em **Salvar**. O nome do fabricante adicionado é exibido na tabela.

       > O nome do fabricante faz distinção entre maiúsculas e minúsculas. Para editar ou excluir um nome de fabricante adicionado, clique na opção **Editar** ou **Deletar** correspondente.

9. Na seção Registro da Apple, selecione o Tipo de registro da Apple:

- **Registro de dispositivos**
- **Registro do usuário**– Por padrão, o Registro do usuário aplica-se a dispositivos iOS e iPadOS.
- (Opcional) **Incluir dispositivo macOS (macOS 10.15+)** – Selecione esta opção para tornar o Registro do usuário aplicável também a dispositivos macOS.

10. Na seção **Método de convite de registro (apenas iOS e Android)**, ative **Registro somente no MAM**.

> Essa opção deve estar ativada para registros de dispositivos somente MAM e, quando ativados, os usuários são redirecionados para a Public App Store para baixar o aplicativo AppStation client.

11. Na seção **Tipo de autenticação de registro do dispositivo**, selecione uma das opções a seguir na lista suspensa **Selecionar tipo de registro**. Se você usar Registro de Dispositivo, certifique-se de que a sua configuração de Registro de Dispositivo corresponda à sua escolha.

    - **Somente senha**
    - **Somente PIN** Quando você seleciona essa opção, o botão Ignorar Autenticação de Registro de Dispositivo do IdP fica bloqueado.
    - **Senha e PIN**

    > Os usuários ainda podem receber um PIN para concluir a ativação da conta.

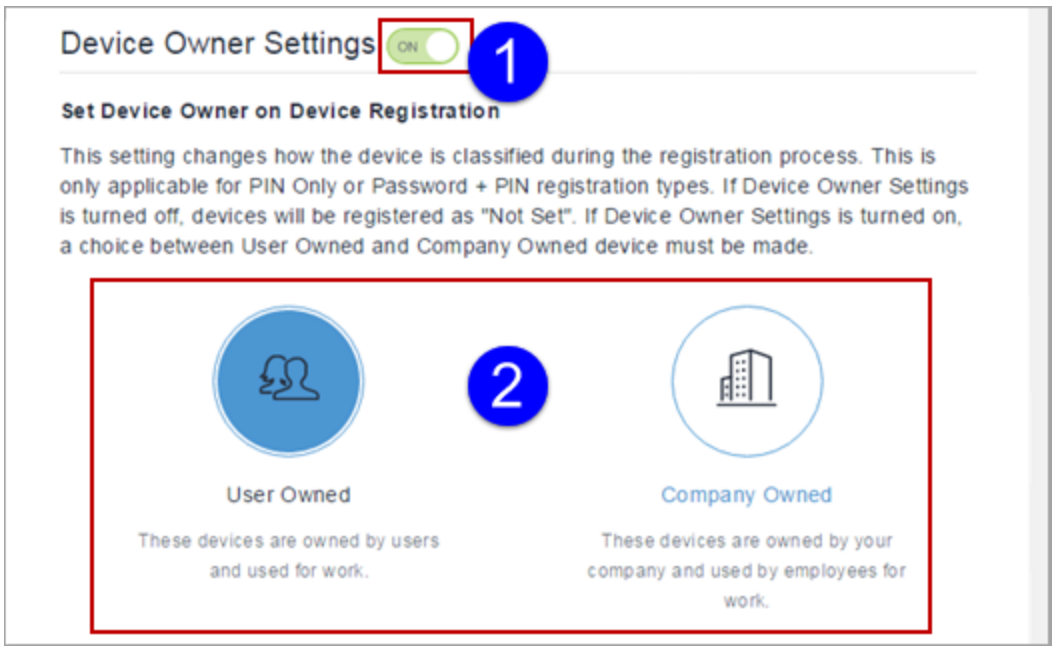
> Esta configuração afeta tanto o registro normal quanto o registro de dispositivos.

12. Para PINs, especifique o seguinte. Durante o registro do dispositivo, um usuário pode clicar em **Reenviar PIN** se necessário.

    - **Duração do PIN**: por quanto tempo o PIN permanece válido (1-30 dias).
    - **Tamanho do PIN**: o número de caracteres (4-12).
    - **Permitir que o usuário solicite um novo PIN**: (ao esquecer ou ele expirar).

13. Como alternativa, ative as **Configurações de Propriedade do Dispositivo** e clique em **Propriedade do Usuário** ou **Propriedade da Empresa**. Essa configuração altera a forma como o dispositivo é classificado durante o processo de registro.

    - Se as **Configurações de Propriedade do Dispositivo** estiverem LIGADAS e o administrador tiver marcado o dispositivo como Propriedade do Usuário, o usuário terá a opção de marcar o dispositivo como Propriedade do Usuário ou Propriedade da Empresa durante a inscrição do dispositivo e também no portal de autoatendimento. Para dispositivos de Registro de usuário registrado, as configurações padrão de Proprietário do dispositivo serão "Propriedade do usuário", independentemente da opção feita pelo administrador.
    - Para os dispositivos supervisionados, as configurações do proprietário do dispositivo serão "Propriedade da Empresa".



14. Clique em **+Adicionar** para pelo menos um grupo de usuários ao qual você deseja distribuir a configuração.
15. (Recurso sob demanda somente para dispositivos iOS e macOS) Opcionalmente, ative a opção **Lista de dispositivos permitidos** para permitir o registro do dispositivo com base nos números de série permitidos.
16. Clique em **Avançar**. A página Distribuição de Configuração do Usuário se abre.
17. Selecione a distribuição do grupo de usuários.

18. Clique em **Concluído**.
19. Envie um convite para os usuários. Para mais informações, consulte "Como convidar usuários" na página 156.

Observe os seguintes pontos:

Se um dispositivo de usuário for registrado usando a opção somente PIN, o usuário receberá um e-mail de confirmação de registro com um PIN para autenticação.

- Um PIN é enviado para o ID de e-mail do usuário.
- O usuário insere o PIN na página de registro do dispositivo.
- Se o PIN estiver correto, o usuário é direcionado para concluir o processo de registro.

Para usuários configurados com Provedor de internet (IdP) baseado em SAML, o Ivanti Neurons for MDM suporta autenticação com PIN ao registrar o dispositivo. O Tipo de Autenticação de Registro do Dispositivo deve ser PIN e Senha. O recurso PIN e Senha atua como autenticação de dois fatores para conferir segurança adicional. Nesse caso, quando esse usuário tenta registrar um dispositivo:

- Um PIN é enviado para o ID de e-mail do usuário.
- O usuário insere o PIN na página de registro do dispositivo.
- Se o PIN estiver correto, o usuário é redirecionado para a página de login do IdP em que o usuário insere o número de usuário e a senha do IdP.
- Se as credenciais do IdP estiverem corretas, o usuário é redirecionado para o dispositivo para concluir o processo de registro.

Como configurar o limite de dispositivos por usuário

Procedimento

1. Edite a configuração **Limite de dispositivos** padrão ou adicione uma nova.
2. Edite ou atribua um nome para identificar a configuração.
3. Digite uma descrição opcional da configuração.
4. Selecione um limite do menu suspenso.

5. Clique em **+Adicionar** para pelo menos um grupo de usuários ao qual você deseja distribuir a configuração.
6. Clique em **Salvar**.

Configuração do limite de apagamento de dispositivos

Procedimento

1. Edite a configuração **Limite de apagamento de dispositivos** padrão.
2. Ative a opção **Habilitar limite de apagamento para todos os usuários (incluindo funções padrão)**.
3. No campo **Número máximo de dispositivos que um usuário pode apagar de uma vez**, digite o número máximo de dispositivos que podem ser apagados de uma vez. O valor padrão é 1. 200 é o valor máximo que pode ser definido para o limite de limpeza do dispositivo.
4. Clique em **Concluído**.

Configuração da autenticação do Portal de autosserviço

Procedimento

1. Edite a configuração **Autenticação do Portal de autosserviço** padrão ou adicione uma nova clicando em **+Adicionar configuração para grupos de usuários específicos**.
2. Edite ou atribua um nome para identificar a configuração.
3. Digite uma descrição opcional da configuração.
4. Selecione um **Tipo de autenticação do Portal de autosserviço** no menu suspenso. Pode ser uma das opções a seguir:
   - Senha
   - Certificado
5. Clique em **Avançar**.
6. Selecione um ou mais grupos de usuários para os quais essa configuração será distribuída.
7. Clique em **Concluído**.

Definindo a complexidade da senha

Você pode definir a complexidade da senha e parâmetros de política para contas locais usadas para registro de dispositivo e acessar o portal do administrador e os portais de autoatendimento.

O tamanho, características e políticas de senha definidos abaixo definem a segurança de uma senha.

Também define a dificuldade para que um usuário selecione uma senha válida. Se você usa conta local para os usuários finais e gostaria de ter senhas seguras para acessar o Portal do administrador, considere usar um PIN para registro de dispositivo, para que a complexidade da senha não interfira no registro. Use a configuração "Autenticação de registro de dispositivo" para selecionar o modo de autenticação para o registro do dispositivo em **Configurações do usuário > Configuração de registro de serviço**.

Procedimento

1. Edite as configurações padrão **Complexidade da senha**.

2. Defina as seguintes configurações de complexidade de senha:

Configuração	O que fazer
Comprimento mínimo da senha	Mova o seletor para especificar a extensão mínima de uma senha para impedir que o usuário crie senhas curtas e não seguras. Intervalos de números entre 8 e 32.
Características obrigatórias	Especifique o número de caracteres da senha que devem ser cumpridos ao selecionar uma senha. O número mínimo de características que devem ser cumpridas é 3 (4 para clientes federais).
Caracteres especiais obrigatórios (símbolos)	Especifique o número de caracteres não alfabéticos que uma senha deve conter.
Caracteres maiúsculos obrigatórios	Especifique o número de caracteres alfabéticos maiúsculos que uma senha deve conter.
Caracteres minúsculos obrigatórios	Especifique o número de caracteres alfabéticos minúsculos que uma senha deve conter.
Caracteres numéricos obrigatórios	Especifique o número de caracteres numéricos que uma senha deve conter.
Validações de senha	
Sequência numérica permitida	Selecione a quantidade de números repetidos em sequência. Exemplo: 123.
Caracteres repetidos permitidos	Selecione o número de caracteres alfabéticos repetidos. Exemplo: bbc.

3. Defina as configurações das políticas de senha a seguir para personalizar o comportamento.

Configuração	O que fazer
Histórico de senhas retidas	Mova o seletor para selecionar o número de novas senhas que devem ser associadas a uma conta de usuário para permitir a utilização de uma senha antiga. Intervalos de números entre 3 e 36.
Período de expiração de senha	Mova o controle deslizante para selecionar a duração da expiração da senha em dias. O número varia entre 30 e 365 dias.
Tempo limite de inatividade	Mova o controle deslizante para especificar o tempo que um usuário pode ficar inativo antes do tempo de sessão do Portal do administrador ou Portal de autoatendimento. O número varia entre 5 a 60 (minutos).
Limite de logins com falha	Mova o seletor para escolher o número de falhas em tentativas de login antes que o bloqueio de 5 minutos da conta entre em vigor. Intervalos de números entre 2 e 5. Quando o número de tentativas está dentro do limite, uma mensagem é exibida ao usuário informando sobre o bloqueio e pedindo que tente o login mais tarde. Quando o número de tentativas excede o limite, uma mensagem é exibida ao usuário informando sobre o bloqueio e pedindo que tente o login após um período especificado (em minutos).

4. Clique em **Concluído** . Se você tiver alterado a configuração padrão de Complexidade da senha, uma senha mais antiga de conta local existente permanecerá inalterada. Quando ocorrer a expiração, o usuário será solicitado a renovar a senha. Administradores tentando fazer login no Portal do Administrador podem contatar o Help Desk para obter orientação sobre a redefinição de senha.

Em um registro de dispositivo, a abordagem recomendada é usar o modo de registro somente PIN.

Como definir os termos de serviço

Procedimento

1. Crie uma nova configuração de **Termos de Serviço**.
2. Atribua um nome para identificar a configuração.
3. Digite uma descrição opcional da configuração.
4. Selecione **Solicitar ao usuário**... .
5. Digite um título e um texto para serem exibidos.
6. Clique em **+Adicionar** para pelo menos um grupo de usuários ao qual você deseja distribuir a configuração.
7. Clique em **Salvar**.

Após serem aceitos, não é possível excluir os termos de serviço. No entanto, você pode desativar os prompts de novo registro desmarcando a opção **Solicitar ao usuário**... .

Configuração dos e-mails de lembrete de Convite do usuário

Administradores podem aumentar as inscrições de dispositivo usando esta configuração para enviar e-mails de lembrete de Convite do usuário.

Procedimento

1. Editar uma **Configuração de lembrete de convite do usuário**, ou adicionar uma nova.
2. Edite ou atribua um nome para identificar a configuração.

3. Digite uma descrição opcional da configuração.
4. Verifique se a opção **Lembretes de convite do usuário** está ligada.
5. Na região Definir datas de início e término, escolha quando iniciar e interromper o envio de lembretes por e-mail.

   O número máximo de e-mails que podem ser enviados é de 30. Para zerar o limite, o administrador deve reenviar o convite.

6. Na região Definir frequência, escolha a frequência para o envio dos lembretes por e-mail.
7. Clique em **Avançar**.
8. Selecione uma distribuição para essa configuração.
9. Clique em **Concluído**.

Como configurar e-mails de confirmação de registro do usuário

Os administradores podem enviar e-mails para novos usuários que concluíram o registro.

Procedimento

1. Edite uma **Configuração de confirmação do registro do usuário** ou adicione uma nova.
2. Edite ou atribua um nome para identificar a configuração.
3. Digite uma descrição opcional da configuração.
4. Verifique se a opção **Enviar um e-mail de confirmação após o registro bem-sucedido do usuário** está ativada.
5. Clique em **Avançar**.
6. Selecione uma distribuição para essa configuração.
7. Clique em **Concluído**.

Definir a configuração de programação de trabalho do usuário

Os administradores podem configurar a programação de trabalho de um usuário que bloqueia todas as comunicações do Sentry com dispositivos gerenciados fora do horário de trabalho prescrito. Isso é útil para usuários em localidades com leis de Direito à desconexão.

Procedimento

1. Selecione **Usuários**.
2. Selecione **Configurações do usuário**.
3. Na seção **Configuração de programação de trabalho do usuário**, selecione **+Adicionar configuração para grupos de usuários específicos**.
4. Forneça um nome para a configuração.
5. Ative a configuração.
6. Selecione o fuso horário.
7. Configure as horas durante as quais o Ivanti Neurons for MDM bloqueia o protocolo Exchange ActiveSync, apps habilitados para AppConnect e apps gerenciados.
8. Clique em **Avançar**.
9. Configure a distribuição e, em seguida, clique em **Concluído**.

As alterações aplicadas podem levar até 1 hora e 15 minutos para entrar em vigor no dispositivo.

Como configurar a autenticação do Portal do administrador

Os administradores podem definir o tipo de autenticação para autenticar o login do usuário. Essa configuração controla se será solicitado ao usuário apenas a senha ou a senha e o PIN.

Procedimento

1. Edite uma **Configuração de autenticação do portal do administrador** ou adicione uma nova.
2. Edite ou atribua um nome para identificar a configuração.
3. Digite uma descrição opcional da configuração.

4. No **Tipo de autenticação do portal do administrador** selecione qualquer uma das seguintes opções:

Opção	Descrição
Senha	Selecione esta opção para autenticar o login usando somente senha. Os usuários ainda podem receber um PIN para concluir a ativação da conta.
Senha e PIN	Selecione esta opção para autenticar o login usando senha e PIN. Quando você seleciona esta opção, os seguintes campos adicionais são exibidos: • **Duração do PIN**: Selecione a duração em minutos do PIN na lista suspensa. Os minutos devem estar dentro de um intervalo de 1 a 15. • **Tamanho do PIN**: Selecione o número de caracteres do PIN da lista suspensa. O PIN deve ter de 4 a 12 caracteres. Esta opção é aplicável apenas a contas locais, e não a contas de Administrador LDAP.
Permitir que o usuário solicite um novo PIN	Selecione esta opção para permitir que usuários solicitem um novo PIN.

5. Clique em **Avançar**.
6. Selecione uma distribuição para essa configuração.
7. Clique em **Concluído**.

Para usuários configurados com Provedor de internet(IdP) com base em SAML, Ivanti Neurons for MDMé suportada a autenticação com base em PIN no portal de administração. O tipo de Autenticação do portal de administração deve ser o PIN e a Senha. Esse recurso funciona como uma autenticação de dois fatores para segurança adicional. Nesse caso, quando esse usuário tenta fazer o login no portal:

- Um PIN é enviado para o ID de e-mail do usuário.
- O usuário insere o PIN na página de login do portal de administração.
- Se o PIN estiver correto, o usuário é redirecionado para a página de login do IdP em que o usuário insere o número de usuário e a senha do IdP.
- Se as credenciais do IdP estiverem corretas, o usuário é redirecionado para o portal de administrador.

Ao fazer o login no portal de administrador, um usuário pode clicar em **Esqueci minha senha** para redefinir sua senha. Na próxima tela, o usuário pode inserir uma nova senha e o PIN (solicitado com base nas configurações do modo de autenticação do usuário anterior) enviado para o endereço de e-mail do usuário. Clique em **Reenviar PIN** se necessário. O usuário deve aguardar quinze minutos entre as solicitações de Esqueci a Senha.

Quando essa configuração é distribuída aos dispositivos, uma tentativa consecutiva de login sem êxito (valor padrão: cinco tentativas) feita pelo usuário que usa senha ou PIN resultará no bloqueio da conta e uma mensagem será exibida ao usuário no bloqueio.

Identidade visual do usuário

A identidade visual do usuário permite personalizar o processo de registro do dispositivo com nomes e logotipos que seus usuários reconhecerão. Você pode personalizar a identidade visual apresentada ao cliente das seguintes maneiras:

- Defina um nome de host personalizado para a URL de registro
- Exiba seu logotipo no e-mail de registro e na tela de registro
- Exiba um favicon personalizado durante atividades de registro

Licença: Gold

Pré-requisito:

- Decida sobre o nome do host que deseja usar em sua URL personalizada. Ele deve Atender aos seguintes requisitos:
  - Não conter espaços
  - Não conter caracteres especiais
- Obtenha um arquivo de logotipo que atenda aos seguintes requisitos:
  - Formato PNG
  - 580 x 80 pixels
- Obtenha um arquivo de favicon que atenda aos seguintes requisitos:
  - Formato PNG
  - 64 x 64 pixels

Procedimento:

1. Acesse **Usuários > Identidade visual do usuário**.
2. Clique em **Personalizar** (canto superior direito).
3. No campo **Nome do host**, digite um nome curto para usar como o nome do host em sua URL.

4. Clique em **Verificar disponibilidade** para confirmar que o nome do host inserido não foi usado por mais ninguém.
5. Caso o nome do host não esteja disponível, insira um nome diferente.
6. Observe a URL de registro resultante em **Visualização da URL**.
7. Clique em **Avançar**.
8. Em **Logotipo**, clique em **Escolher arquivo** para carregar o logotipo a ser usado no e-mail de registro e na tela de registro.
9. Clique em **Avançar**.
10. Em **Favicon**, clique em **Escolher arquivo** para carregar o favicon que será exibido no lugar do favicon do Ivanti Neurons for MDM durante as atividades de registro.
11. Clique em **Concluído**.

Registro do usuário no Apple Business Manager

Esta seção contém os seguintes tópicos:

Aplicável a:

- Dispositivos não supervisionados com iOS 13.0 até a versão mais recente, conforme suporte de Ivanti Neurons for MDM.
- Dispositivos com macOS 10.15 ou versões mais recentes com suporteIvanti Neurons for MDM.

O Apple Business Manager é um local para as equipes de TI automatizarem a implantação de dispositivos, comprarem e distribuírem conteúdo e gerenciarem funções em suas organizações. O Apple Business Manager implementa o registro do usuário, que é uma opção de registro projetada para empresas que implementam BYOD (Bring Your Own Device, Traga Seu Próprio Dispositivo). O registro do usuário é uma versão modificada do protocolo MDM com um foco muito maior na privacidade do usuário, implementada com um nível de segurança que as empresas precisam.

O registro do usuário permite que o administrador:

- Instale e remova aplicativos gerenciados
- Instale e remova configurações de rede
- Instale uma VPN parcial com escopo para aplicativos e contas gerenciados
- Exija o uso de uma senha

Requisitos para ativar o registro do usuário

Abaixo estão os requisitos para ativar o registro do usuário. Se algum deles não for atendido, o tipo de registro será registrado pelo dispositivo.

- Um dispositivo não supervisionado com iOS 13.0 até a versão mais recente é compatível com Ivanti Neurons for MDM ou com um dispositivo com macOS 10.15 ou versões mais recentes com suporteIvanti Neurons for MDM.
- A configuração do usuário para o campo Tipo de registro da Apple deve ser definida como "Registro do usuário".
- Uma conta do Apple Business Manager.
  - A conta de licença de aplicativo da Apple precisa fazer parte da mesma conta do Apple Business Manager.
  - No Apple Business Manager, se você possui uma conta listada em Locais, é necessário que o Apps and Books corresponda ao mesmo local. Pode ser necessário adicionar um novo local (por exemplo, costa oeste).
- Apple ID gerenciado: Apple ID gerenciado a ser associado a cada dispositivo registrado.
  - Esse Apple ID gerenciado fornece autenticação para gerenciamento de MDM e licenciamento de aplicativos.
  - Quando o MDM envia aplicativos e mídias, as licenças Apple necessárias são atribuídas ao Apple ID gerenciado associado ao dispositivo.
  - De acordo com a conformidade com a RGPD, os Apple IDs gerenciados são mascarados nas páginas de lista de usuários e detalhes do usuário, considerando-se que o Apple ID seja dado do usuário.
  - Os Apple IDs gerenciados foram utilizados pela primeira vez pelo Apple School Manager e agora são utilizados pelo Apple Business Manager para registro de usuários.

    > O Apple ID gerenciado do dispositivo e o token de localização do Apps and Books devem ser da mesma organização da conta do Apple Business Manager.

    Se forem diferentes, uma notificação será exibida no portal do administrador Ivanti Neurons for MDM quando a alocação de licença falhar para um aplicativo.
- Microsoft Azure Active Directory configurado para Autenticação federada ou um Apple ID criado manualmente no Apple Business Manager com um domínio validado.

- Para obter instruções sobre o uso da autenticação federada, consulte o Guia do usuário do Apple Business Manager no site da Apple. É necessário fazer login.

- Os usuários do dispositivo sincronizados com o LDAP devem ser atribuídos a uma função de gerenciamento de dispositivos e associados a um Apple ID gerenciado.

Na página da lista Usuários e na página da lista Dispositivos, você pode adicionar a coluna Apple ID gerenciado a ser exibida para todos os usuários. Na página da lista Dispositivos, você pode adicionar a coluna Registro de usuário registrado para exibir o status dos dispositivos de Usuário registrado. Além disso, as exportações de usuário e dispositivo incluem essas colunas nos arquivos CSV.

Prioridade dos registros

- O Registro do usuário é compatível com o Go para iOS client e iReg.
- O registro automatizado de dispositivos e os registros do Apple Configurator sempre serão registrados pelo dispositivo.
- Se a configuração do MAM for aplicada a um dispositivo, o registro do MAM terá precedência sobre o Registro do usuário.
- Se os requisitos auth-only e Registro do usuário forem atendidos, o Registro do usuário terá precedência.
- Se você inscrever novamente um dispositivo do Go para iOS client, o tipo de registro será o mesmo durante o registro do dispositivo, independentemente da alteração no tipo de registro em Ivanti Neurons for MDM. Por exemplo, se um dispositivo foi registrado pelo usuário, altere o tipo para Registro pelo dispositivo em Ivanti Neurons for MDM e inscreva novamente o dispositivo no Go client. O dispositivo ainda será registrado pelo usuário e não pelo dispositivo.

Diferença entre o registro padrão no MDM e o registro do usuário

Esta seção aborda a diferença entre o registro padrão no MDM e o registro do usuário no Apple Business Manager.

Registro padrão no MDM

A lista a seguir indica o que um servidor Ivanti Neurons for MDM pode fazer em um registro padrão no MDM, mas não pode fazer no modo de Registro do usuário.

O servidor MDM:

- Não pode apagar o dispositivo.
- Não vê os aplicativos pessoais que o usuário do dispositivo instalou no dispositivo.
- Não pode converter aplicativos instalados pelo usuário em aplicativos gerenciados pelo MDM.
- Não pode limpar a senha do dispositivo (ou seja, desbloquear o dispositivo).
- Não pode definir um requisito longo e complexo para a senha do dispositivo.
- Não pode configurar uma VPN ou proxy Wi-Fi em todo o dispositivo, nem gerenciar a funcionalidade do celular.
- Não pode ver identificadores de dispositivo como UDID, número de série ou IMEI.
- Não pode aplicar muitas restrições em todo o dispositivo (como restringir a classificação do conteúdo do aplicativo), bloquear o iCloud e aplicar restrições supervisionadas.

Registro do usuário no Apple Business Manager

No registro do usuário, o servidor MDM ainda pode fazer todo o necessário para gerenciar aplicativos, contas e dados corporativos.

O registro do usuário pode:

- Instalar aplicativos internos ou aplicativos por meio de licenças do Apps and Books (Apple) baseadas no usuário.
    - As licenças são aplicadas por ordem de chegada e são consumidas pelos Apple IDs gerenciados.
    - A licença consumida por um aplicativo instalado no dispositivo Registrado pelo usuário será diferente da licença consumida pelo mesmo aplicativo instalado no dispositivo registrado pelo dispositivo.
    - Verifique o tipo de licença dos aplicativos Apple Apps and Books na página de detalhes do usuário, na guia Uso da licença; o Tipo de registro é exibido como Registro do usuário ou Registro do dispositivo.
- Impor configurações de carga útil de senha. Por exemplo:
    - allowSimple = false
    - forcePIN = true

- minLength = 6

- Consultar dados relacionados a aplicativos, certificados e perfis gerenciados pela empresa.
- Configurar uma VPN por aplicativo para aplicativos, e-mail, contatos e calendários que foram instalados pelo MDM.
- Impor algumas restrições, como abertura gerenciada, contatos gerenciados, dados gerenciados na tela de bloqueio e várias outras.

Os dados corporativos são armazenados em um volume separado do Apple File System (APFS), criado no registro e criptografado separadamente dos dados do usuário do dispositivo. Este volume contém dados armazenados por aplicativos gerenciados, Notes corporativo, documentos corporativos do iCloud Drive, entradas do Keychain corporativo, anexos e mensagens de correio gerenciados e anexos de calendário. Cancelar o registro no MDM destrói o volume e as chaves.

Todos os aplicativos de terceiros podem ser apenas aplicativos pessoais ou gerenciados pelo Ivanti Neurons for MDM. O serviço MDM não pode começar a gerenciar aplicativos que o usuário do dispositivo já instalou. Nesse caso, o administrador precisará solicitar que o usuário do dispositivo exclua o aplicativo pessoal antes de instalá-lo pelo MDM. O serviço MDM não pode começar a gerenciar aplicativos que o usuário já instalou. No entanto, alguns aplicativos do sistema, como o Notes e o Files, são compatíveis com contas comerciais e pessoais.

Registro do usuário para dispositivos macOS

O Registro do usuário é compatível com dispositivos com macOS 10.15 ou versões mais recentes com suporteIvanti Neurons for MDM.

- O Mobile@Work para macOS não oferece suporte para dispositivos de Registro de usuário registrado do macOS.
  - Ainda que o aplicativo seja distribuído para o dispositivo de Registro de usuário registrado do macOS, ele não será enviado ao dispositivo pelo MDM.
  - Portanto, recursos do Mobile@Work, como gerenciamento de script e gerenciamento de aplicativo para aplicativos Packager (MIP), não têm suporte em dispositivos de Registro de usuário registrado do macOS.
- Dependência do aplicativo e alterações comportamentais em dispositivos de Registro de usuário registrado do macOS.

- Em dispositivos de Registro de usuário registrado do macOS, a dependência do aplicativo funciona na base do melhor esforço, pois o MDM não detecta (não é capaz de confirmar) o status de instalação de apps necessários antes de distribuir o aplicativo principal.
- Apps e configurações podem ser distribuídos para usuários e grupos de usuários pertencentes aos dispositivos de Registro de usuário registrado do macOS. No entanto, os apps sempre exibem o botão**Instalar**em vez de "Instalado", uma vez que o MDM não pode exibir o status de instalação de apps em dispositivos de Registro de usuário registrado do macOS.
- Os apps instalados são indicados como Apps solicitados na página**Dispositivos > Inventário de apps**, pois os dispositivos de Registro de usuário registrado do macOS não informam ao servidorIvanti Neurons for MDMse os apps estão ou não instalados no relatório do inventário.

- No filtro de distribuição de apps, os atributos Registro de usuário registrado e Registro de dispositivo automatizado registrado podem ser usados para distribuição personalizada, conforme a necessidade.
- Licenças baseadas em usuário são permitidas mediante o uso de Apple IDs gerenciados para instalar os aplicativos Apple Apps and Books. Licenças baseadas em dispositivos não são permitidas. O App Catalog exibe apenas os aplicativos Apple Apps and Books.
- Nem todas as configurações, políticas e ações são permitidas. Veja a lista completa de configurações e políticas depois deste procedimento.
  - Caso configurações não suportadas sejam distribuídas para um dispositivo de Registro de usuário registrado do macOS, elas não serão distribuídas nem aplicadas ao dispositivo e poderão exibir uma mensagem como "Restrições: este tipo de solicitação não é válido".
  - Da mesma forma, ações não suportadas do dispositivo do administrador serão informadas na interface do usuário do Ivanti Neurons for MDM.
  - Os relatórios não suportados não serão enviados pelo Ivanti Neurons for MDM.

Veja a seguir as configurações e políticas sem suporte que devem ser distribuídas para dispositivos de Registro de usuário registrado do macOS:

- Senha
- Túnel
- Tunnel (sob demanda)
- Configurações VPN
- Criação de conta automática do Office 365

- Política de extensão Kernel de macOS
- Preferência de privacidade
- Restrições do macOS
- Atualizações de software
- AirPrint
- Privacidade do cliente MI
- FileVault 2
- Chave de recuperação do FileVault
- Firewall
- Regra de política do sistema
- Preferência de certificado
- Controle de política do sistema
- Gerenciamento da política do sistema
- Restrições de Mac OS app Store
- Restrições de gravação de disco do Mac OS
- Configurações do Finder do Mac OS
- Mobile@Work para macOS
- Script do Mobile@Work para macOS
- Controle de mídia permitido
- Servidor de tempo
- Política de aplicativos permitidos

Diferença entre Registro do usuário e Registro de dispositivo

Esta seção aborda a diferença entre o registro do usuário e o registro do dispositivo.

O Registro do usuário se aplica a dispositivos com iOS 13.0 e macOS 10.15 até a versão mais recente com suporte. Os dispositivos inferiores ao iOS 13.0 e ao macOS 10.15 serão considerados para "registro do dispositivo", independentemente se o usuário do dispositivo tiver sido ativado para registro do usuário ou não.

O registro do usuário para o Apple Business Manager não permite a limpeza ou desbloqueio. No entanto, o portal do usuário ainda terá essas opções disponíveis, mesmo que elas não funcionem.

TABLE 1. REGISTRO DO USUÁRIO VERSUS REGISTRO DO DISPOSITIVO

Funcionalidade	Registro do usuário	MAM	Registro de dispositivos
Apagar o dispositivo e ver os aplicativos pessoais do usuário	✗	✗	✓
Converter gerenciado para não gerenciado ou vice-versa	✗	✗	✓
Limpar a senha do dispositivo, configurar a VPN ou o proxy Wi-Fi em todo o dispositivo ou gerenciar a funcionalidade de celular	✗	✗	✓
Ver identificadores de dispositivo como número de série, IMEI	✗	✗	✓
Aplicar restrições supervisionadas	✗	✗	✓ (Somente dispositivos supervisionados)
Possibilidade de instalar e configurar aplicativos e contas	✓	✓	✓
Possibilidade de configurar uma VPN por aplicativo para apps, e-mail, contatos e calendários que foram instalados pelo MDM	✓	✗	✓
Possibilidade de impor algumas restrições, como abertura gerenciada, contatos gerenciados, dados gerenciados na tela de bloqueio e várias outras	✓	✗	✓
Possibilidade de consultar dados relacionados a aplicativos, certificados e perfis gerenciados pela empresa	✓	✗	✓

Conectando o Ivanti Neurons for MDM ao Apple Business Manager

Esta seção aborda a ativação do registro do usuário para o Apple Business Manager.

Pré-requisitos

- Você deve ter uma conta do Apple Business Manager. Consulte https://business.apple.com/.
- Você deve solicitar e instalar um Certificado MDM da Apple para gerenciar dispositivos iOS.

Criando usuários locais para ativar o registro do usuário

Esta seção aborda a criação de usuários locais e LDAP e a configuração do registro do usuário para dispositivos Apple não supervisionados. O registro do usuário não funcionará em dispositivos supervisionados ou dispositivos registrados no registro de dispositivos da Apple.

Criando um grupo de usuários gerenciado manualmente (estático)

Este procedimento é realizado uma única vez. Se você já criou este grupo, pule para a seção "Criando usuários para registro do usuário".

Procedimento

1. Acesse **Usuários** > **Grupos de usuários**.
2. Crie um grupo de usuários gerenciado manualmente (estático), como o Grupo de registro do usuário, para adicionar usuários com o tipo de registro de dispositivo como registro do usuário.
3. Clique em **Salvar**.

Criando uma configuração de tipo de registro do dispositivo

Este procedimento é realizado uma única vez. Se você já criou este grupo, pule para a seção "Criando usuários para registro do usuário". Para dispositivos de Registro de usuário registrado, as configurações padrão do Proprietário do dispositivo serão "Propriedade do usuário".

Procedimento

1. Acesse**Usuários** >**Configurações do usuário**.
2. Na seção Configuração do registro do dispositivo, clique em **+ Adicionar configuração para grupos de usuários específicos**.

3. Crie uma nova configuração, como Registro UE, para usuários com tipo de registro de dispositivo como registro de usuário.
4. Na seção Registro da Apple, selecione **Registro do usuário** como o tipo de registro da Apple.
5. Clique em **Avançar**.
6. Na página Distribuição de configuração do usuário, selecione o grupo de usuários recém-criado, como Grupo de registro do usuário.
7. Clique em **Concluído**.

Criando um usuário local para registro do usuário

Como pré-requisito, crie um grupo de usuários gerenciado manualmente e uma configuração de registro do dispositivo para registro do usuário.

Procedimento

1. Acesse **Usuários**.
2. Clique em **+Adicionar > Usuário único**.

   Digite as novas informações do usuário e adicione-as ao grupo de usuários recém-criado, como Grupo de registro do usuário. Para obter mais informações, consulte "Adicionando um usuário" no tópico Usuários.

Importando usuários LDAP para ativar o registro do usuário

Como pré-requisito, configure um Ivanti Neurons for MDM conector para acessar os recursos de LDAP. Verifique se a configuração do**Apple ID gerenciado**está definida como**Padrão** (endereço de e-mail do usuário) e, opcionalmente, inclua o subdomínio "appleid" para evitar conflitos com os Apple IDs existentes. Verifique se o padrão para o Apple ID gerenciado é exclusivo. Caso contrário, a conta não será atualizada com o Apple ID gerenciado se o mesmo Apple ID gerenciado existir em outra conta.

Você pode importar usuários do LDAP e convidá-los para o registro do usuário. Os usuários LDAP importados terão seus Apple IDs gerenciados sincronizados com Ivanti Neurons for MDM, que é um requisito para o registro do usuário.

Procedimento

1. Acesse **Usuários**.
2. Clique em **+Adicionar > Convidar usuários do LDAP**.

3. Clique em **Selecionar usuários** na entrada do servidor LDAP.
4. Na página Adicionar usuários LDAP, insira o nome do usuário, grupo ou OU no campo de busca.
5. Para adicionar novos usuários ou grupos, clique em **+Adicionar** ao lado da entrada que deseja adicionar.
6. Clique em **Concluído**.

Importando usuários AAD para ativar o registro do usuário

Como pré-requisito, conecte Ivanti Neurons for MDM com o Microsoft Azure Active Directory (AAD).

Você pode convidar usuários do AAD para registro do usuário. Os usuários AAD importados terão seus Apple IDs gerenciados sincronizados com Ivanti Neurons for MDM, que é um requisito para o registro do usuário.

Procedimento

1. Acesse **Admin** > **Origem do usuário do Azure AD**.
2. Edite as configurações.
3. Selecione **Ativar este AAD**.
4. Na configuração do Apple ID gerenciado, selecione **Padrão** (endereço de e-mail do usuário). Verifique se o padrão para o Apple ID gerenciado é exclusivo. Caso contrário, a conta não será atualizada com o Apple ID gerenciado se o mesmo Apple ID gerenciado existir em outra conta.
5. Opcionalmente, inclua o subdomínio "appleid" para evitar conflitos com os Apple IDs existentes.
6. Selecione **Convidar automaticamente usuários importados do AAD**. Usuários importados do AAD para Ivanti Neurons for MDM são automaticamente convidados a se registrar por e-mail.
7. Clique em **Salvar**.

Instruções do usuário do dispositivo para registrar usando o registro do usuário

Esta seção aborda as ações que o usuário do dispositivo precisa executar para registrar o registro do usuário da Apple.

Procedimento

1. No dispositivo iOS que você deseja registrar, abra o e-mail de convite que contém um link e um texto que direcionam o usuário final para um link de registro, como mobileiron.com/go.
2. Abra o link de registro no Safari.

   A página de login é exibida. O usuário do dispositivo deve efetuar login usando o usuário local ou as credenciais LDAP.

   A página de registro é exibida com uma mensagem informando que o perfil foi baixado.
3. Toque em **Configurações**. A página Configurações é exibida.
4. Toque em **Registrar em [Nome da sua empresa]**.
5. A página Registro do usuário será exibida.

   Toque em **Registrar meu [seu dispositivo].** Por exemplo, toque em Registrar meu iPhone.

   Se você tocar em Cancelar e Excluir perfil, terá que iniciar o processo de registro novamente.
6. Você receberá um login para a Apple ou sua conta federada. Digite a senha para o seu Apple ID gerenciado. (O Apple ID gerenciado será listado na parte superior da sua página de login.)

   Você pode receber a opção de permanecer conectado, escolha uma opção.

   Uma página exibe "Registro bem-sucedido".

Usando logs do dispositivo para solução de problemas

Para solucionar erros ou problemas de um dispositivo registrado pelo usuário, comece examinando os logs do dispositivo.

Procedimento

1. Acesse **Dispositivos**.
2. Clique no nome do dispositivo para exibir a página de detalhes do usuário. Você pode verificar os campos do Apple ID gerenciado registrado e do Registro do usuário registrado.
3. Selecione a guia **Registros**.
4. Na região Filtros, restrinja os logs do dispositivo usando filtros baseados nos nomes de ação (como Check-out, Nome do dispositivo, Definir token de inicialização, Obter token de inicialização, e assim por diante), status, data de início e data de término.

5. Na coluna Ações, clique no ícone de olho para exibir os detalhes do registro do dispositivo, como ID do registro.
6. Clique em **OK**.

Registro do usuário orientado pela conta

Aplicável a

- Dispositivos com o iOS 15+

O Registro do usuário orientado pela conta para dispositivos iOS 15+ é uma opção de registro projetada para empresas que implementam BYOD (Bring Your Own Device, Traga Seu Próprio Dispositivo). O Registro do usuário orientado pela conta é uma versão modificada do protocolo MDM e do Registro do usuário no Apple Business Manager com um foco muito maior na privacidade do usuário, implementada com um nível de segurança que as empresas precisam.

Pré-requisitos

Os requisitos para o Registro do usuário orientado pela conta são os seguintes:

- Um dispositivo não supervisionado com o iOS 15+
- Uma conta de usuário no Ivanti Neurons for MDM com o Apple ID gerenciado (conta escolar ou profissional da Apple)

Configurar o serviço de descoberta

Se sua empresa tiver um nome de domínio corporativo, por exemplo, acme.com, então, o Apple ID gerenciado de seus usuários é username@acme.com. Para habilitar a descoberta de serviço para sua empresa, você deve fornecer um terminal conhecido da seguinte forma:

GET https://acme.com/.well-known/com.apple.remotemanagement

O terminal retornará um objeto JSON contendo o URL base de registro de seu cluster do Ivanti Neurons for MDM, da seguinte forma:

/c/i/reg/userenroll.mobileconfig

O URL do Ivanti Neurons for MDM deve começar com https, não com http.

Exemplo:

```
{
```

```
 "Servidores":[
  {
   "Version": "mdm-byod",
   "BaseURL": "https://<your polaris cluster>/c/i/reg/userenroll.mobileconfig"
   }
  ]
}
```

Para obter mais informações, consulte as informações neste URL:

https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers

Instruções do usuário do dispositivo para registrar usando o Registro do usuário orientado pela conta

Este tópico aborda as ações que o usuário do dispositivo precisa executar para fazer o Registro do usuário orientado pela conta.

Procedimento

1. No dispositivo iOS, abra **Configurações** > **Geral** > **VPN** e **Gerenciamento de dispositivos**.
2. Acesse **Entrar na conta profissional ou escolar**.
3. Digite o endereço de e-mail da conta profissional ou escolar. Assegure que o endereço de e-mail seja de acordo com o formato a seguir:
   username@<nome de domínio empresarial>, por exemplo, username@acme.com.
4. A página de login pega automaticamente o Apple ID gerenciado e o usuário pelo fluxo do iReg. Certifique-se de inserir as credenciais do Ivanti Neurons for MDM.
5. Digite as credenciais da conta profissional ou escolar e clique em **Continuar**.
6. Após uma autenticação com dois fatores, o registro do dispositivo é concluído.

Licenças do usuário

Ivanti Neurons for MDM as licenças baseadas em usuário definem o número de usuários que podem ser registrados, a quantidade de dispositivos permitidos por licença de usuário, a quantidade de conteúdo que pode ser configurado para distribuição aos dispositivos e os recursos disponíveis. Se você atingir o limite de usuários, será exibido um triângulo vermelho na página Administrador. Se você alcançar o limite de conteúdo, o serviço irá impedir mais adições e exibirá uma mensagem indicando que você alcançou o limite.

Para determinar quantas licenças de usuário devem ser planejadas, considere os pontos a seguir:

- Cada licença de usuário comprada no pacote Secure UEM ou Secure UEM Premium permite o registro de até cinco dispositivos.
- Quando um usuário registrar mais de cinco dispositivos, será solicitada outra licença de usuário.
- Não existe um limite imposto para o número de licenças de usuários que um usuário pode solicitar.
- As licenças são liberadas quando os dispositivos são desativados ou apagados.

Por exemplo, quando o Usuário1 registra seu telefone comercial no primeiro dia de trabalho, ele solicita uma licença de usuário. Na semana seguinte, ele registra dois telefones pessoais e um tablet na mesma licença. Ao registrar outro tablet, ele terá cinco dispositivos, então, solicita uma segunda licença de usuário. Se o telefone pessoal for roubado, ele apaga o dispositivo, liberando a segunda licença de usuário.

Exibição do número de dispositivos/licenças de um usuário

Procedimento:

1. Acesse **Usuários**.
2. Clique no link para o usuário.

   O painel esquerdo lista os detalhes do usuário, incluindo o uso da licença.

Como gerenciar usuários

Esta seção contém os seguintes tópicos:

Como adicionar um usuário API para as operações Cisco ISE

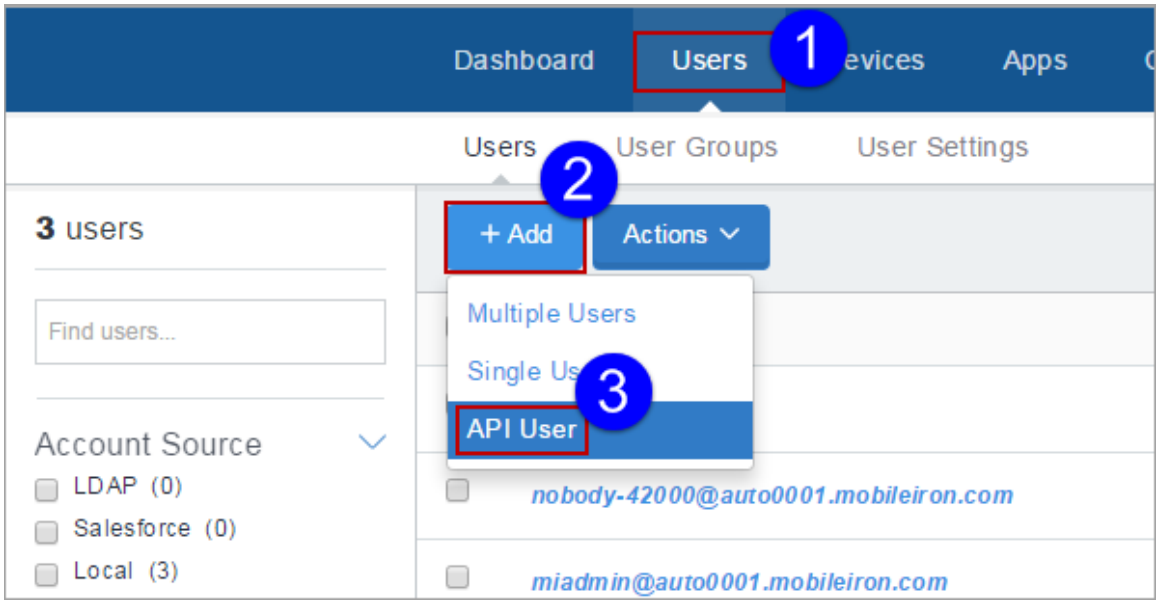
Você pode adicionar um usuário API com a função "Operações Cisco ISE", que permite que o Cisco ISE interaja com APIs Cisco ISE no Ivanti Neurons for MDM. Após criar esse usuário, use essas credenciais de usuário do Cisco ISE para autenticar chamadas de API no Ivanti Neurons for MDM. Essas APIs permitem que o Cisco ISE obtenha informações do dispositivo; execute ações em dispositivos, por exemplo, apagamento completo, apagamento corporativo e bloqueio de PIN; e envie mensagens aos dispositivos.

O usuário da API não poderá acessar o portal de administração. Este usuário é apenas para habilitar o uso da API.

Somente ao Administrador Super de um locatário é atribuída a função Cisco ISE Operations por padrão. O Superadministrador deve escolher explicitamente os usuários do sistema que precisam ter essa função e atribuí-la a eles. Por sua vez, os usuários atribuídos com a função Cisco ISE Operations podem atribuir a função a outros usuários apropriados no sistema.

Procedimento

1. Clique na guia **Usuários**.



2. Clique em **Adicionar**.
3. Selecione **Usuário API**.

4. Conclua o formulário obtido com as informações do usuário:
    - Endereço de e-mail
    - Nome
    - Sobrenome

    > O campo Nome de Usuário exibe o endereço de e-mail inserido. Na maioria dos casos, você não deve editar esse padrão. Veja Quando editar um nome de usuário.

5. Se quiser alterar o nome de exibição desse usuário, edite o texto predefinido no campo **Nome de exibição**.
6. Atribua uma senha digitando-a nos campos **Senha** e **Confirmar senha**.
7. Mantenha a função **Operações de gerenciamento de API Cisco ISE** selecionada na seção **Atribuir funções**.
8. Clique em **Concluído** para adicionar o usuário.

Se você não conseguir executar tarefas na página **Usuários**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Gerenciamento de usuários

Como atribuir funções a usuários

Você pode conceder aos usuários acesso a dados e recursos do Ivanti Neurons for MDM atribuindo funções. É possível atribuir funções diretamente para usuários ou grupos de usuários. A atribuição de uma função a um **grupo de usuários**[1] fornece essa função a todos os usuários nesse grupo.

A função Somente Leitura do Usuário não é atribuída aos usuários por padrão.
A página Funções e as opções associadas ficam ocultas para os locatários que têm acesso ao Ivanti Neurons for UEM e ao Ivanti Neurons for MDM.

Os usuários não podem atribuir permissões que eles já não tenham. As permissões e funções que não estiverem atribuídas aos usuários não estão disponibilizadas para seleção. Neste caso, uma mensagem de erro é exibida. Quando um administrador do Ivanti Neurons for MDM ou um administrador parceiro tenta atribuir funções a um administrador parceiro, o Ivanti Neurons for MDM exibe uma mensagem informando que o administrador parceiro deve realizar essa operação no Portal do Prestador de Serviços.

Para mais informações sobre funções, consulte Roles_Management.htm.

Procedimento:

1. Acesse:
   - **Usuários > Usuários** *ou*
   - **Usuários > Grupos de usuários.**
2. Selecione um ou mais usuários ou grupos de usuários.
3. Clique em **Ações**.
4. Na página Detalhes do usuário ou Detalhes do grupo de usuário, selecione **Atribuir funções** *ou*
   Na página Lista de usuários ou Lista de grupos de usuários, selecione **Incluir funções**.
5. Selecione uma ou mais das seguintes funções que deseja atribuir:
   - Gerenciamento do sistema | Entre espaços
   - Somente leitura do sistema | Entre espaços

[1] a list of users that you want to treat in the same way.

- Gerenciamento do usuário | Entre espaços
- Somente leitura do usuário | Entre espaços
- Importação e convite de usuário do LDAP | Entre espaços
- Gerenciamento do dispositivo | Específico do espaço
- Somente leitura do dispositivo | Específico do espaço
- Gerenciamento de aplicativo e conteúdo | Específico do espaço
- Somente leitura de aplicativo e conteúdo | Específico do espaço
- Ações do dispositivo | Específico do espaço
- Operações de Cisco ISE | Entre espaços
- Gerenciamento de tarefas agendadas | Entre espaços
- Serviços da Plataforma Comum (CPS) | Entre espaços
- Gerenciamento de migração de baixo impacto do usuário | Entre espaços
- Registro de dispositivo personalizado | Entre espaços
- Editar Gráfico da Microsoft | Entre espaços
- Enviar/cancelar apagamento | Entre espaços
- Visualizar Gráfico da Microsoft | Entre espaços
- Gerenciar integração do Access | Entre espaços

6. Clique em **Avançar**.
7. Se as funções selecionadas forem limitadas por espaço, selecione Espaços para todas as funções desse tipo.

   Se houver apenas um Espaço (Espaço padrão), a etapa Especificar Espaço será ignorada durante a atribuição de uma função limitada por Espaço.

   A página de resumo exibe o nome do Espaço para rodadas limitadas por Espaço como Espaço padrão.

8. Revise o resumo das funções a serem atribuídas e clique em **Concluído**.

Conceder permissão à equipe de helpdesk para usar as ações básicas do dispositivo

As funções do helpdesk geralmente permitem que os funcionários visualizem dados. Entretanto, algumas organizações preferem incluir as ações básicas do dispositivo:

- Forçar registro
- Bloquear
- Desbloquear
- Enviar mensagem
- Desativar
- Apagar

Procedimento

Você pode conceder permissão para as ações.

1. Acesse **Usuários > Usuários** *ou* **Usuários > Grupos de usuários**.
2. Selecione um ou mais usuários ou grupos de usuários.
3. Clique em **Ações**.
4. Na página Detalhes do usuário ou Detalhes do grupo de usuário, selecione **Atribuir funções** *ou* Na página Lista de usuários ou Lista de grupos de usuários, selecione **Incluir funções**.
5. Selecione **Somente leitura do dispositivo**.
6. Selecione **Ações do dispositivo**.
7. Clique em **Concluído**.

Certifique-se de selecionar Dispositivo Somente Leitura antes de selecionar Ações do Dispositivo para que os usuários tenham as permissões esperadas.

Funções do usuário

As funções de usuário determinam o que os usuários podem fazer e quais páginas podem ver no . A tabela a seguir lista as funções que você pode atribuir e o que elas significam.

Função	Descrição	Específico do espaço
Gerenciamento do sistema	Permite que um administrador gerencie configurações no nível do locatário, como certificados de MDM, Configurações do App Catalog, entre outras.	Não
Somente leitura do sistema	Permite que um administrador visualize configurações no nível do locatário, como certificados de MDM, Configurações do App Catalog, entre outras.	Não
Gerenciamento de usuários	Permite que um administrador adicione e remova usuários, atribua funções e adicione usuários aos grupos de usuários.	Não
Somente leitura do usuário	Permite que um administrador visualize usuários e grupos de usuários, além de catálogos de aplicativos e conteúdo.	Não
Gerenciamento de dispositivos	Permite que um administrador gerencie grupos de dispositivos, configurações e políticas, além de executar todas as ações do dispositivo.	Yes (Sim)

Função	Descrição	Específico do espaço
Somente leitura do dispositivo	Permite que um administrador visualize grupos de dispositivos, configurações e políticas.	Yes (Sim)
Gerenciamento de aplicativo e conteúdo	Permite que um administrador adicione, distribua e remova Apps e Conteúdos.	Yes (Sim)
Somente leitura de aplicativo e conteúdo	Visualizar dados em Usuários, Apps, Conteúdo, incluindo tarefas AppConnect	Yes (Sim)

Função	Descrição	Específico do espaço
Ações do dispositivo	Permite que um administrador inicie ações do dispositivo, como: • Forçar registro • Bloquear • Desbloquear • Enviar mensagem • Desativar • Apagar Você deve selecionar Somente leitura do dispositivo antes de selecionar Ações do dispositivo.Caso contrário, os usuários não terão as permissões esperadas.	Yes (Sim)
Convite e importação de usuário do LDAP	Permite que um administrador registre usuários do LDAP e envie convites para registrar dispositivo(s)	Não
Operações de Cisco ISE	Permite que um administrador chame as API necessárias para integração com Cisco ISE.	Não

Função	Descrição	Específico do espaço
Gerenciamento de tarefas agendadas	Permite que um administrador crie e gerencie tarefa(s) agendada(s) para várias operações administrativas.	Não
Serviços da Plataforma Comum (CPS)	Permite que um administrador use os Serviços da Plataforma Comum.	Não
Gerenciamento de migração de baixo impacto do usuário	Permite que um administrador gerencie as configurações de migração de baixo impacto do usuário.	Não
Registro de dispositivo personalizado	Permite que um administrador registre um dispositivo usando o registro de dispositivo personalizado.	Não
Editar Gráfico da Microsoft	Permite que um administrador edite as configurações de API de gráfico da Microsoft para proteção de aplicativos do Office 365.	Não

Função	Descrição	Específico do espaço
Ver Gráfico da Microsoft	Permite que um administrador visualize as configurações de API de gráfico da Microsoft para proteção de aplicativos do Office 365.	Não
Enviar/cancelar apagamento	Permite que um administrador envie um comando de apagamento a um dispositivo ou cancele um comando de apagamento emitido antes de ser executado.	Não
Gerenciar integração do Access	Permite que um administrador gerencie a integração do Access.	Não

Para obter mais informações, consulte Como atribuir funções

Localizar e filtrar usuários

Esta seção contém os seguintes tópicos:

Como localizar um usuário

Após adicionar muitos usuários, pode ser útil usar filtros ou pesquisas para encontrar rapidamente uma entrada de usuário.

Procedimento

1. Acesse **Usuários**.
2. Digite os caracteres na caixa de pesquisa.

Usando a Pesquisa avançada para usuários

Você pode usar a opção Pesquisa avançada para pesquisar usuários com base em regras para identificar e visualizar os usuários com critérios específicos. As opções de regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). Os usuários correspondentes às regras são exibidos abaixo da seção. As regras podem ser construídas usando-se os seguintes operadores:

- começa com
- termina com
- contém
- não contém
- não começa com
- não termina com

- é menor que
- é maior que
- está no intervalo
- é igual a
- é diferente de

A partir do Ivanti Neurons for MDM 91, o Administrador do Ivanti Neurons for MDM exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo Nome do grupo de usuários é selecionado no Criador de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

Procedimento

1. Na página Usuários, clique no link **Pesquisa avançada**.
2. Clique em **Qualquer** se os usuários precisarem corresponder a pelo menos uma das regras, ou clique em **Todos** se os usuários precisarem corresponder a todas as regras.
3. Crie uma regra que defina os critérios de pesquisa, como Grupo de usuários, Atributo de usuário personalizado e Atributo LDAP personalizado.
4. (Opcional) Clique em + para criar regras adicionais, se necessário.
5. (Opcional) Clique em **Salvar** para salvar a consulta.
6. Clique em **Pesquisar**. A lista de usuários que correspondem aos critérios de pesquisa é exibida na página.

Carregando as consultas de pesquisa para usuários

Procedimento

1. Na página Usuários, clique no link **Pesquisa avançada**.
2. Clique no ícone Pasta. A janela **Pesquisa avançada** é exibida. A lista das consultas de pesquisa criadas é exibida na seção **Consulta carregada**. Os seguintes detalhes são exibidos nessa seção:
   - **Nome da consulta** - O nome da consulta carregada.
   - **Conteúdo da consulta** - Exibe o conteúdo sobre as regras que definem a consulta de pesquisa.
   - **Ações** - Selecione a ação a ser executada na consulta.
3. Clique em **Carregar consulta** na coluna **Ações** para exibir a lista de usuários que correspondem aos critérios definidos na consulta carregada.
   Para excluir uma consulta carregada, clique no ícone Excluir.

Como filtrar usuários

A barra de navegação lateral Filtros apresenta várias seções que ajudam a pesquisar um usuário específico na lista de usuários. O assistente Gerenciar Filtros contém a lista de todas as seções que você pode selecionar para exibição na barra de navegação Filtros.

Procedimento

1. Acesse **Usuários**.

2. Clique nas caixas de seleção relevantes das seções presentes no assistente Gerenciar Filtros. Você pode pesquisar nas seguintes seções:

    - Administradores
    - Status do Google
    - Status do convite
        - Concluído (O usuário recebeu e respondeu.)
        - Expirado (O usuário não respondeu a tempo.)
        - Não convidado (Você não convidou esse usuário.)
        - Pendente (resposta do usuário pendente.)
    - Expiração da senha
        - Expira (Usuários com opção de expiração de senha definida para data finita.)
        - Nunca (Usuários com opção de expiração de senha definida para nunca.)
    - Grupo de usuários (Selecione o **grupo de usuários**[1] de interesse.)
    - Origem do usuário
        - LDAP
        - AAD
        - Registro
        - Salesforce
        - Local

[1] a list of users that you want to treat in the same way.

- Sincronização
  - Sincronização direta: lista os usuários que foram sincronizados diretamente do servidor LDAP
  - Sem sincronização: lista os usuários que foram removidos do servidor LDAP
  - Sincronização indireta: lista os usuários que foram sincronizados indiretamente do servidor LDAP
  - N/A

3. (Opcional) Clique em **Restaurar padrões** para retornar a seleção aos filtros predefinidos. A barra de navegação Filtros exibe as seções selecionadas. Se você desmarcar todas as caixas de seleção do assistente Gerenciar Filtros, a barra de navegação lateral Filtros exibirá todas as seções.
4. Clique em qualquer lugar fora do assistente Gerenciar Filtros para sair do assistente.
5. Clique no ícone X para fechar a barra de navegação lateral Filtros e clique em **Filtros** para reabri-la.

Como atribuir usuários aos grupos de usuários

Esta seção contém os seguintes tópicos:

Atribuir usuários a grupos de usuários é uma boa forma de minimizar o número de vezes necessárias para repetir tarefas como:

- distribuir apps
- atribuir funções

Atribuição de usuários na página Usuários

1. Acesse **Usuários**.
2. Selecione os usuários com os quais você deseja trabalhar.
3. Clique em **Ações**.
4. Selecione **Atribuir ao grupo**.
5. Selecione os grupos ou clique em **Criar novo** para começar um novo grupo.
6. Clique em **Salvar**.

Atribuição de usuários na página Grupos de usuários

1. Acesse **Usuários > Grupos de usuários**.
2. Selecione os grupos de usuários com os quais você deseja trabalhar.
3. Clique em **Ações** (canto superior direito).
4. Selecione **Atribuir usuários**.

5. Digite o endereço de e-mail para cada usuário.
6. Clique em **Atribuir usuários**.

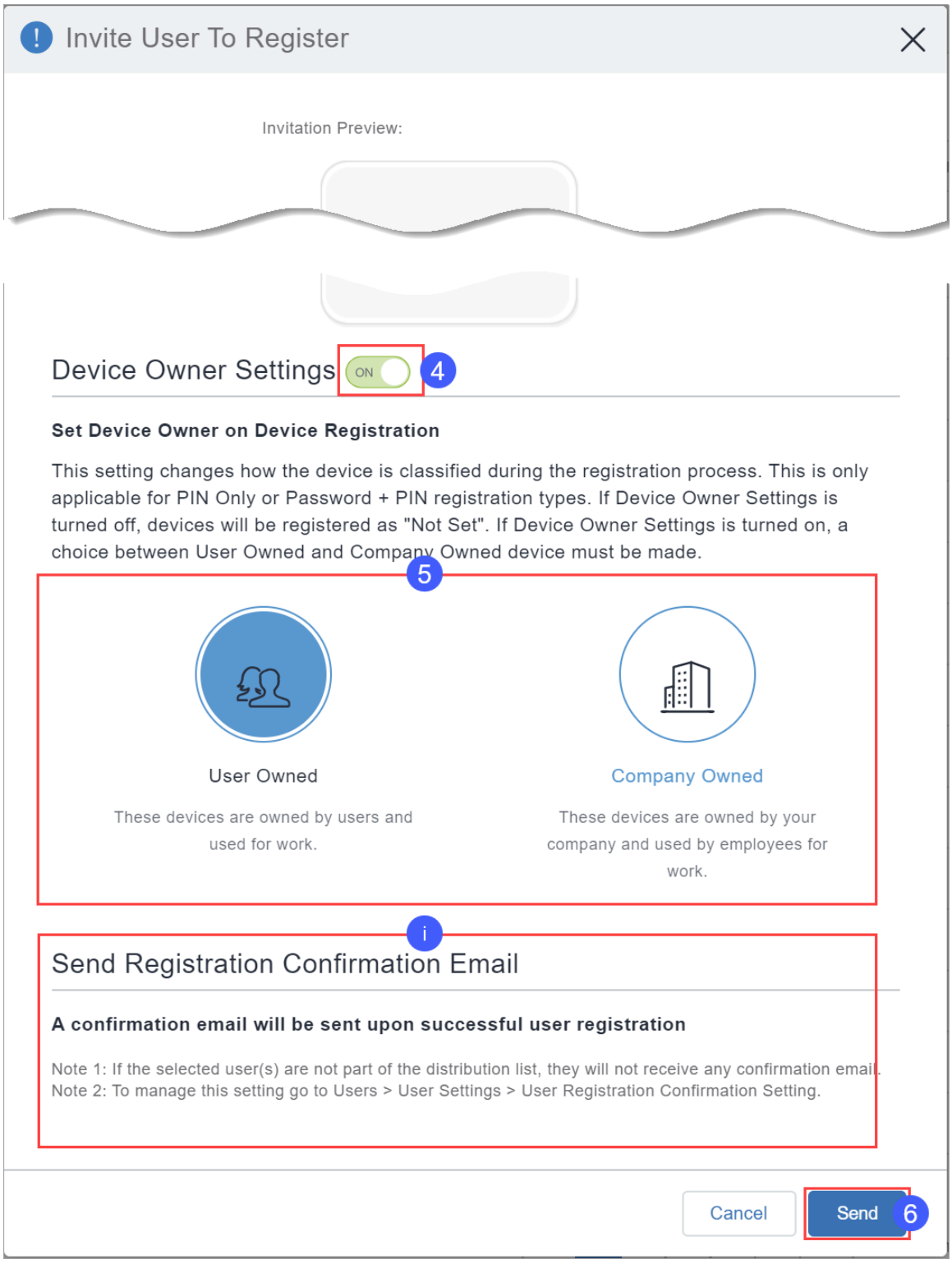
Como convidar usuários

Ao adicionar um usuário, você tem a oportunidade de convidá-lo para registrar dispositivos. Na verdade, essa opção é selecionada por padrão. O usuário convidado recebe uma mensagem por e-mail com as informações necessárias para o registro. Você também pode convidar (ou convidar novamente) um usuário na página **Usuários > Usuários**.

Procedimento

1. Acesse **Usuários**.
2. Selecione os usuários que deseja convidar.
3. Selecione **Ações > Enviar convite**. A Visualização de convite aparece junto com uma opção para

definir a propriedade do dispositivo como **Propriedade do usuário** ou **Propriedade da empresa**.



4. Como alternativa, ative as **Configurações de Propriedade do dispositivo**.
5. Clique em **Propriedade do usuário** ou **Propriedade da empresa**. Essa configuração altera a forma como o dispositivo é classificado durante o processo de registro. Isso é aplicável apenas aos tipos de registro Somente PIN ou Senha + PIN. Se **Configurações de propriedade do dispositivo** estiver habilitado, os dispositivos serão registrados como "Não definido". Para dispositivos supervisionados, a configuração de propriedade do dispositivo será "Propriedade da empresa".
6. Clique em **Enviar**. Se um registro de dispositivo baseado em PIN foi realizado, o usuário receberá um PIN em seu endereço de e-mail registrado. Se um registro baseado em código QR for definido, o usuário receberá um código QR.
7. Clique em **Ok**.

Se o recurso de e-mail de confirmação de registro estiver ativado, conforme descrito em "Como configurar e usar e-mails de confirmação de registro" na página 25, você também verá um lembrete de que o usuário receberá um e-mail de confirmação de registro após o registro feito com sucesso. Para receber o e-mail, o usuário precisa fazer parte da lista de distribuição especificada em "Como configurar e-mails de confirmação de registro do usuário" na página 113 em "Configurações do usuário" na página 98.

Para obter mais informações, consulte Importação de usuários LDAP.

Ativação e desativação de usuários

Esta seção contém os seguintes tópicos:

Os usuário locais e LDAP podem ter status ativado ou desativado. Com base em seu status, você pode criar políticas personalizadas usando a condição Usuário ativado e configurando uma ação para a condição no construtor de regras. Por exemplo, pode haver uma regra de política personalizada para desativar os dispositivos que pertencem a usuários locais/LDAP desativados.

Ativação e desativação de usuários locais

Por padrão, os usuários locais são criados com status ativado.

Procedimento

1. Acesse **Usuários**.
2. Clique no nome de exibição do usuário local.
3. Clique em **Editar**. É exibida a janela **Autenticação necessária**.
4. Digite a senha do administrador e clique em **Autenticar**.

   Quando a senha é digitada incorretamente diversas vezes, e o "Limite de falhas de login" definido em "Configurações de complexidade de senha" é ultrapassado, a conta é bloqueada, e sua sessão atual é encerrada.

5. Marque ou desmarque a opção **Ativado** para ativar ou desativar o usuário local.
6. Clique em **Salvar**.

Ativação e desativação de usuários LDAP

Os usuários LDAP somente podem ser ativados ou desativados no Microsoft Active Directory. No Microsoft Active Directory, quando você abre as propriedades de uma conta de usuário, clica na guia **Conta** e marca ou desmarca as caixas de seleção na caixa de diálogo de opções **Conta**, os valores numéricos são atribuídos ao atributo **UserAccountControl**. O valor atribuído ao atributo informa ao Windows quais opções foram ativadas. Depois de atribuir um valor ao atributo UserAccountControl, o status do usuário o refletirá após a sincronização do LDAP com o Ivanti Neurons for MDM.

Você pode atribuir os seguintes valores:

- 512 - Ativado.
- 514 - Desativado.
- 66048 - Ativado, senha nunca expira.
- 66050 - Desativado, senha nunca expira.

Exibir contas de usuário

Procedimento

1. Clique em **Iniciar**.
2. Vá para **Programas**.
3. Vá para **Ferramentas Administrativas**.
4. Clique em **Usuários e computadores do Active Directory**.

Para mais informações, consulte https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro.

Você pode exibir e editar os atributos usando a ferramenta Ldp.exe ou o snap-in Adsiedit.msc. Somente administradores experientes devem usar essas ferramentas para editar o Active Directory. As duas ferramentas ficam disponíveis após a instalação das ferramentas de suporte da mídia de instalação original do Windows.

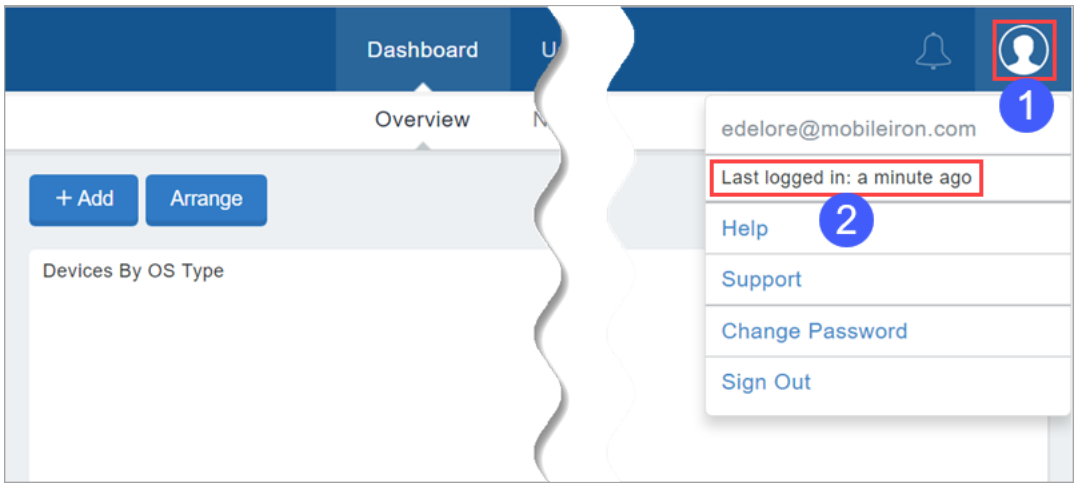
Gerenciar vários logins de administrador

O portal administrativo do Ivanti Neurons for MDM aceita múltiplas sessões, de modo que o administrador possa visualizar diferentes páginas do portal ao mesmo tempo. Se você for administrador, poderá visualizar sua última data de login para ajudar a acompanhar os vários logins.

Exibir o último login do administrador

Procedimento

1. Clique no ícone da Conta.



2. Visualize a entrada **Data do último login:**.

Como alterar a senha

Esta seção contém os seguintes tópicos:

Se o usuário tiver a função de Gerenciamento do Sistema, somente um Superusuário ou o usuário atualmente conectado poderão ver a opção **Alterar senha**.

Você pode alterar sua senha do Ivanti Neurons for MDM. Você também pode alterar a senha para outro usuário, caso tenha permissão.

Procedimento

1. Clique no ícone da Conta (canto superior direito).

2. Selecione **Alterar senha** no menu suspenso.
3. Insira sua senha atual.
4. Insira sua nova senha.
5. Insira a nova senha novamente.
6. Para não definir uma data de expiração, selecione **Definir senha para nunca expirar**.

   Definir uma senha sem data de expiração substitui a configuração **Período de expiração de senha** definida em Usuários > Configurações do usuário > Configuração da complexidade da senha.

7. Clique em **Concluído**.

> Para redefinir a senha da conta local prestes a expirar, desmarque **Definir senha para nunca expirar**. Quando a opção é desmarcada, uma janela pop-up exibe a data de expiração da senha anterior aplicada ao usuário.

Como alterar a senha pela guia Usuários

Procedimento

1. Acesse **Usuários**.
2. Clique no nome de exibição para o usuário.
3. Clique em **Editar** (canto superior esquerdo). A janela **Autenticação necessária** é exibida. Antes de editar o usuário, os administradores (que são usuários locais ou usuários do LDAP) devem se autenticar inserindo a senha de administrador.
4. Digite a senha do administrador e clique em **Autenticar**.

> Quando a senha é digitada incorretamente diversas vezes, e o "Limite de falhas de login" definido em "Configurações de complexidade de senha" é ultrapassado, a conta é bloqueada, e sua sessão atual é encerrada.

5. Insira a senha atual no campo **Senha atual**.

> Esse campo não será exibido se você estiver alterando a senha para outro usuário.

6. Insira a nova senha no campo **Alterar senha**.
7. Confirme a nova senha.
8. Clique em **Salvar** (canto superior esquerdo).

Aplicação de ajuste para que senhas nunca expirem

1. Acesse **Usuários**.
2. Selecione um ou mais usuários.

3. Clique em **Ações**.
4. Selecione **Atribuir senha para nunca expirar**. A janela **Definir que a senha da conta local nunca expira** é exibida.
5. Clique em **Enviar**.

Remoção da configuração para que senhas nunca expirem

1. Acesse **Usuários**.
2. Selecione um ou mais usuários.
3. Clique em **Ações**.
4. Selecione **Remover senha para nunca expirar**. A janela **Remover senha da conta local para nunca expirar** é exibida.
5. Clique em **Enviar**. Depois de remover essa configuração, a data de expiração da senha anterior será aplicada aos usuários.

Como alterar o nome de usuário do administrador do locatário

Você pode alterar o nome de usuário do administrador de locatários para facilitar a introdução de um novo administrador de locatários. Como o administrador do locatário nunca poderá ser excluído, essa é uma forma de alterá-lo para outro nome de usuário.

Esse recurso oferece suporte aos seguintes cenários:

Um usuário com todas as funções altera o nome de usuário do administrador do locatário

1. O administrador do locatário deixa a empresa.
2. Um usuário com funções de gerente de usuário altera o nome de usuário, o endereço de e-mail, o nome, o sobrenome e a senha do administrador do locatário do novo administrador do locatário.

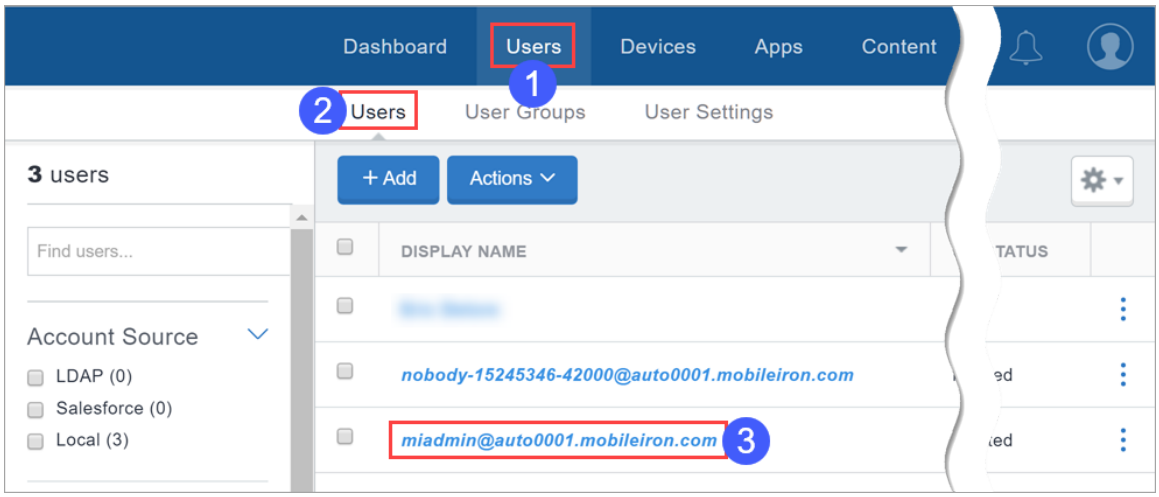
   Consulte Como atribuir funções e Como alterar uma senha para obter informações sobre atribuições de funções e alterações de senha.

O administrador do locatário altera o nome de usuário para um novo administrador do locatário antes de deixar a empresa

1. Antes de deixar a empresa, o administrador do locatário altera o nome de usuário e a senha.
2. O administrador do locatário deixando a empresa passa essas informações ao novo administrador do locatário.

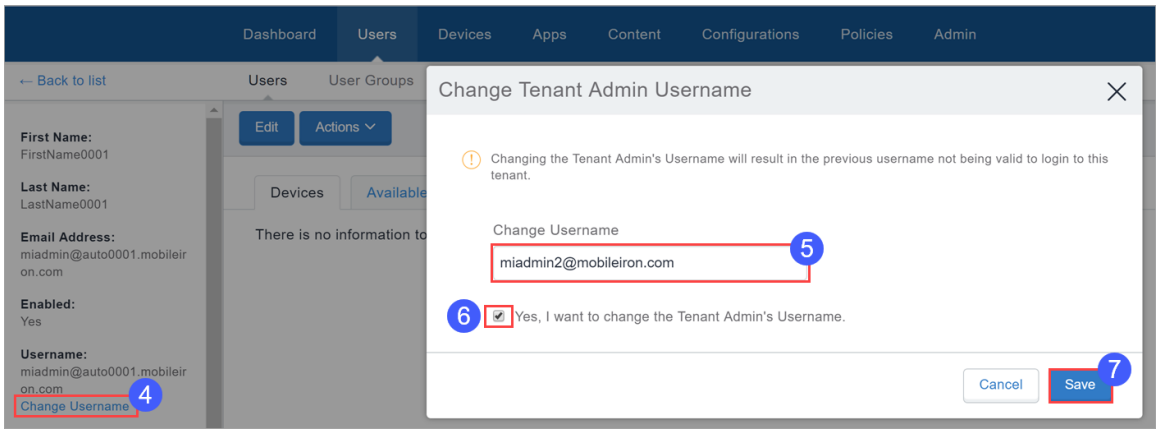
Como alterar o nome de usuário do administrador do locatário

1. Selecione **Usuários**.



2. Selecione a subguia **Usuários**.

3. Clique no nome de exibição do administrador do locatário.



4. Clique em **Alterar nome de usuário**.

5. Insira o novo nome de usuário.

6. Clique na caixa ao lado de **Sim, desejo alterar o nome de usuário do administrador do locatário** até que apareça uma marca de seleção.

7. Clique em **Salvar**.

Como enviar uma mensagem

Esta seção contém os seguintes tópicos:

Você pode enviar uma mensagem a qualquer usuário conhecido. As mensagens podem ser e-mail ou **notificações push**[1]. Somente usuários com dispositivos registrados podem receber notificações por push.

Pré-requisitos

- Para dispositivos iOS, certifique-se de que o cliente Go esteja instalado.
- Para dispositivos macOS, certifique-se de que o cliente Mobile@Work esteja instalado.

Enviando uma mensagem para usuários

1. Acesse **Usuários > Usuários**.
2. Selecione os usuários para os quais deseja enviar uma mensagem.
3. Clique em **Ações** (canto superior direito).
4. Selecione **Enviar mensagem**.
5. Se você não quiser enviar um e-mail, desmarque a caixa **Enviar uma mensagem por e-mail**.
6. Ao enviar um e-mail, insira o assunto e a mensagem.
7. Ao enviar uma notificação por push, selecione a caixa **Enviar uma notificação por push** e insira o texto da mensagem.
8. Clique em **Enviar**.

[1] a message or alert that is sent to the device.

Enviando uma mensagem para dispositivos

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione os dispositivos para os quais deseja enviar uma mensagem.
3. Clique em **Ações** (canto superior direito).
4. Selecione **Enviar mensagem**.
5. É possível clicar no link do nome do dispositivo para ir para a página de detalhes do Dispositivo e, depois, clicar no ícone **Enviar mensagem**  .
6. Se você não quiser enviar um e-mail, desmarque a caixa **Enviar uma mensagem por e-mail**.
7. Ao enviar um e-mail, insira o assunto e a mensagem.
8. Ao enviar uma notificação por push, selecione a caixa **Enviar uma notificação por push** e insira o texto da mensagem.

   > Uma mensagem de notificação por push também pode incluir URLs que os usuários podem acessar.

9. Clique em **Enviar**.
   Quando uma notificação por push é enviada ao usuário, o usuário poderá ver um ícone de sino na barra de ferramentas do dispositivo. Tocando no ícone de sino, o usuário poderá visualizar o histórico de notificações recebidas e realizar uma ação ou excluir uma notificação.

Como remover usuários dos grupos de usuários

Esta seção contém os seguintes tópicos:

- "Removendo usuários na página Usuários" abaixo
- "Removendo usuários na página Grupos de usuários" abaixo

Remover um usuário de um grupo de usuários significa que:

- qualquer função atribuída ao grupo será removida do usuário
- qualquer aplicativo atribuído ao grupo não estará mais disponível no **App Catalog**[1] do usuário
- os apps configurados para serem removíveis serão removidos dos dispositivos do usuário

Removendo usuários na página Usuários

1. Selecione o usuário com o qual você deseja trabalhar.
2. Clique em **Ações** (canto superior direito).
3. Selecione **Remover do grupo**.
4. Selecione os grupos.
5. Clique em **Remover**.

Removendo usuários na página Grupos de usuários

1. Clique no grupo de usuários para exibir seus detalhes.
2. Clique em **Editar** (canto superior direito).

[1]a list of mobile apps you have made available for your users. Includes apps that users can download from public app stores and apps you intend to distribute using the device management system (In-house apps).

3. Clique no link **Remover** ao lado do usuário que você deseja remover.
4. Clique em **Salvar** (canto superior direito).

Como excluir um usuário

Esta seção contém os seguintes tópicos:

- "O que acontece ao excluir um usuário local" abaixo
- "E os usuários LDAP?" abaixo

Procedimento

1. Acesse **Usuários** > **Usuários**.
2. Selecione a entrada para o usuário.
3. Clique em **Ações** (canto superior direito).
4. Selecione **Excluir**.

Quando um administrador do Ivanti Neurons for MDM ou um administrador parceiro tenta excluir um administrador parceiro, o Ivanti Neurons for MDM exibe uma mensagem informando que o administrador parceiro deve realizar essa operação no Portal do Prestador de Serviços.

O que acontece ao excluir um usuário local

- Todas as informações relacionadas a um usuário excluído são excluídas do sistema.
- Os dispositivos associados ao usuário serão desativados.
- O conteúdo carregado pelo usuário permanece.
- Não são mais permitidos registros do dispositivo para a conta do usuário.

E os usuários LDAP?

- Se o servidor LDAP foi desabilitado, um usuário LDAP não poderá ser excluído permanentemente. A próxima sincronização dos dados do LDAP irá restaurar um usuário LDAP excluído.
- Se o grupo ou servidor LDAP foi excluído, os usuários LDAP se tornam usuários locais e não poderão ser excluídos.

- Quando um usuário for excluído do LDAP, ele não será excluído do Cloud. O status de sincronização mudará para "NO_SYNC", mas o usuário não será removido.

Como exportar usuários

Como administrador, você pode exportar uma lista de usuários a partir do Ivanti Neurons for MDM.

Quando o PIN de registro de dispositivo do usuário for exportado para um arquivo CSV, será usada a máscara '****' em vez do PIN real, por motivos de segurança.

Procedimento

1. Acesse **Usuários** > **Usuários**.
2. Selecione um ou mais usuários na lista.
3. Clique em **Exportar para CSV**.

Você será avisado com um pop-up informando que o relatório de exportação levará algum tempo para ser processado. Após enviar a solicitação, você deve aguardar a conclusão dela para enviar outra. Quando o relatório estiver pronto, você receberá uma mensagem para Baixar ou Excluir o relatório gerado. Você também receberá um e-mail contendo um link para baixar o relatório.

Os detalhes dos atributos **Usuário personalizado** e **LDAP** também podem ser exportados para um arquivo CSV junto com outros detalhes.

Quando for adicionado um usuário com algum valor de campo que contenha os caracteres +,-,=, ou @, os dados do usuário no arquivo CSV exportado prefixarão automaticamente o campo com aspas simples ('), e o símbolo de barra vertical (|) será adicionado com uma barra invertida (\). Isso é feito para evitar a vulnerabilidade de injeção no Excel.

Como atribuir atributos personalizados aos usuários

Você pode atribuir atributos personalizados de usuário, como Departamento, a um ou mais usuários. Cada atributo tem um valor correspondente que você pode usar para tarefas, como criar configurações e grupos de usuários. Você pode atribuir atributos personalizados a um ou mais usuários.

Procedimento

1. Acesse **Administrador > Sistema > Atributos** para criar novos atributos personalizados, se necessário.
2. Acesse **Usuários**.
3. Selecione um ou mais usuários.
4. Clique em **Ações**.
5. Selecione **Atribuir atributos personalizados**.
6. Selecione uma das opções a seguir:
   - Forçar a designação (substituição) de todos os atributos, mesmo que quaisquer valores existentes sejam encontrados.
   - Substituir apenas se o valor estiver vazio e ignorar os atributos com valores existentes.
7. Selecione os atributos que deseja atribuir e insira seus valores (valores vazios não são permitidos).
8. Clique em **Atribuir**.

Tópicos relacionados:

- "Atributos" na página 1164
- "Variáveis" na página 503

Como remover atributos personalizados dos usuários

Você pode remover atributos personalizados de um ou mais usuários.

 Proceda com cuidado, pois esta ação não poderá ser revertida.

Procedimento

1. Acesse **Usuários**.
2. Selecione um ou mais usuários.
3. Clique em **Ações**.
4. Selecione **Remover atributos personalizados**.
5. Selecione os atributos que deseja remover.
6. Clique em **Remover**.

Tópicos relacionados:

- "Atributos" na página 1164
- "Variáveis" na página 503

Alteração da localidade do usuário

Por padrão, a localidade do usuário é definida como a localidade do locatário. Se necessário, você pode alterar a localidade de um locatário individual.

Procedimento

1. Acesse **Usuários**.
2. Clique no nome de exibição para o usuário.
3. Clique em **Editar**. É exibida a janela **Autenticação necessária**.
4. Digite a senha do administrador e clique em **Autenticar**.

   Quando a senha é digitada incorretamente diversas vezes, e o "Limite de falhas de login" definido em "Configurações de complexidade de senha" é ultrapassado, a conta é bloqueada, e sua sessão atual é encerrada.

5. No campo Localização, clique em **Alterar**.
6. Na janela **Alterar localidade do usuário**, selecione a localidade desejada na lista suspensa **Alterar localidade do usuário para:**.
7. Clique em **Concluído**.
8. Clique em **Salvar**.

Edição de nome do usuário

Ao adicionar um usuário, o texto inserido para o endereço de e-mail é listado automaticamente para o nome de usuário. Na maioria dos casos, deixe o nome de usuário padrão, pois:

- É necessário um nome de usuário no formato de endereço de e-mail.
- É conveniente usar a variável do nome de usuário em **configurações**[1], embora o endereço de e-mail também possa ser usado.

O único momento para editar um nome de usuário é quando, raramente, existe um conflito com um nome de usuário existente, pois eles devem ser únicos em todo o sistema de gerenciamento do dispositivo. Um conflito pode acontecer, por exemplo, se dois departamentos em uma organização registrarem o mesmo dispositivo no sistema de gerenciamento de dispositivo.

Se acontecer um conflito com o nome de usuário

Se você não conseguir adicionar um nome de usuário devido a um conflito de nome de usuário, insira um nome de usuário diferente usando o formato de endereço de e-mail. O endereço de e-mail não precisa corresponder a uma conta de e-mail real. Por exemplo, você pode alterar o seguinte endereço de e-mail:

ksmith@minhaempresa.com

para

ksmith21@minhaempresa.com

Se você editar o nome de usuário, todas as configurações que incluírem o nome de usuário como uma variável não funcionarão para esse usuário. Crie configurações alternativas que usam a variável do endereço de e-mail.

[1]collections of settings that you send to devices.

Optar por não exibir o conjunto de dados de localização

Esta seção contém os seguintes tópicos:

- "Para dispositivos iOS" abaixo
- "Para dispositivos Android" abaixo

Se estiver aplicada uma configuração de privacidade para permitir a coleta de dados de localização, o usuário do dispositivo poderá substituir a configuração.

Para dispositivos iOS

Os usuários de dispositivos iOS podem desativar os serviços de localização para evitar o envio de dados de localização ao sistema de gerenciamento de dispositivos, a partir da seguinte configuração:

Configurações > Privacidade > Serviços de localização

Para dispositivos Android

Os usuários de dispositivos Android podem desativar a configuração de localização para impedir a coleta de dados. A localização dessa configuração varia de acordo com o fabricante. Também é solicitado que os usuários dos dispositivos Android aceitem a solicitação para os dados de localização.

Informações de tempo limite

O tempo de inatividade do portal administrativo varia de 5 a 15 minutos, e o tempo para expiração é de 24 horas.

Procedimento

1. Acesse **Usuários > Configurações do usuário**.
2. Edite as configurações padrão **Complexidade da senha**.
3. Na seção Políticas de senha, mova o controle deslizante **Tempo limite de inatividade** para especificar o tempo que um usuário pode ficar inativo antes do tempo de sessão do Portal do administrador ou Portal de autoatendimento. Intervalos de números entre 5 e 15 (minutos).
4. Clique em **Concluído**.

Como optar por não usar a análise de uso do sistema

Diagnósticos de produto e dados de utilização anônimos são coletados para ajudar na melhoria de produtos.

Se quiser manter a privacidade dos dados de utilização, você pode cancelar o envio de análises de uso do sistema.

Procedimento

1. Clique no link **Utilização de dados** na parte inferior da página, no portal administrativo do Ivanti Neurons for MDM. A janela **Utilização de dados** é exibida.
2. Desmarque a caixa de seleção **Enviar dados de diagnóstico e utilização**.
3. Clique em **Salvar**.

Dispositivos

Esta seção contém os seguintes tópicos:

Introdução a dispositivos

Esta seção contém os seguintes tópicos:

Cada entrada na página **Dispositivos** representa um dispositivo móvel que foi registrado no Ivanti Neurons for MDM e lista informações importantes sobre o dispositivo. A página da lista Dispositivos exibe dispositivos com informações como:

- Nome
- Endereço de e-mail
- Número de telefone
- SO
- Tipo de dispositivo
- Status
- Último check-in
- Contagem de violações
- Espaço
- Proprietário legal (para iPads compartilhados)

O endereço IP do Wi-Fi é reportado ao servidor do Ivanti Neurons for MDM. Todas as alterações no endereço IP são reportadas a cada registro. O endereço IP compatível com a RGPD está disponível como opção na página da lista de dispositivos e na página de detalhes do dispositivo. Este recurso exige que os dispositivos sejam registrados via Go 5.5 para iOS ou versões posteriores, e Go 72 ou versões posteriores para Android, segundo a compatibilidade com o Ivanti Neurons for MDM.

À medida que novos campos da RGPD (com Endereço IP e ID eSIM) são adicionados às versões do Ivanti Neurons for MDM, os administradores que já configuraram a RGPD precisam editar o perfil de RGPD caso desejem ocultar os novos campos.

O Identificador de equipamento (EID) aparece como um atributo de iOS quando uma lista de dispositivos é exportada para o formato de planilha (CSV). O EID e o EID móvel (MEID) (quando presente) têm como prefixo uma string de EID ou string de MEID, respectivamente.

O servidor do Ivanti Neurons for MDM não processa o mesmo dispositivo com identificadores de clientes diferentes e registrado com locatários diferentes. O servidor pode processar somente instâncias do mesmo dispositivo com identificadores de clientes diferentes e registrado para o mesmo locatário.

Gerenciamento de dispositivos

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Dispositivos**.
3. Selecione um ou mais dispositivos.
4. Selecione uma ação na lista suspensa **Ações**.

A tabela a seguir lista as ações disponíveis na página Dispositivos:

Categoria	Ação
Comum	• Adicionar ao grupo • Desbloqueio do AppConnect> • Designar atributos personalizados • Atribuir ao Usuário • Desativar área de trabalho remota • Ativar área de trabalho remota • Ativar/desativar Bluetooth • Forçar registro • Bloquear • Remover atributos personalizados • Reiniciar/desligar • Sincronização do status de conformidade do dispositivo • Remover dispositivo • Enviar mensagem • Definir Propriedade • Desbloquear • Apagar
iOS	• Atribuir ao Proprietário legal (somente iPads compartilhados) • Reinstalar apps do sistema do iOS • Definir fuso horário

Categoria	Ação
macOS	• Definir senha de administrador automático do macOS • Definir/alterar a senha de firmware • Definir/Alterar o bloqueio de recuperação
Android	• Entrar no modo de quiosque • Sair do modo de quiosque
Windows 10	Redefinir PIN (somente dispositivos móveis)

Executando ações em um dispositivo

O menu Ações (botão de reticências) permite executar várias ações em um dispositivo selecionado.

Procedimento

1. Clique no nome de um dispositivo. A página de detalhes do dispositivo é exibida.
2. Clique no menu Ações (reticências) para realizar uma das seguintes ações:
   - **Alterar nome do dispositivo**
   - **Excluir dispositivo**
   - **Editar associação ao grupo**
   - **Ativar/desativar Bluetooth**
   - **Scripts e ações via Ivanti Bridge**
   - **Recuperar log do Ivanti Bridge**
   - **Renunciar a propriedade**
   - **Solicitar logs de depuração**
   - **Reiniciar/desligar dispositivo**
   - **Desativar**
   - **Definir Propriedade**

- **Definir/Alterar o bloqueio de recuperação**
- **Apagar**

Definir o fuso horário para um dispositivo

Aplicável para: dispositivos iOS 14.0+ e tvOS 14.0+

Esta ação não exige serviços de localização. A ação do dispositivo de fuso horário também é exibida na página de detalhes de um dispositivo. As mudanças feitas no fuso horário no dispositivo também refletirão no servidor do Ivanti Neurons for MDM.

Esta ação do dispositivo dispara um erro se a restrição **Forçar data e hora automáticas** estiver habilitada na configuração Restrições do iOS.

Procedimento

1. Selecione um ou mais dispositivos.
2. Clique em **Ações** > **Definir fuso horário** nos dispositivos selecionados.
3. Informe a string de fuso horário no formato de ID de fuso horário Olson. Por exemplo, Pacífico/Midway.
4. Clique em **Definir fuso horário.**

Listando dispositivos por critérios

Você pode usar a barra de navegação lateral Filtros para pesquisar e visualizar dispositivos específicos da lista de dispositivos. Use a lista suspensa Espaço para selecionar todos os espaços ou espaços específicos, a fim de visualizar os dispositivos e suas informações relacionadas. Você também pode pesquisar dispositivos usando a versão de exibição ou a versão do pacote. A página Dispositivos exibe tanto a versão do pacote como a versão de exibição dos dispositivos.

Quando você navega na página Grupo de Dispositivos e clica no número abaixo da coluna **Nº de dispositivos**, ou na coluna **Nº instalado** na página **Inventário de Aplicativos**, aparece uma mensagem indicando o nome do espaço para o qual os dispositivos estão listados na página.

Exibição de informações detalhadas do dispositivo

Clique no link na coluna Nome de uma entrada para exibir a página Detalhes do Dispositivo. A página Detalhes do Dispositivo contém diversas abas organizando a seguinte informação:

- **Visão geral** - a tabela a seguir lista todos os detalhes exibidos na guia Visão Geral:

Nome da seção	Descrição
Geral	◦ Localização do dispositivo ◦ Fabricante ◦ Endereço MAC do Wi-Fi ◦ Endereço Wi-Fi-IP (dispositivos Android) ◦ Rede com tether – (dispositivos iOS) ◦ Número de série ◦ Número de série alternativo (dispositivos Android) – Número de série específico do fabricante aplicável a dispositivos Samsung no modo Administrador do dispositivo ou Proprietário do dispositivo ◦ Uso do armazenamento – Armazenamento interno usado (com exceção do Windows) e disponível nos dispositivos ◦ Bateria disponível (Android) ◦ Status da bateria (Android) - carregando, descarregando, cheia e não carregando ◦ Carga estimada da bateria restante (Windows) ◦ Tempo de execução estimado da bateria (Windows) ◦ Atualização disponível (macOS) ◦ Nome da atualização disponível (macOS) ◦ Versão do SO ◦ Versão de desenvolvimento do SO ◦ Versão de compilação suplementar ◦ Extra da versão/SO suplementar ◦ Dispositivo Apple Silicon

Nome da seção	Descrição
	◦ Versão do Firmware ◦ Origem do dispositivo ◦ Proprietário legal ◦ Modo multiusuários ◦ Fuso horário ◦ Atualização do sistema (dispositivos Android) ◦ Versão do patch do Zebra (dispositivos Android) ◦ Último ID do hotfix – (dispositivos Windows) ◦ Último hotfix instalado ligado – (dispositivos Windows)

Nome da seção	Descrição
Configuração	◦ Nome do dispositivo ◦ Identificador do dispositivo ◦ GUID do dispositivo ◦ Dispositivo de registro de dispositivo (dispositivos Apple) ◦ Registro de dispositivo registrado (dispositivos Apple) ◦ Registro de dispositivo automatizado habilitado ◦ Registro de dispositivo automatizado registrado ◦ Registro de usuário registrado (dispositivos Apple) ◦ Apple ID gerenciado registrado (dispositivos Apple) ◦ Grupos de dispositivos ◦ Idioma ◦ Identificadores de dispositivos MDM ◦ ID do cliente do dispositivo ◦ Versão do aplicativo cliente ◦ BundleID do aplicativo do cliente ◦ Cliente registrado ◦ Identificadores de dispositivos EAS ◦ Trava de ativação ativada ◦ Código de bypass do bloqueio de ativação ◦ Termos de serviço ◦ Propriedade

Nome da seção	Descrição
	◦ Conta do iTunes ativa ◦ Serviço de localização do dispositivo ativado ◦ Em quarentena ◦ Sentry bloqueado ◦ Acesso bloqueado ◦ Ação de conformidade bloqueada ◦ Capacidade APNS ◦ Modo supervisionado (dispositivos iOS e macOS) – identifica um dispositivo supervisionado. O dispositivo permanece no controle direto da equipe de TI. O modo supervisionado habilita recursos adicionais do dispositivo (por exemplo, implantações de serviço de campo, dispositivos de ponto de vendas de varejo), dispositivos "credores" usados em serviços e hospitalidade e dispositivos compartilhados entre os alunos em um laboratório de sala de aula. ◦ PIN de apagamento – Clique em **Visualizar** para mostrar o PIN. ◦ Usuário administrador do macOS gerenciado (dispositivos macOS) ◦ Status de criptografia do dispositivo (dispositivos macOS) ◦ Criptografia FileVault habilitada ◦ Chave de recuperação pessoal usada ◦ Chave de recuperação institucional usada ◦ Token de inicialização disponível ◦ Proteção de integridade do sistema ativada

Nome da seção	Descrição
	◦ Senha de firmware ◦ Senha ◦ Alteração pendente ◦ Status do comando ◦ Permitir ROMs de opções ◦ Bloqueio de recuperação ◦ Senha ◦ Bloqueio de recuperação habilitado ◦ Configurações de firewall (dispositivos macOS) ◦ Firewall ativado ◦ Bloquear Todas as Conexões de Entrada ◦ Modo escondido ◦ Status de firewall do aplicativo (dispositivos macOS) ◦ Último backup ao iCloud (dispositivos iOS) ◦ Prazo de tolerância de bloqueio de senha (dispositivos iOS) ◦ ID do Android ◦ Nível da correção de segurança do Android (dispositivos com Android) ◦ Modo de quiosque (dispositivos com Android) ◦ Tipo de certificação Android SafetyNet (dispositivos Android) ◦ Compatível com Android corporativo (dispositivos com Android) ◦ AFW ativado (dispositivos com Android)

Nome da seção	Descrição
	◦ Compatível com Samsung SAFE (dispositivos com Android) ◦ Dispositivos gerenciados de trabalho com Android (Proprietário do dispositivo) ativados ◦ Perfil de trabalho do Android ativado em dispositivos de propriedade da empresa ◦ Dispositivo gerenciado Android com Work Profile ◦ Bloqueio de perfil de trabalho do Android ativado em dispositivos de propriedade da empresa ◦ Help@Work disponível ◦ Compatível com Zebra ◦ Status de Secure Apps ◦ Status de criptografia de Secure Apps ◦ Modo de Criptografia de Aplicativos Seguros ◦ FCM habilitado
Proteção das informações do Windows (dispositivos com Windows)	◦ WIP ◦ Bloqueador do aplicativo configurado ◦ Configurações obrigatórias de EDP

Nome da seção	Descrição
Telefonia	◦ Número do telefone ◦ Tecnologia de celular ◦ IMSI ◦ ICCID ◦ IMEI ◦ IMEI 2 – (Somente em dispositivos Android com porta SIM dupla. Aplicável a Android 8.0 ou mais recente) ◦ MEID ◦ Localização do dispositivo ◦ Operadora ◦ MCC inicial ◦ MNC inicial ◦ Nome do País Atual ◦ Nome do País de Origem ◦ Tecnologia de celular ◦ Roaming ◦ Operador atual ◦ MCC atual ◦ MNC atual ◦ Roaming de dados ◦ Roaming de voz

Nome da seção	Descrição
	Para dispositivos iOS suportados, essas propriedades são exibidas para várias assinaturas de serviço ativo eSIM.
Conformidade do dispositivo do Azure	◦ Identificador de dispositivo do Azure ◦ Status de conformidade do dispositivo do Azure ◦ Código de status do cliente Azure ◦ Hora do relatório de conformidade do dispositivo do Azure ◦ UPN do usuário do dispositivo Azure Intune
Informações da bateria	◦ Nível da bateria - exibe o nível atual de carga da bateria conforme relatado pelo SO Android ◦ Status de integridade da bateria - conforme relatado pelo SO Android ◦ Status de carregamento da bateria - conforme relatado pelo SO Android ◦ Percentual de integridade da bateria (específico do OEM) - integridade da bateria em porcentagem, para os fabricantes de dispositivos suportados, tais como dispositivos Zebra ◦ Data de fabricação da bateria (OEM) - data em que a bateria foi fabricada, para fabricantes de dispositivos suportados, tais como dispositivos Zebra ◦ Ciclos de carga da bateria (OEM) - número de ciclos integralmente concluídos, para fabricantes de dispositivos suportados, tais como dispositivos Zebra

- **Configurações** - exibe os detalhes das **configurações**[1] aplicadas. Para mais informações, consulte "Trabalhando com configurações" na página 445.

[1] collections of settings that you send to devices.

- **Aplicativos instalados**- exibe os detalhes dos aplicativos instalados no dispositivo. A data de instalação da versão atual do aplicativo instalado é exibida na coluna **Data relatada do aplicativo**.

  A data de instalação do aplicativo dos dispositivos que saem da quarentena é a data em que o dispositivo é removido da quarentena.

- **Aplicativos disponíveis** - exibe os detalhes dos aplicativos disponíveis para o dispositivo. A coluna Status indica o status de instalação do aplicativo no dispositivo.

  Somente aplicativos gerenciados têm o status de instalação capturado. O status de instalação de aplicativos não gerenciados aparece como "Não instalado". Você deve converter o aplicativo em Gerenciado para visualizar o status de instalação correto. Não é possível classificar pelo status de instalação do aplicativo.

- **Aplicativos AppConnect** - exibe os detalhes dos aplicativos AppConnect instalados

- **Políticas** - detalhes das **políticas**[1] aplicadas. Para dispositivos comprometidos, verifique o motivo da violação na coluna Violação. Se o dispositivo tiver sido roteado, o sistema exibirá o motivo mostrado na coluna **Violação**:

Prioridade (1 = maior)	Violação
1	Plugin comprometido
2	Cliente violado
3	Fabricante do dispositivo desconhecido: desconhecido
4	Pasta suspeita detectada: [path]
5	Binário suspeito encontrado em: [path]
6	Pasta /data é navegável OU Pasta /data/data é navegável
7	/system/app/Superuser.apk encontrado
8	Gerenciador de pacotes comprometido
9	Aplicativo suspeito encontrado: [package]

[1]sets of requirements and compliance actions defined for devices.

- **Certificados** - detalhes dos certificados instalados.
  Para uso do certificado, marque a coluna Tipo de uso. Se o certificado for específico a um dispositivo, ele exibe o tipo de uso como "dispositivo". Se o certificado for específico a um usuário, ele exibe o tipo de uso como "usuário".
- **Sentry** – Informações do Sentry (Associações do ActiveSync)
- **Atributos** – Atributos personalizados e atributos do dispositivo
- **Usuários** – Exibe a lista de usuários ativos para o dispositivo MacOS supervisionado.

  A guia **Usuários** foi aprimorada e mostra o ID Apple gerenciado como um hiperlink que, se clicado, redireciona à página de detalhes da conta do usuário em um dispositivo iPad compartilhado.
- **Registros** – Visualize e personalize filtros de dispositivos
- **Hardware** – Detalhes de inventário de hardware (sistema, placa mãe, BIOS, unidade de disco rígido, CD-ROM, processador e memória física)

Atribuição ou alteração de usuários e atributos personalizados em massa em dispositivos

Você pode usar o ícone Atribuir em Massa via Upload para carregar um arquivo CSV a fim de atribuir ou alterar usuários e/ou atributos personalizados em massa nos dispositivos.

Procedimento

1. Na página de dispositivos, clique em **Atribuição em massa** no ícone de Upload (ao lado do botão de ações).
2. (Opcional) Clique em **Fazer download do modelo** para salvar um arquivo de modelo CSV que você pode editar e fazer upload.
3. Depois que o arquivo CSV estiver pronto, clique em **Escolher arquivo** para procurar a localização do arquivo CSV ou arraste e solte o arquivo CSV na seção Dados do arquivo.
4. Selecione uma das opções a seguir:

- **Força atribuição (substituição) de todos os atributos, mesmo se algum valor existente for encontrado.**
- **Substituir apenas se o valor estiver vazio e ignorar atributos com valores existentes**

5. Clique em **Upload**.

Exportar dispositivos para um arquivo CSV

Você pode exportar os detalhes de um dispositivo específico usando a opção **Exportar para CSV** da página **Dispositivos**.

Procedimento

1. Acesse **Dispositivos**.
2. Selecione todos ou vários espaços para ver as informações relativas a espaços específicos.
3. Clique no link de contagem de dispositivos. A página com a lista de dispositivos relativa ao espaço selecionado é exibida.
4. Clique na opção **Exportar para CSV** para exportar a lista de dispositivos e os detalhes relacionados para um arquivo CSV. Uma mensagem pop-up aparece informando que o relatório de exportação pode levar algum tempo para ser processado. Aguarde a conclusão da solicitação antes de enviar outra. Quando o relatório estiver pronto, você receberá uma mensagem para Baixar ou Excluir o relatório.
5. Clique em **Baixar**. Você também receberá um e-mail contendo um link para baixar o relatório.
6. (Opcional) Clique em **Excluir** para excluir o relatório.

Pesquisando registros de dispositivos

Procedimento

1. Acesse **Dispositivos** > **Dispositivos**, clique no link da coluna **Nome** de uma entrada.
2. Clique na guia de **Registros**.
3. Utilize os filtros de Ação, Status, Data de Início e Data Final para restringir as mensagens exibidas.

Se você não conseguir visualizar a página **Dispositivos**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Grupos de dispositivos

Esta seção contém os seguintes tópicos:

Na página **Grupos de Dispositivos**, você pode criar listas dos dispositivos que deseja tratar da mesma maneira. É possível definir e atribuir políticas e configurações a grupos de dispositivos. A seguir estão os grupos de dispositivos padrão criados pelo Ivanti Neurons for MDM:

- Todos os dispositivos
- Dispositivos com Android
- Dispositivos com Android corporativo
- Dispositivos com iOS
- Dispositivos tvOS
- Dispositivos macOS
- Dispositivos com Windows

Os detalhes dos apps atribuídos a um grupo de dispositivos específico é exibida na guia **Apps** para o grupo de dispositivos específico.

O grupo de dispositivos tvOS é um subconjunto do grupo de dispositivos iOS. Portanto, as configurações e as políticas aplicadas ao grupo tvOS podem ser substituídas pelo grupo de dispositivos iOS.

Adição de um grupo de dispositivos

Dependendo do tipo de licença que você tem, é possível adicionar um novo grupo de dispositivos com base em regras para identificar dispositivos com critérios específicos. Os dispositivos correspondentes às regras são exibidos abaixo da seção do construtor de regras. As regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). As regras podem ser construídas usando-se os seguintes operadores:

- começa com
- termina com
- contém
- não contém
- não começa com
- não termina com
- é menor que
- é maior que
- está no intervalo
- é igual a
- é diferente de
- não em branco
- em branco

O Administrador do Ivanti Neurons for MDM exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo Nome do grupo de usuários é selecionado no Criador de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

Licença Bronze:

As regras podem identificar dispositivos pelos seguintes critérios:

- Tipo de dispositivo
- SO - sistema operacional (pré-preenchido)
- Versão do SO
- Grupo de usuários

Licença Silver:

As regras podem identificar dispositivos pelos seguintes critérios:

- AAD inscrito
- Número de série alternativo (Android apenas, aplicável a dispositivos Samsung no modo Administrador do dispositivo ou Proprietário do dispositivo)
- Dispositivo dedicado Android
- Compatível com Android corporativo
- Dispositivo gerenciado Android com Work Profile
- Tipo de certificação Android SafetyNet
- Android Work habilitado
- Dispositivos gerenciados de trabalho com Android (Proprietário do dispositivo) ativados
- Perfil de trabalho Android ativado
- Perfil de trabalho do Android ativado em dispositivos de propriedade da empresa
- Capacidade APNS
- Registro de dispositivo automatizado habilitado
- Identificador de dispositivo do Azure
- Status de conformidade do dispositivo do Azure
- Código de status do cliente Azure
- Hora do relatório de conformidade do dispositivo do Azure
- Criptografia BitLocker
- Sentry bloqueado
- Acesso bloqueado
- Token de inicialização disponível
- Tipo provisionado em massa (Apple Configurator, Nenhum ou Registro automatizado de dispositivo registrado)
- Operadora

- Último registro do cliente
- Cliente registrado
- Conformidade
- Ação de conformidade bloqueada
- Nome do país atual (selecione o nome do país atual na lista suspensa)
- MCC atual
- MNC atual
- Atributo de dispositivo personalizado
- Atributo LDAP personalizado
- Atributo de usuário personalizado
- Roaming de dados
- Dispositivo registrado
- Origem do dispositivo
- Tipo de dispositivo
- Nome de exibição
- Criptografia ativada
- Partições de disco rígido
- Nome do país de origem (selecione o nome do país de origem na lista suspensa)
- MCC inicial
- MNC inicial
- Endereço IP
- Modo de quiosque
- Último check-in

- Somente MAM
- Fabricante
- SO
- Edição do SO
- Versão do SO
- Propriedade
- Número de telefone
- Em quarentena
- Bloqueio de recuperação habilitado
- Roaming
- Status de Secure Apps
- Número de série
- Status
- Supervisionado
- Versões do sistema
- Versão do TPM
- Token de desbloqueio disponível (iOS)
- Registro do usuário habilitado
- Grupo de usuários
- Roaming de voz
- Chave de recuperação pessoal do macOS garantida
- Tipo de chave de recuperação do macOS

Procedimento

1. Clique em **Adicionar**.
2. Insira um nome para o grupo.
3. Insira uma descrição opcional para o grupo.
4. Selecione o tipo de grupo do dispositivo que você deseja criar:
   - **Gerenciado dinamicamente**: use regras para definir quais dispositivos estão no grupo.
   - **Gerenciado manualmente**: insira todos os usuários cujos dispositivos serão incluídos no grupo.
5. Para grupos gerenciados dinamicamente:
   a. Crie uma regra que defina o grupo.

      Exemplo: o sistema operacional é o iOS

   b. Clique em **+** para criar regras adicionais, se necessário.

      Por exemplo: dispositivo é iPhone 5S

   c. Clique em **Qualquer** se o dispositivo precisar corresponder com pelo menos uma das regras.

   d. Clique em **Todas** se o dispositivo precisar corresponder com todas as regras.
6. Para grupos gerenciados manualmente:
   a. Digite o nome de um usuário cujo dispositivo você deseja adicionar.

   b. Selecione o dispositivo a partir da lista exibida.

   c. Repita os passos a e b até que todos os dispositivos sejam exibidos na lista.
7. Clique em **Salvar**.

Remoção de um grupo de dispositivos

Procedimento

1. Acesse **Dispositivos** > **Grupos de dispositivos**.
2. Clique na caixa de seleção do grupo de dispositivos que você deseja remover.
3. Clique em **Excluir grupo de dispositivos**.

Exportar dispositivos para um arquivo CSV

Você pode exportar os detalhes de um grupo de dispositivos específico usando a opção **Exportar para CSV** da página **Grupos de Dispositivos**.

Procedimento

1. Acesse **Dispositivos** > **Grupos de dispositivos**.
2. Selecione todos ou vários espaços para ver as informações relativas a espaços específicos.
3. Clique no link de contagem do grupo de dispositivos. A página com a lista de dispositivos relativa ao espaço selecionado é exibida.
4. Clique na opção **Exportar para CSV** para exportar a lista de dispositivos e os detalhes relacionados para um arquivo CSV. Uma mensagem pop-up aparece informando que o relatório de exportação pode levar algum tempo para ser processado. Aguarde a conclusão da solicitação antes de enviar outra.
5. Clique em **Baixar**. Você receberá um e-mail contendo um link para baixar o relatório.
6. (Opcional) Clique em **Excluir** para excluir o relatório.

Se você não conseguir visualizar a página **Grupos de dispositivos**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Dispositivos não gerenciados

Esta seção contém os seguintes tópicos:

Licença: Silver

Se você configurou o controle de acesso ao e-mail do Sentry, os dispositivos não registrados que acessarem seu sistema de e-mail serão chamados de dispositivos não gerenciados. Você define se os dispositivos não gerenciados terão acesso ao e-mail por padrão ao configurar o Sentry. Você poderá permitir ou bloquear manualmente o acesso ao e-mail para esses dispositivos.

A página Dispositivos não gerenciados é atualizada a cada 5 minutos. Entretanto, as alterações no gerenciamento não são refletidas imediatamente.

Bloquear dispositivos

Procedimento

1. Selecione o dispositivo.
2. Selecione **Ações > Bloquear**.

O dispositivo permanece bloqueado até que você selecione **Ações > Permitir** ou **Ações > Excluir**.

Desbloquear dispositivos

Procedimento

1. Selecione o dispositivo.
2. Selecione **Ações > Permitir.**

O dispositivo continua a ter acesso ao e-mail até que você selecione **Ações > Bloquear** ou **Ações > Excluir**.

Remover dispositivo da lista de dispositivos

Procedimento

1. Selecione o dispositivo.
2. Selecione **Ações > Excluir**.

Na próxima vez que você tentar acessar o sistema de e-mail, ele será exibido novamente nessa lista e você deverá repetir a ação Bloquear ou Permitir aplicada anteriormente ao dispositivo.

Inventário de aplicativos

Esta seção contém os seguintes tópicos:

O inventário de aplicativos é a lista de apps detectados em dispositivos registrados.Como administrador, você pode usar essa página para obter informações sobre os apps sendo utilizados pelos dispositivos registrados. Você pode responder a perguntas, como:

- Qual aplicativo é o mais popular?
- Os dispositivos iOS obtêm seus apps diretamente da App Store?
- Quantos usuários Android baixaram um **aplicativo interno**[1] opcional?
- Quantos dispositivos estão utilizando uma versão desatualizada de um aplicativo?

Filtrando a exibição de apps

Todos os aplicativos são listados quando você exibe a página **Dispositivos > Inventário de aplicativo**. Use os filtros (painel esquerdo) para limitar essa lista para alguns apps. Por exemplo, para reduzir a lista para exibir somente os aplicativos privados do Google Play, selecione **Privado** na seção **Origem**.

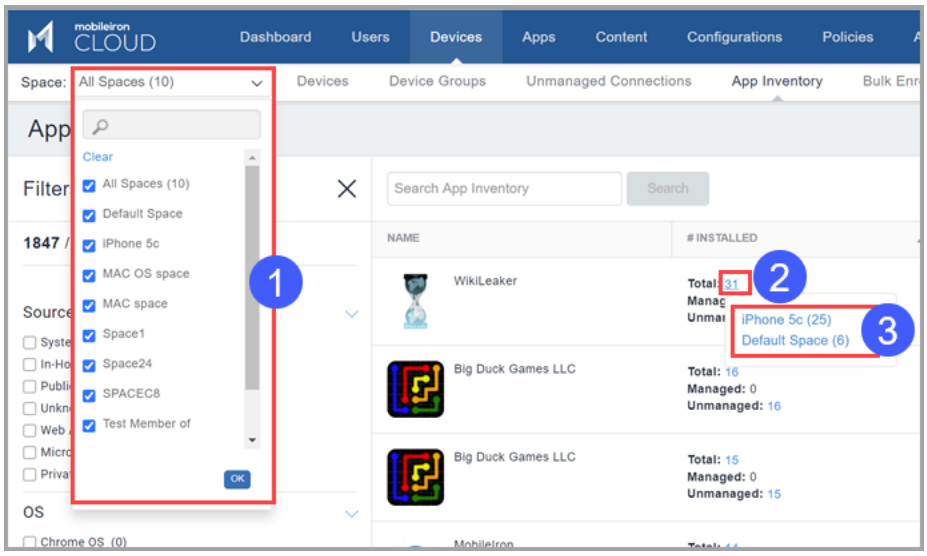
Para visualizar o inventário de aplicativo em todos os dispositivos ou em dispositivos de múltiplo espaço, selecione múltiplos espaços na lista suspensa. Quando você passa o ponteiro do mouse sobre os aplicativos, as contagens do dispositivo são exibidas. Clique na contagem de um aplicativo para exibir todos os dispositivos que contêm esse aplicativo. Cada registro de inventário de aplicativo será agrupado por espaço.

---

[1]an app distributed by the device management service rather than downloaded from a public app store.

Você pode pesquisar usando o nome do aplicativo ou o ID do lote/pacote.

Se você 1 selecionou diversos espaços, então 2 ao passar o cursor sobre o valor **Total** na coluna **# Instalado** exibirá o número de instalações por espaço de dispositivo 3.



Exibindo os dispositivos instalados para um aplicativo

Clique no número **Gerenciado**, **Não gerenciado** ou **Todos** listados na coluna **Nº instalado**.

Exibindo a lista de apps

Clique em **Número solicitado** em relação ao aplicativo no inventário para visualizar os dispositivos que o solicitaram. Vale apenas para dispositivos Apenas MAM.

Exibindo os apps Win32 instalados em um dispositivo

O inventário de aplicativos exibirá os apps Win32 em um dispositivo se a configuração de privacidade para esse dispositivo permitir a coleta de informações de todos os apps que estão nele. Você pode configurar a política de privacidade do dispositivo.

Procedimento

1. Determine qual configuração de privacidade se aplica ao dispositivo desejado seguindo as instruções em Dispositivos.
2. Vá até **Configurações**.
3. Para a configuração de privacidade observada na etapa 1:
    a. Selecione a configuração.
    b. Clique em Editar.
    c. Em **Coletar Inventário de aplicativos**, selecione **Para todos os aplicativos no dispositivo**.
    d. Clique em **Concluído**.

Criando permissão de exibição personalizada

Você pode especificar permissões de exibição personalizadas para usuários.

Procedimento

1. Acesse **Administrador**.
2. **Gerenciamento de funções**.
3. Clique em **Adicionar função personalizada**.
4. Selecione a opção **Função específica do espaço**.
5. Insira o nome de usuário no campo **Nome**.
6. No menu **Dispositivos**, clique em **Inventário de aplicativos**.
7. Marque a caixa de seleção **Exibição**.
8. No menu **Dispositivos**, clique em **Ações do dispositivo**.
9. Clique em **Salvar**.
10. Acesse **Usuários** no menu principal.
11. Clique no novo usuário que você criou.
12. Clique em **Atribuir funções**.
13. Marque a caixa de seleção **aplicativo | Específico do espaço**, clique em **Avançar**.

14. A página **Resumo** exibe as permissões que foram atribuídas à função que você criou.
15. Clique em **Concluído**.
16. Faça login como o novo usuário.
17. Clique em **Dispositivos** no menu principal.
18. Clique em **Inventário de aplicativos**.
19. A página **Inventário de aplicativos** agora exibe apenas os aplicativos permitidos para o usuário.

Exportando um inventário de aplicativos

Como administrador, você pode solicitar relatórios de inventário de aplicativos usando a opção **Exportar para CSV** .

Procedimento

1. Acesse **Dispositivos > Inventário de Aplicativos**.
2. Selecione um inventário na lista.
3. Clique em **Exportar para CSV.**

O administrador será avisado com um pop-up informando que o relatório de exportação levará algum tempo para ser processado. Após enviar a solicitação, o administrador deve aguardar a conclusão dela para enviar outra solicitação. Quando o relatório estiver pronto, o administrador receberá uma mensagem para Baixar ou Excluir o relatório que foi gerado. O administrador também receberá um e-mail contendo um link para baixar o relatório.

Se você não conseguir visualizar a página **Inventário de apps,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Gerenciamento de dispositivos

Esta seção contém os seguintes tópicos:

Implantando dispositivos Windows

Esta seção contém os seguintes tópicos:

Visão geral

O Ivanti Neurons for MDM ajuda você a gerenciar todos os laptops e desktops Windows, incluindo o gerenciamento do ciclo de vida de dispositivos HoloLens 2: desde configuração, registro, provisionamento, proteção, aplicativos, gerenciamento, monitoramento, atualizações de software e SO até a desativação.

Gerenciamento de dispositivos

Dispositivos Windows compatíveis:

- PC Windows 10+
- Microsoft HoleLens 2

Para mais informações sobre Gerenciamento de Dispositivos e a funcionalidade de relatórios, consulte "Dispositivos" na página 182

Inscrição e registro de dispositivos Windows

Ivanti Neurons for MDM suporta todos os métodos convencionais de registro para dispositivos Windows:

- Registro manual
- Inscrição em massa
- via SCCM e Ivanti EPM
- Piloto automático do Windows
- Registro do AAD

Para mais informações sobre os métodos de registro, consulte "Usando o Microsoft Azure" na página 1337

Para obter informações sobre suporte multiusuário, consulte "Suporte multiusuário para dispositivos Windows" na página 1339.

Gerenciamento de atualizações do Windows

- Configurando e agendando atualizações do Windows - para configurar e agendar atualizações do Windows, crie uma configuração usando Configuração - "Atualizações de software" na página 728.
- Gerenciamento de Atualizações do Windows - você pode ver e aprovar as atualizações relatadas pelos dispositivos Windows 10 que deseja atualizar usando o Gerenciamento de Atualizações do Windows 10. Ao usar esse recurso, você pode evitar que atualizações desnecessárias ou não testadas sejam instaladas nos dispositivos. Para mais informações, consulte "Gerenciamento de atualização do Windows 10" na página 1068.

Gerenciamento e distribuição de aplicativos

Os usuários podem gerenciar o ciclo de vida completo (importação, configuração, agendamento, distribuição, atualização e remoção) de aplicativos do Windows.

Tipos de aplicativos suportados:

- Interno
- MSB
- Loja pública

Extensões de aplicativo suportadas:

- MSI
- MSIX

- APPX
- Pacotes APPX
- EXE (Bridge)

Para mais detalhes sobre como gerenciar aplicativos Windows, consulte "Configuração do aplicativo" na página 354. Para automatizar atualizações de aplicativos, consulte "Programação de aplicativo do Windows" na página 1071 e "Trabalhando com configurações" na página 445.

Controle de aplicativo

A configuração Controle do aplicativo permite que você classifique apps como Lista de permitidos ou Lista de bloqueados no nível do dispositivo. Os apps já instalados não estarão visíveis e não poderão ser executados. Os apps ainda estarão visíveis na App Store, mas não poderão ser baixados ou iniciados. Todo dispositivo para o qual a configuração Controle de Aplicativo seja distribuída usará essa configuração e ignorará as definições da Política de Aplicativos Permitidos. A configuração Controle de Aplicativo substitui qualquer política relacionada ao mesmo aplicativo nos dispositivos de destino.

Para mais informações, consulte "Configuração de controle do aplicativo: Controle os apps que serão instalados por dispositivo" na página 470.

Configurações de gerenciamento de dispositivos do Windows

O suporte para PC Windows 10 e Microsoft HoloLens 2 inclui os seguintes recursos:

- "Registro do dispositivo (Windows 10+ PC e Microsoft HoloLens 2)" na página 226
- " Configuração da senha" na página 709
- " Configuração do Exchange" na página 814
- "Configurações" na página 444
- "Dispositivos" na página 182
- "Aplicativos" na página 300
- "Programação de aplicativo do Windows" na página 1071
- "Configuração de controle do aplicativo: Controle os apps que serão instalados por dispositivo" na página 470
- "Gerenciamento de atualização do Windows 10" na página 1068

- "Relatório de status de dispositivo do Ivanti Neurons for MDM para o Azure" na página 1367
- "Configuração de perfis do Windows Autopilot" na página 1324
- "Envio de SyncML aos dispositivos usando configurações personalizadas" na página 462
- "Políticas" na página 1099
- Restrições do Windows
- Certificados de identidade
- Windows Hello para Empresas
- Perfis de Wi-Fi e VPN

As configurações distribuídas a dispositivos HoloLens que não sejam compatíveis com esse tipo de dispositivo não serão relatadas como configurações distribuídas na guia Configurações, nos Detalhes do Dispositivo.

Recursos do Windows (compatíveis apenas com PC Windows):

- "Ivanti Bridge" na página 429
- "Configuração da BIOS do Windows" na página 1073
- "BitLocker do Windows" na página 1088
- "Configuração do quiosque do Windows" na página 1089
- "Configuração de licença do Windows" na página 1097
- "Configuração de integração do servidor EMA" na página 1028
- "Configurações da impressora" na página 1044
- "Configuração remover bloatware" na página 1049
- "Navegador ADMX (GPO)" na página 1333

Conformidade de dispositivos Windows

O Ivanti Neurons for MDM pode ser configurado em conjunto com o Microsoft Azure para a inscrição integrada dos usuários em seus tablets e desktops que rodem Windows 10+. Para configurar a integração do locatário do Azure a fim de habilitar a conformidade de dispositivos do Windows, consulte "Usando o Microsoft Azure" na página 1337.

Aplicativos do Windows e inventário de hardware

Inventário de Aplicativos do Windows

O inventário de aplicativos é a lista de apps detectados em dispositivos registrados. Use essa página para obter informações sobre os apps sendo utilizados pelos dispositivos registrados. Para mais informações, consulte "Inventário de aplicativos" na página 211.

O Inventário de Aplicativos exibirá os apps Win32 em um dispositivo se a configuração de privacidade para esse dispositivo permitir a coleta de informações de todos os apps que estão nele.

Configurando intervalos do inventário de aplicativos

Você pode definir intervalos de coleta de inventário de aplicativos do Windows 10 para vários inventários de tipos de fontes de aplicativos. Os intervalos são usados quando a configuração de privacidade está definida para coletar todos os aplicativos do dispositivo.

Para mais informações, consulte "Configurando intervalos de inventário de aplicativos" na página 1334.

Inventário de hardware do Windows

Você pode habilitar a coleta de informações de hardware em dispositivos Windows 10. Esses detalhes são recuperados usando o Bridge. Para mais informações, consulte "Inventário de hardware" na página 1335.

Configurar o Apple Remote Desktop em dispositivos macOS

Esta seção contém os seguintes tópicos:

Ativando o Apple Remote Desktop em dispositivos macOS

O recurso Apple Remote Desktop habilita o recurso de compartilhamento de tela e permite gerenciar os dispositivos remotamente. O recurso Apple Remote Desktop está disponível para dispositivos supervisionados com macOS 10.14.4+.

Procedimento

1. Acesse **Dispositivos** e selecione um ou mais dispositivos macOS supervisionados.
2. Clique em **Ações** > **Ativar área de trabalho remota** para os dispositivos.
3. Clique em **Ativar Remote Desktop** para confirmar.

Desativando o Apple Remote Desktop em dispositivos macOS

Procedimento

1. Acesse **Dispositivos** e selecione um ou mais dispositivos macOS supervisionados.
2. Clique em **Ações** > **Desativar área de trabalho remota** para os dispositivos. O recurso de compartilhamento de tela é desabilitado, e você não pode gerenciar remotamente os dispositivos.

Registro de dispositivo (iOS, macOS e Android)

Esta seção contém os seguintes tópicos:

A maioria dos usuários começa registrando um dispositivo. Você pode usar uma das seguintes abordagens para iniciar o processo de registro:

- Envie um convite para um ou mais usuários finais (registro iReg)
- Instrua os usuários finais a baixar o Go (registro no aplicativo)

O Ivanti Neurons for MDM oferece suporte a gerenciamento em nível de usuário de um único usuário (usuário local ou usuário registrado do Active Directory (AD)) em dispositivos macOS.Os administradores podem gerenciar dispositivos para os usuários, aplicar perfis de dispositivos e perfis de usuários e, consequentemente, usar o App Store, distribuição de aplicativo, configurações e políticas (incluindo o Apps@Work, restrições, segurança).

Para gerenciar dispositivos macOS com o usuário AD, o usuário AD precisa ser o usuário conectado durante o registro. Qualquer outro usuário não registrado não pode visualizar os perfis específicos do usuário registrado (por exemplo, certificações de identidade, VPN). No entanto, as configurações no nível do dispositivo podem ser visualizadas e usadas por qualquer usuário conectado.

Para poder iniciar o processo de registro do dispositivo, é necessário que o usuário final tenha uma conta no Ivanti Neurons for MDM. Para usuários LDAP, isso significa que devem estar configurados um Connector e um servidor LDAP, e o usuário deve ser importado do servidor LDAP. Para usuários locais, isso significa adicionar um usuário.

A URL de inscrição do dispositivo gerada nas versões anteriores do Ivanti Neurons for MDM deixará de funcionar com a versão atual. O administrador precisará gerar novamente a URL de inscrição do dispositivo para registrar o dispositivo.

Instalação manual do perfil de gerenciamento

Aplicável a:

- iOS 12.2 até a versão mais recente com suporte do Ivanti Neurons for MDM.
- macOS 11.0 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Registro de dispositivo iOS

Registro no aplicativo em dispositivos iOS:

- Durante o registro do dispositivo usando o Go app, aparece uma página com instruções para instalar o perfil.
- Clique na opção **Instalar perfil baixado** e clique em **Entendi**.
- O perfil baixado é válido por alguns minutos, depois disso, um novo registro será necessário.

Registro de dispositivo macOS

Para registrar um dispositivo macOS no portal de autoatendimento, o usuário deve seguir estas etapas:

Procedimento

1. Faça login usando as respectivas credenciais.
2. Na página Instalar perfil de gerenciamento, o perfil é baixado no sistema local do usuário.
3. Clique duas vezes no perfil baixado para torná-lo visível nas Preferências do sistema do usuário.

   O usuário tem um tempo limitado para instalar o perfil antes que ele se torne inválido.

4. Abra **Perfis** em Preferências do sistema. Quando o perfil é baixado no dispositivo, os usuários podem visualizar uma página da web que traz o link do perfil. Clique em **Perfis** para abrir o aplicativo Configurações.
5. Clique em **Instalar** para instalar o perfil de gerenciamento.
6. Prossiga e conclua o procedimento de instalação. Insira a senha do sistema quando ela for solicitada.

Envio de um convite (iOS, macOS e Android)

Inicie o processo de registro enviando um convite. Ivanti Neurons for MDM oferece as seguintes maneiras de enviar um convite aos usuários finais para que eles registrem um dispositivo:

- No Assistente de Inicialização
- Ao adicionar um ou mais usuários
- Na página Usuários (Ações > Enviar convite)

Se os usuários finais perderem o convite, você poderá compartilhar o URL listado nele. Certifique-se de adicionar **/go** no final do URL.

Usuários finais que tenham uma conta do Ivanti Neurons for MDM com senha não precisam de convite para iniciar o processo de registro. Você pode enviar a URL que está listada no convite.

Instrução dos usuários finais para baixar o aplicativo (iOS e Android)

O aplicativo Go está disponível para dispositivos Android e iOS. Você pode fornecer aos usuários finais instruções sobre como baixar o aplicativo de uma app store pública e iniciar o processo de registro no aplicativo. O convite por e-mail contém as seguintes informações:

- Um link para a página de registro
- Um PIN avulso (se definido pelo administrador)
- Instruções básicas para os próximos passos

Se você já definiu uma senha para a conta, pode enviá-la ao endereço de e-mail corporativo do usuário final. Se você estiver usando o LDAP para autenticação, informe ao usuário final que são necessárias credenciais de rede.

Se o usuário não concluir a instalação do perfil de MDM durante o registro, o Ivanti Neurons for MDM enviará notificações por push periódicas ao dispositivo solicitando que o usuário conclua o processo de registro.

O usuário pode usar o nome de usuário e a senha ou digitalizar o código QR para iniciar o registro do dispositivo no Go app. Os detalhes são os seguintes:

- **Nome de usuário**: endereço de e-mail
- **Senha**: se especificada em Configurações do Usuário e uma senha temporária estiver definida pelo administrador

- **Código QR**: gere o código QR no portal de autosserviço do Ivanti Neurons for MDM. Quando você tenta ler o código QR usando a opção **Escanear Código QR**, um prompt aparece na tela solicitando que você conceda permissão para acessar a câmera no dispositivo. Após você conceder a permissão, a câmera escaneará o código QR e o dispositivo será registrado. Essa opção é compatível com Android 9, iOS 14 e suas respectivas versões posteriores.

Como usuário final, se você receber um e-mail de registro em seu dispositivo móvel, toque no link para iniciar o processo de registro. Se você receber o e-mail em um laptop ou desktop, insira o URL em um navegador no seu dispositivo móvel para iniciar o processo de registro.

Se você ainda não tiver uma senha definida para sua conta de usuário do Ivanti Neurons for MDM ou suas Configurações de Usuário exigirem um PIN de registro, um PIN avulso será incluído. Após inserir o PIN, você deverá configurar a senha da conta, caso não tenha uma.

Para dispositivos Android Enterprise, quando o registro for concluído, qualquer certificado de CA instalado manualmente em um perfil de trabalho em dispositivo de propriedade da empresa ou dispositivo gerenciado de trabalho será desinstalado.

Registrando dispositivos Android novamente

O administrador pode registrar novamente um dispositivo usando as operações de desativação, apagamento ou exclusão, sem limpar manualmente a entrada ativa existente. Esse método é especialmente mais útil para novos registros em que a nova entrada e a entrada existente pertençam ao mesmo locatário. A página Dispositivos exibe o status do dispositivo no portal administrativo do Ivanti Neurons for MDM da seguinte forma:

- **Ativo** - o registro do dispositivo foi bem-sucedido
- **Desativado** - o dispositivo é redefinido, e o status desativado é exibido
- **Apagado** - o dispositivo é redefinido, e o status apagado é exibido
- **Redefinido** - o dispositivo é redefinido e fica em status ativo no servidor até o próximo registro

A página Trilhas de Auditoria lista os status de registro, reinscrição e desativação para dispositivos Android. Para mais informações, consulte "Trabalhando com widgets" na página 37.

Para Android 9.x e versões anteriores, uma única entrada será exibida após o novo registro. No caso do Android 10.x e versões posteriores, serão exibidas várias entradas. No entanto, apenas a entrada mais recente estará ativa; as entradas mais antigas estarão em estado desativado.

Registro do dispositivo (Windows 10+ PC e Microsoft HoloLens 2)

Esta seção contém os seguintes tópicos:

O processo de registro de dispositivo se dá por:

- Registro manual
  - Convite
  - Registro do usuário final
- Piloto automático do Windows
- Com SCCM e Ivanti EPM, por meio de inscrição de pacote de provisionamento com PIN. Consulte Inscrição de pacote de provisionamento com PIN.
- Inscrição em massa

Registro manual

A maioria dos usuários começa registrando um dispositivo. Você pode usar uma das seguintes abordagens para iniciar o processo de registro:

- Convite por e-mail
- Direcione os usuários para a URL da sua implementação

- Para poder iniciar o processo de registro do dispositivo, é necessário que o usuário final tenha uma conta no Ivanti Neurons for MDM. Para usuários LDAP, isso significa que devem estar configurados um Connector e um servidor LDAP, e o usuário deve ser importado do servidor LDAP. Para usuários locais, isso significa adicionar um usuário.
- A URL de inscrição do dispositivo gerada nas versões anteriores do Ivanti Neurons for MDM deixará de funcionar com a versão atual. O administrador precisará gerar novamente a URL de inscrição do dispositivo para registrar o dispositivo.

Como enviar um convite

Na maioria dos casos, você vai começar o processo de registro enviando um convite. O Ivanti Neurons for MDM oferece as seguintes maneiras de enviar um convite aos usuários finais para que eles registrem um dispositivo:

- No Assistente de Inicialização,
- ao adicionar um ou mais usuários
- na página Usuários (**Ações > Enviar convite**)

Se os usuários finais perderem o convite, receberem-no em um desktop ou laptop ou não o receberem por algum motivo, você pode enviar a URL listada no convite. Basta adicionar **\go** ao final do URL do seu serviço.

Usuários finais que tenham conta do Ivanti Neurons for MDM com senha configurada não precisam de convite para iniciar o processo de registro. Você pode enviar a URL listada em um convite.

Conclusão do processo de registro de usuários finais

Diga aos usuários do dispositivo como concluir o processo de registro. Você pode usar as instruções a seguir como modelo e fazer as alterações necessárias:

Procedimento

1. Abra um navegador em seu Windows 10+ PC.
2. Acesse mobileiron.com/go.
   Você será redirecionado para uma nova página, contendo uma URL de inscrição.
3. Copie a URL de inscrição na área de transferência.

4. Toque em **adicionar conta** na parte inferior da página **Configurações**.
5. Insira o endereço de e-mail associado ao convite que recebeu.

   Se o nome de usuário no Ivanti Neurons for MDM não for igual ao endereço de e-mail inserido no Ivanti Neurons for MDM, peça para o usuário inserir o nome de usuário quando lhe for solicitado o endereço de e-mail.

6. Cole a URL do servidor do Workplace que você copiou no campo de texto seguinte.
7. Toque em **entrar**.
8. Insira sua senha no campo seguinte.
9. Deixe os outros campos em branco.
10. Toque em **entrar**.
11. Clique em **concluído** na tela **CONTA ADICIONADA**.
    A tela inicial do Workplace mostra que uma conta foi adicionada.

Piloto automático do Windows

O Windows Autopilot é um recurso da Microsoft que ajuda os administradores a configurar e pré-configurar novos dispositivos para deixá-los prontos para uso. O recurso Autopilot ajuda com um provisionamento rápido, confiável e contínuo de dispositivos Windows Desktop ou HoloLens 2. Além disso, o recurso Autopilot ajuda a executar as seguintes tarefas:

- Unir dispositivos automaticamente ao Azure Active Directory (AAD)
- Registrar automaticamente dispositivos em serviços MDM
- Criar e atribuir automaticamente dispositivos para grupos de configuração com base no perfil do dispositivo
- Personalizar a experiência de registro
- Aplicar configurações e políticas
- Instalar aplicativos essenciais

Ivanti suporta todos os modos de perfil do Autopilot:

- Orientado pelo usuário
- Pré-provisionado orientado pelo usuário (previamente White Glove)
- Modo de autoimplementação

Para obter mais informações, consulte "Configuração de perfis do Windows Autopilot" na página 1324.

Para segurança e uso não autorizado do dispositivo, todos os dispositivos com Windows Autopilot podem ser travados para um locatário usando o recurso TenantLockdown CSP. Para usar este recurso, os dispositivos devem ser registrados utilizando a opção Autopilot. Essa configuração é aplicada no nível do dispositivo. Consulte "TenantLockdown CSP" na página 1332.

Registro padrão do AAD

Quando os usuários são adicionados ao locatário do AAD, podem registrar seus dispositivos diretamente por meio da conta de trabalho.

Procedimento

1. Em um dispositivo Windows, vá para **Configurações > Contas > Acessar trabalho ou escola**.
2. Selecione Adicionar conta corporativa ou de estudante e clique em **Conectar**.
3. Forneça o endereço de e-mail da sua conta de trabalho.

O dispositivo é inscrito automaticamente no Ivanti Neurons for MDM.

Provisionamento do registro do pacote com PIN

O administrador pode inscrever os dispositivos gerenciados pelo SCCM ou pelo Ivanti Endpoint Manager no Ivanti Neurons for MDM. A Ferramenta Pacote de Implantação permite que as organizações simplifiquem a transição de dispositivos Windows para o gerenciamento moderno do Ivanti Neurons for MDM, sem tempo de inatividade ou interrupção para o usuário final. A transição perfeita é alcançada fazendo o download de um pacote de implantação exclusivo a partir do Console do Ivanti Neurons for MDM e, em seguida, implantando-o por meio do domínio ou ferramenta de gerenciamento existente. Após a execução do pacote, ele registrará o ponto de extremidade no Ivanti Neurons for MDM de forma silenciosa para o gerenciamento vigente. A abordagem permite que os administradores primeiramente migrem os dispositivos facilmente e, depois, tenham a flexibilidade para configurar os dispositivos posteriormente over-the-air. Quando um dispositivo conclui o registro silencioso no Ivanti Neurons for MDM, ele é ingressado no MDM e gerenciado conjuntamente pelas duas autoridades de gerenciamento. Assim que o administrador tiver configurado a experiência desejada do Windows no Ivanti Neurons for MDM, a plataforma de gerenciamento legada pode ser encerrada, deixando o Ivanti Neurons for MDM como a única autoridade de gestão de dispositivos.

Há uma exceção a essa regra se o dispositivo estiver sendo transferido do Microsoft Endpoint Manager (MEM) ou do antigo SCCM. O MEM Client existente continuará a funcionar no Modo de coexistência (em oposição ao Modo de gerenciamento conjunto), até a plataforma MEM ser encerrada. Quando o Modo de coexistência está habilitado, o MEM Client desabilita automaticamente certas funcionalidades em favor do Ivanti Neurons for MDM que fornece essas cargas de trabalho. Para mais informações, consulte Documentação de coexistência da Microsoft.

Para comportamentos mais exatos ao usar MEM e outras plataformas de gerenciamento de terceiros, a Ivanti sugere primeiramente testar a Ferramenta Pacote de Implantação do Ivanti Neurons for MDM em seu ambiente.

Pré-requisitos

- As contas de usuário devem ser importadas no Ivanti Neurons for MDM usando LDAP, Azure AD (AAD), Upload de Usuário Local ou outras integrações de identidade
- Todos os dispositivos devem ter o Designer de Configuração do Windows instalado.
- Habilitar registro baseado em PIN no Ivanti Neurons for MDM
- Os usuários não devem ter espaços no nome de usuário; isso pode causar falha na transição do dispositivo do usuário.

- Essa ferramenta pode ser implantada em ambientes que não utilizem o AAD.
- Os principais elementos do Ivanti Neurons for MDM Modern Windows Management Suite não requerem o AAD. O cogerenciamento ou a coexistência podem exigir que determinadas cargas de trabalho/configurações sejam implantadas mediante registro silencioso, para evitar qualquer impacto durante a transição.
- Atualmente, o Pacote de Implantação é compatível apenas com SCCM e Ivanti Endpoint Manager.

Procedimento

1. Acesse **Administrador > Windows > Pacote de implantação**.
2. Selecione **Usuário** ou **Grupos de usuários** para gerar PINs e clique em **Baixar pacote de implantação** (arquivo .zip).
3. O pacote de implantação é fornecido aos administradores do SCCM/Ivanti Endpoint Manager para que o descompactem e transfiram os arquivos aos respectivos dispositivos gerenciados por eles. Para informações sobre como executar esta etapa, consulte Pacotes e programas no Configuration Manager.
4. Após a transferência, os administradores acionam remotamente o script `setup.ps1` nos dispositivos. Para informações sobre como acionar o script, consulte Criar e implantar scripts a partir do Configuration Manager.
5. Os dispositivos são registrados no Ivanti Neurons for MDM.

- Os PINs gerados para os usuários são válidos somente por 24 horas. Quando o PIN expirar, um novo PIN precisará ser gerado.
- O arquivo que contém os PINs é excluído do dispositivo após a conclusão da tentativa de registro.

Inscrevendo dispositivos SCCM no Ivanti Neurons for MDM

Procedimento

1. Baixe do Ivanti Neurons for MDM todos os arquivos relacionados à implantação dos usuários selecionados.
2. Selecione as contas ou grupos que devem ser inscritos.

3. Implante os arquivos do pacote nos dispositivos cliente usando o SCCM:
    - Verifique se os clientes necessários estão presentes no SCCM. Se o designer de configuração do Windows não estiver presente no cliente, o administrador deve enviar o designer e implantá-lo no cliente.
    - No servidor SCCM, crie uma pasta, copie o arquivo zip de implantação e extraia o conteúdo do arquivo.
    - Crie um arquivo .bat que copiará o conteúdo da pasta de extração dos arquivos para o dispositivo cliente.
    - No SCCM, vá para **Biblioteca de software > Gerenciamento de aplicativos > Pacotes** e crie um pacote para copiar o conteúdo da pasta para o cliente. Insira a pasta de destino para a qual deseja copiar o conteúdo.
    - Implante o pacote no dispositivo ou no local do dispositivo.
    - Na seção Monitoramento, você pode monitorar o status da implantação e confirmar se os arquivos foram copiados para a pasta de destino no cliente.
4. Execute o script para inscrever um dispositivo:
    - Vá para **Biblioteca de software > Scripts** e crie o script.
    - Insira um nome para o script e importe o script do PowerShell **setup.ps1** da pasta descompactada.
    - Aprove o script e execute-o no dispositivo de destino.
    - Selecione **Iniciar agora** e clique em **Salvar**. As tarefas agendadas começam a executar o script. Se a execução for bem-sucedida, o status ficará Verde.
5. Para verificar a inscrição do dispositivo, **Configurações** > **Adicionar ou remover um pacote de provisionamento** > **Detalhes**.

Inscrevendo dispositivos do Ivanti Endpoint Manager no Ivanti Neurons for MDM

Procedimento

1. Baixe do Ivanti Neurons for MDM todos os arquivos relacionados à implantação dos usuários selecionados.
2. Selecione as contas ou grupos que devem ser inscritos.

Caso 1: um nome de dispositivo é considerado para inscrever o dispositivo com o mesmo nome de usuário - nesse caso, o endereço de e-mail não é um endereço de e-mail de usuário válido. Um e-mail com o nome do dispositivo concatenado com o domínio do AD é considerado o endereço de e-mail de inscrição. O administrador deve definir Conta como LocalSystemAccount e usar setup.ps1 como arquivo principal para iniciar a execução do PowerShell.

Caso 2: um endereço de e-mail de usuário válido é considerado para inscrever o dispositivo e não há restrições para modificar arquivos no local do dispositivo - use o endereço de e-mail do usuário conectado para inscrever. Para habilitar essa inscrição, o administrador deve definir Conta como Conta de usuário atual e usar setup.ps1 como arquivo principal para iniciar a execução do PowerShell.

Caso 3: um endereço de e-mail válido é considerado para inscrever o dispositivo, e há restrições para modificar arquivos no local do dispositivo - use o endereço de e-mail do usuário conectado na inscrição. Este caso tem dois subcasos:

- Usando dois scripts para inscrição - crie um pacote de distribuição com **setupEPMCopyContentsToTempFolderStep1.ps1** e execute como Conta de usuário atual. Os arquivos são copiados para um local temporário. Crie outro pacote de distribuição com **setupEPMCopyContentsToTempFolderStep2.ps1** e execute como Conta Sistema Local.

  Caso o usuário do dispositivo tenha restrições para modificar a pasta que contém os arquivos do pacote - copie os arquivos para uma pasta temporária, verifique o ID do usuário e crie um pacote do PowerShell. O pacote do PowerShell é executado pelo script **setupEPMCopyContentsToTempFolderStep2.ps1**. Após a instalação, a pasta temporária será excluída.

- Habilitar/dasabilitar UAC

  a. Atualize a entrada do registro para desabilitar o controle UAC e reinicialize a máquina

  b. Execute o pacote do PowerShell como Conta de usuário atual e usando setup.ps1

  c. Atualize a entrada do registro para habilitar o controle UAC e reinicialize a máquina

3. Crie o pacote do PowerShell:
    - Verifique se os clientes necessários estão presentes no Endpoint Manager.
    - Copie os arquivos para C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\. Crie uma subpasta dentro dessa pasta e extraia os arquivos.
    - Criar pacote: **Distribuição > Pacotes de distribuição > Novo > Windows > PowerShell**.

      O administrador pode distribuir os pacotes a diferentes dispositivos com base no nível de restrições definido nos dispositivos.

    - Na seção Arquivo primário, insira o nome do pacote e carregue setup.ps1 da pasta que contém os arquivos copiados
    - Na seção Arquivos adicionais, copie os arquivos restantes (exceto o script setup.ps1) usando **Adicionar**.
    - Na seção Contas, selecione Conta do usuário atual.
    - Clique em **Salvar**.
4. Criar tarefa agendada:
    - Selecione o pacote criado, clique com o botão direito e selecione **Criar tarefa(s) agendada(s)**. Uma tarefa agendada é criada.
    - Arraste o dispositivo e adicione-o à seção do pacote agendado.
    - No pacote agendado, clique com o botão direito e selecione **Propriedades**.
    - Verifique o pacote.
    - Em Tipo de tarefa, selecione **Enviar por push**.
    - Selecione **Iniciar agora** e clique em **Salvar**. As tarefas agendadas começam a executar o script. Se a execução for bem-sucedida, o status ficará Verde.
5. Para verificar a inscrição do dispositivo, **Configurações** > **Adicionar ou remover um pacote de provisionamento** > **Detalhes**. Como alternativa, o administrador pode verificar a inscrição nos Logs de Diagnóstico do dispositivo.

Como usar o registro em massa para dispositivos Windows

O recurso de registro em massa permite que você registre rapidamente vários dispositivos Android no Ivanti Neurons for MDM.

Pré-requisitos:

- As contas de usuário devem ser importadas no Ivanti Neurons for MDM usando a Conta Premium do Azure AD (AAD).
- Todos os dispositivos devem ter o Designer de Configuração do Windows instalado.

Procedimento:

1. Vincule os locatários do Ivanti Neurons for MDM e do AAD. Consulte Conectando o AAD ao UEM para dispositivos Windows 10.
2. Abra o aplicativo **Designer de Configuração do Windows** e selecione **Provisionar dispositivos de área de trabalho**. A janela Novo projeto aparece na tela.
3. Insira os seguintes detalhes:
   - Nome - um nome exclusivo para o seu projeto
   - Pasta do projeto - local em que você deseja salvar o projeto no dispositivo
   - Descrição - descrição opcional do projeto
4. Clique em **Concluir** para fechar a nova janela de projeto e executar uma sequência de etapas.

   Configurar dispositivo

5. Insira um nome exclusivo para seus dispositivos. O nome pode incluir um número de série (%SERIAL%) ou um conjunto aleatório de caracteres.
6. Opcionalmente, você pode inserir uma chave de produto se estiver atualizando o Windows, configurando o dispositivo para uso compartilhado ou removendo software pré-instalado.

   Configurar rede

7. Opcionalmente, você pode configurar os dispositivos de rede Wi-Fi aos quais se conectar na primeira inicialização. Se os dispositivos de rede não estiverem configurados, será necessária uma conexão de rede com fio quando o dispositivo for iniciado pela primeira vez.

   Gerenciamento de contas

8. Selecione **Registrar no Azure AD**, insira a data de **Vencimento do Token em Massa** e clique em **Obter Token em Massa**.
9. Insira suas credenciais do Azure AD para obter um token em massa.
10. Na página **Permanecer conectado a todos os apps**, clique em **Não, conectar apenas a esse app**.
    - Clique em Avançar quando o token em massa for obtido com sucesso e crie o pacote.
    - Um usuário com pacote de provisionamento é criado no portal do Azure - nome principal do usuário (como package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com). Copie o arquivo (ferramenta ppkg de tempo de execução) para um dispositivo de armazenamento.

    > O usuário do AAD para criar o token em massa e o usuário do pacote não devem estar com a MFA habilitada. Para verificar, você precisa realizar a associação OOBE + AAD nesse usuário.

11. Recrie ou sincronize o usuário do pacote (criado no Azure) com o Ivanti Neurons for MDM.

Registre em massa um dispositivo com uma unidade flash contendo o pacote de provisionamento. Você também pode clicar duas vezes no dispositivo existente para realizar a experiência pós-OOBE. Se o pacote não for instalado na primeira tentativa, a segunda tentativa também falhará. Verifique se o novo dispositivo foi criado no Ivanti Neurons for MDM e se o AAD pertence ao usuário do pacote.

Como alterar as configurações de senha

Esta seção contém os seguintes tópicos:

- "Alteração da configuração de senha atribuída" abaixo
- "Atribuir uma configuração de senha diferente" abaixo

Use a Configuração de senha atribuída a um dispositivo para alterar as configurações de senha.Você também pode:

- alterar as configurações para a configuração atribuída

  OU

- atribuir uma configuração de senha diferente

As alterações feitas na configuração afetarão todos os dispositivos aos quais ela está atribuída.

Alteração da configuração de senha atribuída

Procedimento

1. Acesse **Dispositivos**.
2. Encontre a entrada para o dispositivo na lista.
3. Clique no link na coluna **Nome**.

   Se a configuração da senha estiver atribuída, ela será exibida na guia Configurações.

4. Na guia Configurações, clique no link **Configuração da senha**.
5. Clique em **Editar** (canto superior direito).
6. Faça as alterações.

Atribuir uma configuração de senha diferente

Procedimento

1. Verifique se alguém criou a configuração necessária.
2. Acesse **Dispositivos**.
3. Encontre a entrada para o dispositivo na lista.
4. Clique no link na coluna **Nome**.

Como alternar o nome do dispositivo

Administradores podem manualmente alterar o nome de um dispositivo (sem usar a configuração Editar nome do dispositivo).

Aplicável a:

- Dispositivos iOS supervisionados
- Dispositivos macOS 10.10+

Procedimento

1. Acesse **Dispositivos**.
2. Encontre a entrada para o dispositivo na lista.
3. Execute uma das seguintes etapas:
    - Adicione a coluna **Nome do dispositivo** se ela não estiver adicionada ao clicar no ícone de engrenagem Configurações à direita e selecionar **Nome do dispositivo**.
    - Clique no link na coluna **Nome** para acessar a página de detalhes do dispositivo.
4. Ao lado de **Nome do dispositivo**, clique no ícone de lápis Editar.
5. Insira um novo nome para o dispositivo e clique no ícone de tique.
6. Na caixa de exibição Substituir nome do dispositivo, leia as observações e clique em **OK**.

O nome alterado será enviado ao dispositivo na próxima vez que ele fizer check-in. Essa ação não poderá ser desfeita.

Se a configuração do Nome do dispositivo padrão tiver sido configurada anteriormente, esta ação substituirá o nome definido na configuração.

Localizar e filtrar dispositivos

Esta seção contém os seguintes tópicos:

Localizando um dispositivo

O portal administrativo do Ivanti Neurons for MDM exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo Nome do grupo de usuários é selecionado no Criador de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

Procedimento

1. Acesse **Dispositivos**.
2. Digite o nome do dispositivo no campo **Pesquisar**. São listados todos os dispositivos que contenham os caracteres.

Filtrando dispositivos

A barra de navegação lateral Filtros apresenta várias seções que ajudam a pesquisar um dispositivo específico na lista de dispositivos. O assistente Gerenciar Filtros contém a lista de todas as seções que você pode selecionar para exibição na barra de navegação Filtros.

Procedimento

1. Acesse **Dispositivos**.
2. Clique nas caixas de seleção relevantes das seções presentes na barra de navegação lateral Filtros. **Por exemplo**:

- Na seção **Usuário ativado**, selecione **Sim** para exibir somente os dispositivos nos quais os usuários estão com status ativado.
- Se você atribuiu atributos personalizados aos dispositivos, poderá filtrar os dispositivos com base nesses atributos clicando no ícone de configurações (engrenagem).
- Na seção **Status**, selecione **Desativado** e **iOS** para exibir somente dispositivos desativados com iOS.

3. (Opcional) Clique em **Restaurar padrões** para retornar a seleção aos filtros predefinidos. A barra de navegação Filtros exibe as seções selecionadas. Se você desmarcar todas as caixas de seleção do assistente Gerenciar Filtros, a barra de navegação lateral Filtros exibirá todas as seções.
4. Clique em qualquer lugar fora do assistente Gerenciar Filtros para sair do assistente.
5. (Opcional) Clique no ícone X para fechar a barra de navegação lateral Filtros e clique em **Filtros** para reabri-la.

- Se você usar alguma das palavras irrelevantes listadas no arquivo stopwords.txt, que faz parte da configuração do servidor Apache SOLR, as palavras não serão indexadas e, consequentemente, as entidades que contenham as palavras irrelevantes não serão exibidas nos resultados da pesquisa.
- Exemplos de entidades: dispositivos, usuários, grupos, atributos, aplicativos, certificados, trilhas de auditoria, conteúdos e módulos de notificação.
- Exemplos de palavras irrelevantes: um, uma, se, estar, em e assim por diante.

Usando a pesquisa avançada

Você pode usar a opção Pesquisa avançada para pesquisar um dispositivo com base em regras para identificar e visualizar os dispositivos com critérios específicos. As regras podem ser criadas usando os operadores aplicáveis, incluindo os operadores "começa com", "termina com", "contém", "não contém", "não começa com", "não termina com", "é menor que", "é maior que", "está no intervalo", "é igual a" e "é diferente de". As opções de regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). Os dispositivos que correspondem às regras são exibidos abaixo da seção.

O portal administrativo do Ivanti Neurons for MDM exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo Nome do grupo de usuários é selecionado no Criador de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

Procedimento

1. Na página de Dispositivos, clique no link **Pesquisa avançada**. O assistente Pesquisa Avançada é exibido.
2. Clique em uma das opções a seguir:
   - **Qualquer**: o dispositivo precisa atender a pelo menos uma das regras
   - **Todas**: o dispositivo precisa atender a todas as regras
3. Crie uma regra que defina os critérios de busca. **Exemplo**: Capacidade APNS igual a Sim.
4. (Opcional) Clique em **+** para criar regras adicionais.
5. Clique em **Pesquisar**. A lista dos dispositivos que correspondem aos critérios de pesquisa é exibida.

- Para dispositivos iOS 14.0+, o ID eSIM (EID) está disponível na página de detalhes do dispositivo. O ID eSIM (EID) permite às operadoras atribuir o SIM a um dispositivo específico. O campo ID eSIM (EID) é compatível com a RGPD.
- À medida que novos campos da RGPD (como Endereço IP e ID eSIM) são adicionados às versões do Ivanti Neurons for MDM, os administradores que já configuraram a RGPD precisam editar o perfil de RGPD caso desejem ocultar os novos campos.
- A Pesquisa avançada mostra o status do bloqueio de recuperação de um dispositivo.

Carregando as consultas de pesquisa

Você pode visualizar a lista das consultas de pesquisa salvas.

Procedimento

1. Clique em Pesquisa avançada e, em seguida, clique no ícone da pasta. A lista das consultas de pesquisa criadas é exibida na seção **Consulta carregada**, e os seguintes detalhes são exibidos.
   - **Nome da consulta** - O nome da consulta carregada.
   - **Conteúdo da consulta** - Exibe o conteúdo sobre as regras que definem a consulta de pesquisa.
   - **Ações** - Selecione a ação a ser executada na consulta.
2. Clique em **Carregar consulta** na coluna **Ações** para exibir a lista de dispositivos que correspondem aos critérios definidos na consulta carregada.
3. Clique em **Excluir** para excluir uma consulta carregada.

Usando o Proprietário do dispositivo

Esta seção contém os seguintes tópicos:

Licença: Gold

Você pode designar os dispositivos como Propriedade da empresa ou Propriedade do funcionário após os dispositivos terem sido registrados. Essa designação ajuda a gerenciar políticas que estão baseadas em se um usuário possui um dispositivo pessoal ou um dispositivo de propriedade da empresa. Com a licença adequada, você poderá usar a propriedade em regras para a criação de grupos de dispositivos.

Ao iniciar um dispositivo novo ou redefinido com as configurações de fábrica, use o aplicativo Provisioner para fornecer o modo do proprietário do dispositivo usando uma das opções a seguir:

- Entrada NFC (Near Field Communication, Comunicação por campo próximo)
- Digitalização de código QR

Uma entrada NFC envolve utilizar o dispositivo principal ou modelo contra um dispositivo novo ou redefinido com as configurações de fábrica para configurá-lo.

Uma digitalização de código QR envolve tocar na tela de um dispositivo novo ou redefinido com as configurações de fábrica, configurar uma rede Wi-Fi e digitalizar o código quando o dispositivo estiver pronto para ser provisionado.

No provisionamento do modo de Proprietário do dispositivo usando NFC ou código QR, o aplicativo provisionador aceita um token de registro. No registro, o token de inscrição é enviado ao servidor. Se está presente no servidor e o dispositivo está atribuído a um usuário, o dispositivo foi registrado com sucesso.

O cliente Go controlará o dispositivo quando ele estiver no modo Proprietário do Dispositivo e bloqueará a tela até o dispositivo ser registrado no Ivanti Neurons for MDM para evitar que os usuários saiam do processo de provisionamento. O modo de proprietário dos dispositivos também é compatível com o modo de quiosque. Para informações sobre configuração, acesse: Configuração de bloqueio e quiosque.

Importante

- Se você aposentar um dispositivo no modo de Proprietário do dispositivo, o dispositivo será redefinido com as configurações de fábrica.
- Todos os dispositivos no modo de Proprietário do dispositivo podem, opcionalmente, ter todos os apps do sistema ativados.
- Um dispositivo pode ter somente um proprietário de dispositivo ativo por vez.
- Somente os dispositivos com capacidade para Android enterprise podem ser provisionados no modo de proprietário do dispositivo.
- Para dispositivos Samsung Knox Standard que estejam no modo Proprietário do Dispositivo, os usuários serão solicitados a ativar a licença Samsung ELM. Essa solicitação também aparece nos dispositivos Samsung que estão no modo Proprietário do Dispositivo quando o aplicativo Go client é atualizado de uma versão anterior para a versão mais recente compatível com o Ivanti Neurons for MDM. Após a ativação, o número de série é exibido na página Detalhes do dispositivo, que corresponderia com o campo Dispositivo > Configurações > Número de série.

Provisionando dispositivos Android Enterprise usando código QR ou entrada NFC

Para provisionar dispositivos de Android Enterprise usando código QR ou entrada NFC, é necessário fazer download e instalação do aplicativo Provisioner no Google Play no dispositivo principal.

Componentes compatíveis

Versão do Provisioner: 1.3.0.

O Provisioner é compatível com ou funciona com:

Item	Versão
Android SO (no dispositivo a ser provisionado)	• 5.0 ou versões mais recentes com suporte são exigidas, se usarem NFC. • 7.0 ou versões mais recentes com suporte são exigidas, se usarem código QR. O dispositivo deve ser compatível com Android enterprise.
Android SO (no dispositivo principal)	5.1 até a versão mais recente. O dispositivo precisa ter NFC para usar a entrada NFC. Não é necessário para código QR.
Produto de servidor UEM, habilitado para Android corporativo	Um dos seguintes: Ivanti Neurons for MDM ou Ivanti Neurons for MDM com permissão.
Aplicativo cliente do Android	A versão mais recente do aplicativo cliente é instalada automaticamente no dispositivo provisionado pelo Provisioner.

Pré-requisitos

Para provisionar um dispositivo de Android corporativo para que seja um dispositivo gerenciado de trabalho, você precisa:

- Garantir que a configuração necessária relacionada ao Android corporativo esteja definida e será aplicada ao dispositivo registrado.

  > A configuração padrão Android Enterprise: dispositivo gerenciado de trabalho deve estar ativada no dispositivo.

- Ativar o Android corporativo no servidor.

- Ter um dispositivo Android com o recurso NFC (apenas se NFC for usado) para atuar como dispositivo principal, com o aplicativo Provisioner instalado.
- Ter dispositivos compatíveis com Android corporativo para provisionar.

Para configurar o feixe Android para utilização com a entrada NFC:

Procedimento

1. Acesse **Configurações** no dispositivo.
2. Acesse **Redes > Redes sem fio**.
3. Na **seção Conectividade**, selecione **Compartilhar e conectar**.
4. Deslize o botão **NFC** para **Ativado**.
5. Deslize o botão **Feixe Android** para **Ativado**.

 As etapas para ativar o feixe Android e o NFC podem variar em diferentes dispositivos.

Provisionar dispositivos Android Enterprise para se tornarem dispositivos gerenciados de trabalho

Procedimento

1. Usando o dispositivo principal Android, faça download do aplicativo Provisioner no Google Play e instale-o.
2. Fornecedor de lançamento no dispositivo principal.
3. Selecione NFC ou código QR para o método de provisionamento.
4. Toque em **Aplicativo para provisionamento** e escolha o aplicativo cliente a ser instalado no dispositivo provisionado:

Selecione este aplicativo cliente:	Para registrar com este servidor UEM:
Ir	Ivanti Neurons for MDM
At Work UEM	Ivanti Neurons for MDM (com permissão)

5. Preencha os campos restantes no aplicativo Provisioner. Alguns campos podem ser preenchidos automaticamente se algum tipo de Wi-Fi suportado estiver presente. Os campos de Wi-Fi não serão mostrados se o código QR for selecionado. Use estas orientações:

Campo	Valor
Selecionar aplicativo para o fornecimento	Go ou At Work
Fuso horário	Insira o fuso horário a ser configurado no dispositivo
Local	Insira o local a ser configurado no dispositivo
Ativar todos os apps do sistema	Clique na caixa de seleção para ativar todos os apps do sistema
SSID de rede de Wi-Fi	Insira o SSID de Wi-Fi que o dispositivo de destino deve usar
Tipo de segurança Wi-Fi	Insira o tipo de segurança Wi-Fi
Senha Wi-Fi	Insira a senha do Wi-Fi
Inscrição em massa	O recurso de inscrição em massa é opcional. Para usar a inscrição em massa, é necessário um nome de host. Como opção, é possível inserir um nome de usuário e selecionar a opção de início rápido. Para ignorar o recurso de inscrição em massa, deixe estes campos em branco.

6. Toque em **Continuar**.

7. Se você selecionou **NFC**, toque em **Continuar**. A tela **Tocar dispositivos!** aparece no dispositivo principal. Continue com a seção **Entrada NFC** abaixo.

Se você selecionou **Código QR**, a tela **Escaneie este código QR!** aparece no dispositivo principal. Continue com a seção **Código QR** abaixo.

Use as etapas abaixo para entrada NFC

8. Confirme se o dispositivo de destino está exibindo a tela de Boas-vindas do Android.
9. Pressione o dispositivo principal contra o dispositivo de destino, traseira com traseira, para iniciar a transferência NFC. Se a transferência NFC for bem-sucedida, o dispositivo de destino poderá emitir um som e prosseguir com o download do aplicativo cliente. Se não for possível estabelecer uma conexão Wi-Fi, ou se o dispositivo não conseguir fazer download do aplicativo cliente, o dispositivo realizará uma redefinição para as configurações de fábrica automaticamente.
10. Se você ouvir o som ou vir uma tela que não seja a tela de Boas-vindas, você poderá desacoplar os dispositivos. Isso geralmente demora alguns segundos. Se o dispositivo não estiver criptografado, ele iniciará o processo de criptografia antes de continuar.

    Você pode continuar a provisionar outros dispositivos "encostando" os dispositivos no dispositivo principal. O dispositivo alvo deve estar mostrando a tela de boas-vindas, e o dispositivo principal deve estar mostrando a tela "Tocar dispositivos!".

Use as etapas abaixo para provisionamento por Código QR

11. Confirme se o dispositivo de destino está exibindo a tela de Boas-vindas do Android.
12. Toque em na tela de Boas-vindas do Android do dispositivo de destino 6 vezes no mesmo ponto da tela.
13. Você será solicitado a configurar uma rede Wi-Fi para que o assistente de configuração possa fazer download de um leitor de código QR no dispositivo de destino.
14. Após o download do leitor de código QR, a câmera é iniciada.
15. Segure o dispositivo de destino alguns centímetros acima do dispositivo principal até que o código QR seja digitalizado. O assistente de configuração prosseguirá com o download do aplicativo cliente. Se não conseguir fazer download do aplicativo cliente, ele realizará uma redefinição para as configurações de fábrica automaticamente.
16. Você pode continuar a provisionar outros dispositivos digitalizando o código QR no dispositivo principal. O dispositivo de destino deve ter uma câmera pronta para escanear, e o dispositivo mestre deve estar mostrando a tela "Escaneie este código QR!".

17. O código QR também pode ser exportado tocando no ícone Compartilhar. As opções oferecidas para exportação variam segundo o dispositivo.

Provisionando dispositivos Android Enterprise usando token do cliente

Você pode provisionar um dispositivo Android corporativo no modo Proprietário do Dispositivo usando um token de cliente com marca em vez de usar os métodos de entrada NFC ou código QR. Este método permite que você faça login em um dispositivo com um token, o que facilita uma instalação automática do Go ou At Work client e o provisionamento no modo de proprietário do dispositivo:

Tokens de clientes com marca são suportados em dispositivos provisionados com Contas gerenciadas do Google Play, usando Android 6 ou versões mais recentes com suporte. Para mais detalhes, consulte o guia de Desenvolvedores de UEM do Android. https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

Requisitos para usar este método:

- Você precisa estar inscrito em uma conta de Android corporativo.
- O dispositivo precisa ser compatível com Android corporativo.
- O dispositivo deve usar o Android 6 até a versão mais recente.
- Você precisa ter um dispositivo novo ou redefinido com as configurações de fábrica.

Configurar (para dispositivos executando Android 5.0+)

Procedimento

1. No portal doIvanti Neurons for MDM, acesse **Configurações**.
2. Clique em **+Adicionar**.
3. Selecione **Bloqueio e quiosque: configuração do Android enterprise**.

   A página **Criar bloqueio e quiosque: Configuração do Android enterprise** é exibida.
4. Insira um nome de configuração e uma descrição.

   Escolha um tipo de bloqueio.
5. Clique em **Dispositivos gerenciados de trabalho (Proprietário do dispositivo)**.

As opções de configuração de bloqueio do Proprietário do dispositivo Android serão exibidas.

Opcionalmente, escolha

- Desativar o WI-FI ou configurações WI-FI
- Desabilitar câmera
- Desabilitar Bluetooth
- Desabilitar configurações de Bluetooth
- Desabilitar captura de tela
- Silenciar volume principal
- Desabilitar o controle de apps
- Desabilitar credenciais
- Desabilitar transmissões de emergência
- Desabilitar redes móveis
- Desabilitar compartilhamento de internet
- Desabilitar VPN
- Desabilitar restaurar configurações de fábrica
- Ativar proteção de reinicialização para configurações de fábrica.

  Caso queira, você pode especificar uma lista de IDs de conta do Google autorizados (um valor inteiro) que podem provisionar o dispositivo depois da reinicialização para as configurações de fábrica, ou passar o mouse sobre o ícone de ajuda para ver como recuperar os IDs de conta autorizados.

- Proibir modificação de contas
- Desativar NFC (feixe de saída)
- Desabilitar realização de chamadas
- Desabilitar inicialização segura

- Desabilitar compartilhamento de localização
- Não permitir recursos de depuração
- Garantir verificação dos apps
- Desabilitar SMS
- Desabilitar a desativação do mudo do microfone
- Desabilitar ajuste de horário automático
- Desabilitar ajuste de fuso horário automático
- Desabilitar roaming de dados
- Desabilitar suspensão do Wi-Fi
- Restringir métodos de entrada
- Restringir serviços de acessibilidade
- Desativar transferência de arquivo por USB
- Desativar mídia externa
- Desativar proteção do teclado (sem efeito se o PIN/senha for definido)
- Mantenha a tela ligada enquanto estiver conectado à energia
- Não permitir a criação de janelas
- Ignorar as primeiras dicas de uso

6. Na seção**Ativar/desativar apps do sistema,** você pode escolher ativar para desativar os seguintes Apps do sistema:

Item	Versão
Redefinir apps do sistema	
Câmera integrada	Clique no botão de alternar para **ATIVAR** ou **DESATIVAR** o aplicativo da câmera integrada.
Telefone integrado	Clique no botão de alternar para **ATIVAR** ou **DESATIVAR** o aplicativo de telefone integrado.
Nome do pacote do aplicativo do sistema	Para ativar ou desativar qualquer outro aplicativo do sistema além dos aplicativos pré-definidos, clique no ícone + (mais) e adicione o nome do pacote do aplicativo do sistema. Para remover o aplicativo do sistema, clique no ícone - (menos).

Opcionalmente, escolha habilitar o **Modo de quiosque**.

As seguintes configurações serão exibidas:

- Ativar o modo de tarefa de bloqueio
- Inserir o Quiosque automaticamente (somente na configuração inicial)
- Desabilitar configurações rápidas
- Permitir acesso do usuário às configurações do Wi-Fi
- Permitir acesso do usuário às configurações do Bluetooth
- Permitir acesso do usuário às configurações de localização
- Permitir que o usuário atrase as atualizações do aplicativo
- Permitir que o usuário acesse as configurações de data e hora
- Permitir que o usuário acesse as configurações de rede móvel
- Permitir que o usuário selecione o idioma

- Ativar dispositivo compartilhado (selecione uma das opções a seguir)
  - Ativar login
  - Ativar logout (indique a configuração de tempo limite em horas)

7. Caso queira, selecione as opções de atribuição de marca personalizadas ou padrão na lista suspensa.
8. Como alternativa, crie um Pino de saída do quiosque usado para sair do Modo de quiosque.
9. Opcionalmente, crie uma lista de apps permitidos que estarão disponíveis para os usuários no modo de quiosque.

Provisionar o dispositivo

Procedimento

1. Ligue o dispositivo e insira a senha do Wi-Fi. O dispositivo pode solicitar uma senha diferente.
2. Na tela **Verifique sua conta**, insira seu token do Android enterprise. Clique em **Avançar**.
3. Na tela **Serviços do Google**, clique em **Instalar**.
4. Aceite os termos e condições.
5. Na tela Configurar dispositivo de trabalho, clique em **Avançar**. O Go ou At Work client é transferido e instalado no dispositivo. O dispositivo agora entra no modo Proprietário do dispositivo.

Tópicos relacionados

- Como usar o registro em massa para Android
- Grupos de dispositivos

Dispositivo gerenciado com Work Profile

Dispositivo gerenciado pelo Work Profile em dispositivo de propriedade da empresa é um modo em que o dispositivo Android Enterprise é de propriedade de uma empresa, com dados pessoais separados dos demais. Este modo permite ter dois perfis: um perfil gerenciado para implementação de aplicativos de trabalho e um pessoal para o usuário. O modo Dispositivo gerenciado pelo Work Profile em dispositivo de propriedade da empresa é criado distribuindo uma configuração de Dispositivo gerenciado com perfil de trabalho para um dispositivo que seja provisionado no modo de proprietário do dispositivo.

Para mais informações sobre as Configurações de bloqueio do Dispositivo gerenciado com Work Profile, consulte "Bloqueio e Quiosque: Android Enterprise" na página 620.

Este modo requer o Android 8.0 até a versão mais recente lançada.

É possível aplicar a Dispositivo gerenciado com Work Profile: configurações de app, widgets de compartilhamento de apps entre perfis, aliases de certificado de cliente e certificados de ID.

As configurações a seguir se aplicam a Dispositivo gerenciado com Work Profile:

- Senha avançada
- VPN Sempre Ativa
- Certificado
- Certificado de identidade
- Conta do Google
- Senha
- Restrição de telefone Samsung
- Defensa contra ameaças
- Wi-Fi
- Permissões padrão de tempo de execução do aplicativo
- Certificação SafetyNet

- Senha
- Ações locais de defesas contra ameaças

Como usar o registro em massa para Android

O recurso de registro em massa permite que você registre rapidamente vários dispositivos Android no Ivanti Neurons for MDM.

Licença: Silver

Execute as tarefas a seguir antes de usar o registro em massa:

1. Instale o Android SDK, que inclui o Android Debug Bridge (adb), no computador usado para registrar os dispositivos.
   Para obter mais informações sobre o Android Debug Bridge, consulte http://developer.android.com/tools/help/adb.html.
2. Ativar depuração USB.
   O procedimento para ativar a depuração USB em dispositivos Android varia dependendo da versão do Android. Consulte: http://developer.android.com/tools/device.html para obter informações sobre ativar a depuração USB.
3. Instale o Go client em cada dispositivo.
4. Conecte os dispositivos por cabo USB no computador provisionado que será usado para registrá-los.

O Go pode ser iniciado e registrado em um servidor usando o shell Android Debug Bridge (adb). O Android Debug Bridge é uma ferramenta que pode ser usada a partir da linha de comando do Windows ou no utilitário Terminal do iOS. Ele permite que você se comunique com um dispositivo Android conectado. A partir do shell do adb, o formato do comando é:

> adb shell

```
$ am start -a android.intent.action.MAIN -d
"mirp://na1.mobileiron.com?key=value&key=value" -n
com.mobileiron.anyware.android/com.mobileiron.polaris.manager.ui.StartActivity
```

O Protocolo de registro (**mirp**) é usado para codificar dados relevantes para registro.

As chaves e valores válidos são:

Chave	Valor
usuário	Endereço de e-mail do usuário que poderia ter sido digitado no campo nome de usuário se estivesse usando iReg. Requerido.
senha	Senha do usuário
pin	Pin de registro para
quickStart	**Quando definido como VERDADEIRO:** a tela inicial será exibida, mas não completa. Na tela de boas-vindas, quando o controle giratório mudar para o botão Continuar, a tela será movida automaticamente sem a necessidade de tocar em Continuar. Além disso, esse fluxo simplificado de provisionamento está presente em todos os dispositivos: • Os avisos de privacidade e de atalho para o usuário são ignorados. • On zebra devices, the client shall grant admin privileges to itself without a user prompt. Requer versão Zebra MX 4.3 ou mais recente. **Quando definido como FALSO:** a tela inicial será exibida normalmente e o usuário precisará tocar em Continuar na tela de Boas-vindas. Opcional, padrões para FALSO.

O uso de uma senha, pin ou token é necessário para usar o registro em massa.

Este comando de exemplo especifica um servidor, usuário, senha, PIN e iniciação rápida:

```
am start -a android.intent.action.MAIN -d
"mirp://ppp183.auto.mobileiron.com?user=miadmin@auto0001.mobileiron.com&passwo
rd=P@$$W0R3&pin=12345&quickStart=true" -
n com.mobileiron.anyware.android.qa/com.mobileiron.polaris.manager.ui.StartAct
ivity
```

Script de amostra do registro em massa

Você pode usar este script como um exemplo ao projetar seu próprio script de registro em massa. Este script de amostra registra todos os dispositivos anexados à máquina de provisionamento com o mesmo usuário e senha.

```
for i in `adb devices | grep -v devices |

do

 echo "Registrando $i"

    adb -s $i shell "am start -a android.intent.action.MAIN -d
\"mirp://<servername?user=user email addresspassword=password

done
```

Mensagens de erro em potencial

Aqui estão alguns erros potenciais que você poderá encontrar ao usar o registro em massa:

Erro	Resolução
esquema mirp não encontrado	Comando de exemplo de um esquema mirp: `am start -a android.intent.action.MAIN -d "xxxmirp://?`
A URL é inválida	Ocorre se nenhuma sequência de dados for enviada. Verifique se a URL está correta.
Nenhuma informação do servidor foi encontrada	Informações de servidor ausentes ou inseridas incorretamente.
Nenhuma informação de usuário encontrada	Verifique se a chave do usuário foi inserida.
Nenhuma informação de senha/PIN encontrada	Verifique se o pin OU a senha foram inseridos.

Registro em massa de dispositivos com upload de arquivo CSV

O registro em massa permite que você registre vários dispositivos Android usando identificadores de dispositivo. É possível carregar o arquivo CSV para adicionar dispositivos em massa.

Procedimento

1. Na página **Dispositivos**, clique na guia **Registro em massa**. A página **Registro em massa** é exibida.
2. Clique em **Adicionar**.
3. No campo de texto **Nome do perfil**, insira o nome do perfil. Opcionalmente, clique em **+Adicionar descrição** para fornecer uma descrição para o arquivo CSV.
4. Na seção **Carregar CSV**, clique em **Baixar modelo CSV** para baixar o modelo CSV. Usando o formato existente, é possível editar o arquivo para adicionar dispositivos.

   Permite até 200.000 linhas por vez no CSV de registro em massa.

5. Após editar e salvar o arquivo CSV, clique em **Carregar CSV** para carregar o arquivo CSV. Uma confirmação sobre o carregamento bem-sucedido é exibida.

   Linhas com informações inadequadas podem resultar em falha no upload do CSV. Cada registro deve incluir, pelo menos, o número de série e as informações do fabricante; ou o valor IMEI.

   Para remover o arquivo CSV adicionado, clique no ícone de 'menos'. Para escolher um arquivo CSV para carregar, clique no link **Escolher um arquivo diferente**.

6. Opcional: selecione **Atribuir atributos personalizados sem token** para registrar em massa todos os tipos de dispositivos sem gerar um token. Essa opção não está selecionada por padrão.

   O registro em massa sem token também pode ser aplicado quando o IMEI ou a combinação de número de série e fabricante (com ou sem atributos personalizados) é fornecido no arquivo CSV carregado. No entanto, o registro do dispositivo demanda que os valores de atributos carregados no arquivo CSV estejam corretos. A tabela a seguir explica os cenários resultantes, com base na combinação de valor de atributo inserida para registro em massa:

Cenário	**Valores de atributo inseridos**			**Status de registro do dispositivo**
	IMEI	**Número de série**	**Fabricante**	
1	Correto	Incorreto	Incorreto	O dispositivo está registrado
2	Incorreto	Correto	Correto	O dispositivo está registrado
3	Incorreto	Incorreto	Correto	O dispositivo não está registrado
4	Incorreto	Correto	Incorreto	O dispositivo não está registrado

   O nome do fabricante faz distinção entre maiúsculas e minúsculas.

7. No campo **Selecionar usuário**, há a opção de selecionar usuários.
   O token do registro é exibido na coluna Token do registro. Para atualizar o token de registro, clique em **Atualizar**.
   A data de expiração do token é exibido na coluna **Expiração do token**. Para estender o período de expiração do token, clique em **Estender**. No campo **Estender até**, insira o número de dias para estender o token.

   O número de dias especificado deve estar no intervalo de 7 a 99. A expiração padrão do token é de 7 dias.
   Essa página não será exibida se você tiver selecionado a opção **Atribuir atributos personalizados sem token**.

8. Clique em **Concluído**.

Após o carregamento, os seguintes detalhes do arquivo CSV carregado são exibidos em uma tabela na página **Perfis de Inscrição em Massa**.

Configuração	Descrição
Nome do perfil	O nome do perfil.
Descrição	Alguma descrição sobre o perfil.
Última modificação	A data mais recente de modificação feita no arquivo CSV.
TIPO	Algumas informações sobre o perfil. Por padrão, é definido como Automanutenção.
Número de dispositivos	O número de dispositivos no registro em massa.
Usuário associado	Nome do usuário associado. Clique no link **Modificar usuário** para modificar o usuário.
Ações	É possível realizar qualquer das seguintes ações: **Baixar inventário existente** - clique nesse botão para baixar detalhes de todos os dispositivos disponíveis no perfil. **Visualizar** – clique no link para visualizar os detalhes dos perfis carregados em massa para registro. **Editar** - clique nesse botão para editar os detalhes do perfil. Essa opção fica disponível apenas quando a opção de dispositivo único está selecionada. **Excluir** – clique no link para excluir perfil Na janela de confirmação, clique em **Sim** para confirmar a exclusão do perfil carregado.

O token gerado durante o carregamento do CSV deve ser usado para o registro. Inserir o token errado redireciona para o fluxo IReg normal em que o ID ou a senha devem ser inseridos.

Ações

Ao visualizar os perfis de inscrição em massa na seção de detalhes Visualizar Perfil, você pode executar outras tarefas na guia Ações, presente na página de detalhes Visualizar Perfil.

- **Adicionar mais dispositivos** - use esta opção para adicionar mais dispositivos a um perfil. Você precisa fornecer as informações relativas a **Número IMEI**, **Fabricante**, **Número de Série** e **Atributos Personalizados** e então clicar em **Salvar**.
- **Modificar configuração** - use esta opção para modificar uma configuração existente. Você pode adicionar **Chaves específicas da Ivanti**, fazer alterações em **Extras pré-definidos do sistema Android** ou **Chaves de sistema personalizadas do Android** e então clicar em **Atualizar**.
- **Gerar código QR** - use esta opção para gerar um código QR para inscrição em massa de perfis.
- **Atualizar token** - use esta opção para atualizar um token ou estender a validade de um token.
- **Excluir** - use esta opção para excluir dispositivos do perfil selecionado. Depois de selecionar os dispositivos e clicar no botão Excluir, um pop-up de confirmação aparece na tela. Clique em **Excluir**.
- **Editar** - use esta opção para editar dispositivos do perfil selecionado. Você precisa selecionar os dispositivos e clicar no botão **Editar**.

Uso do Samsung Knox Mobile Enrollment

O Samsung Knox Mobile Enrollment permite que os administradores registrem dispositivos Samsung qualificados para usar o Ivanti Neurons for MDM. Com o Knox Mobile Enrollment, um dispositivo pode ser enviado diretamente de um revendedor aprovado para um usuário final e o Go Android client será automaticamente baixado com os dados de registro preenchidos previamente. Para obter detalhes, consulte o Samsung Knox Mobile Enrollment for Android Enterprise.

Requisitos

- Dispositivo listar por IMEI
- CSV arquivo que contém uma lista de dispositivos que têm um IMEI ou número de série, e opcionalmente um nome de usuário e senha de registro.
- Ivanti Neurons for MDM (versão atual).
- Conta do Samsung Knox aprovada para registro móvel
- Dispositivos Samsung suportados. Uma lista de dispositivos Samsung suportados está disponível aqui.

Inscrever dispositivos Oculus

Ivanti Neurons for MDM agora pode gerenciar os dispositivos Quest for Business (dispositivos Oculus). Atualmente, o Meta suporta dispositivos Oculus for Business (OFB) e Quest for Business (QFB) para MDM. Você precisa executar algumas tarefas básicas no console Meta para deixar os dispositivos prontos para MDM e, em seguida, registrar-se no Ivanti Neurons for MDM.

Você pode inscrever a frota de dispositivos Oculus no Gerenciador de Dispositivos, no console do Meta Workplace. Você precisa fazer login no Oculus Business Workplace usando as credenciais compartilhadas no seu e-mail registrado. Na página inicial, serão exibidas informações de todos os dispositivos na seção Frota de Dispositivos. A seção Frota de Dispositivos apresenta um panorama geral de todos os dispositivos disponíveis no Gerenciamento de Dispositivos. As informações incluem nome do dispositivo, status do dispositivo, SO (sistema operacional), modelo etc.

Esta seção contém os seguintes tópicos:

- Pré-requisitos para inscrever dispositivos Oculus
  - "Configurar um aplicativo MDM no Gerenciador de Dispositivos" abaixo
  - "Configurar o dispositivo Oculus" na página seguinte
- Registrar um dispositivo OFB com MobileIron Go
  - "No console do Ivanti Neurons for MDM" na página 266
  - "No cliente Go" na página 266

Pré-requisitos para inscrever dispositivos Oculus

Configurar um aplicativo MDM no Gerenciador de Dispositivos

Os dispositivos/headsets são provisionados e atualizados para, pelo menos, a **v28** do **Oculus for Business**. No Meta Console, o administrador deve configurar um MDM no Gerenciador de Dispositivos e mapear os dispositivos Oculus para esse serviço MDM específico.

Procedimento

1. Na página inicial do **Oculus Business Workplace**, selecione **Aplicativos**.
2. Em **Biblioteca de Aplicativos**, clique no aplicativo MDM de terceiros que você deseja instalar e clique em **Atualizar**.
3. Selecione o MDM apropriado para o aplicativo na lista em **Gerenciamento de Dispositivos Móveis** e clique em **Atualizar Aplicativo**.
4. Clique no headset Oculus em que deseja instalar o MDM. As informações do dispositivo aparecerão na tela.
5. Na guia **Sobre**, role para baixo até **Gerenciador de Dispositivos Móveis**.
6. Clique no botão **Editar** ao lado da opção **Autoridade MDM**.

   Por padrão, a opção Gerenciador de Dispositivos Oculus estará selecionada. Você precisa selecionar o App da Autoridade MDM e selecionar **MobileIron Go** na lista App da Autoridade MDM.

7. Clique em **Salvar**. O dispositivo é redefinido automaticamente, e você precisa configurar o dispositivo Oculus usando o aplicativo de configuração.

Configurar o dispositivo Oculus

Você pode adicionar dispositivos Oculus Quest 2 Headset usando o aplicativo Device Setup. Esse aplicativo deve ser compartilhado com os usuários necessários para que eles possam baixá-lo e instalá-lo em seus dispositivos Android.

Procedimento

1. Na seção **Frota de Dispositivos**, clique em **Dispositivos não configurados**.
2. Clique em **Obter app de configuração**. A página **Enviar link de download** aparece na tela.
3. Selecione um ou mais membros da equipe na lista ou clique em **Adicionar destinatário** para selecionar na lista.
4. Clique em **Enviar link**. Os usuários selecionados receberão um e-mail com um link para instalar o aplicativo **Device Setup**.
5. Clique no link **Baixar App Device Setup** no e-mail para instalar o **App Device Setup** no seu dispositivo Android.

   > Após o download, esse aplicativo não aparecerá na App Store do seu dispositivo. Você precisa pegá-lo na seção Downloads do seu dispositivo e instalá-lo.

6. Abra o aplicativo **Oculus for Business** no seu dispositivo Android.
7. Ligue os dispositivos Oculus pressionando o botão liga/desliga por 2 segundos.
8. Ligue o Bluetooth e coloque seu dispositivo Android próximo aos dispositivos Oculus até que a configuração seja concluída.
9. Procure os dispositivos Oculus usando o Bluetooth do seu dispositivo Android.
10. Assim que o dispositivo Oculus desejado for encontrado, será preciso conectá-lo a uma rede Wi-Fi para concluir a configuração.
11. Clique em **Inserir informações de Wi-Fi**, forneça o nome da rede e a senha e clique em **Salvar**. Agora, o dispositivo Oculus está conectado à rede Wi-Fi.
12. Clique em **Iniciar configuração**. Uma notificação é exibida na tela informando que a configuração está em andamento e você não deve fechar o aplicativo nem manusear os headsets enquanto ela estiver em curso.

Uma confirmação aparece na tela. Você pode continuar a busca por outros dispositivos usando o botão **Encontrar mais dispositivos**.

Registrar um dispositivo OFB com MobileIron Go

No console do Ivanti Neurons for MDM

É possível registrar um dispositivo OFB com MobileIron Go no console do Ivanti Neurons for MDM. No entanto, a configuração do modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP) (em **Configurações**) deve ser distribuída a esses grupos de dispositivos OFB.

No cliente Go

É possível registrar um dispositivo OFB no cliente MobileIron Go. Você precisa executar as seguintes tarefas para registrar o dispositivo OFB:

- Após concluir a configuração usando o aplicativo OFB Setup, siga as instruções na tela no headset OFB e conclua a configuração do dispositivo.
- O aplicativo MobileIron Go é iniciado automaticamente, e você precisa fornecer as credenciais de login e concluir o registro seguindo as instruções do MDM.

Agora, o dispositivo está provisionado no modo DO e configurado para ser gerenciado pelo MDM.

Como ativar o Bluetooth em um dispositivo

Aplicável a:

- iOS 11.3+
- macOS 10.13.4+

É possível ativar ou desativar o Bluetooth em um dispositivo.

Procedimento

1. Navegue até o dispositivo na **página Dispositivos**.
2. Execute uma das seguintes ações:
    - Selecione o dispositivo da lista.
    - Clique no nome do dispositivo para exibir a página de detalhes do Dispositivo.
3. No menu **Ações**, clique em **Ativar/Desativar Bluetooth**.
4. Clique em **OK**.

As alterações serão enviadas ao dispositivo na próxima vez que ele fizer o registro.

Agendar atualização do iOS

Aplicável a:

- Dispositivos de inscrição com iOS 9.0+ supervisionado
- Dispositivos com iOS 10.3+ supervisionado.

Programe um dispositivo iOS para atualizar para a versão mais recente do iOS atualmente disponível. A opção **Atualizar Versão do SO** em **Dispositivo** > **Ações** para dispositivos iOS Supervisionados exibe uma lista contendo apenas as versões de iOS aplicáveis ao dispositivo.

Procedimento

1. Navegue até o dispositivo na página Dispositivos.
2. Clique no nome do dispositivo para exibir a página de detalhes do Dispositivo.
3. No menu **Ações**, clique em **Atualizar Versão do SO**.
4. No assistente **Atualizar Versão do SO**, examine a versão do iOS e selecione a versão do SO na lista suspensa **Atualizar para versão**.

   > Se você inserir uma versão igual ou mais antiga, será exibida uma mensagem de erro indicando que a versão de destino do iOS deve ser maior que a versão atual.

5. Clique em **Atualizar**.

O dispositivo iOS ficará programado para receber a versão mais recente do iOS que estiver disponível quando fizer check-in. Se o dispositivo tiver uma senha, depois que o MDM enviar a atualização para o dispositivo, o dispositivo colocará a atualização na fila e o usuário será solicitado a inserir sua senha para iniciar a instalação. Para obter mais informações, consulte Software_Updates.

Reinstalar apps do sistema do iOS

Aplicável a:

- Dispositivos iOS 11.3+.

Reinstale apps do sistema iOS que foram excluídos em dispositivos iOS.

Procedimento

1. Navegue até a página Dispositivos. Ou clique no nome do dispositivo e realize esta ação na página Detalhes do dispositivo.
2. Selecione um ou mais dispositivos iOS.
3. No menu **Ações**, clique em **Reinstalar apps do sistema do iOS**.
4. Na caixa de exibição Reinstalar apps do sistema iOS, selecione um ou mais apps disponíveis para serem instalados nos dispositivos.
5. Clique em **Reinstalar apps**.

Os aplicativos serão instalados nos dispositivos iOS selecionados e compatíveis quando estes fizerem check-in. Os aplicativos do sistema instalados dessa maneira não serão considerados aplicativos gerenciados. Se não houver dispositivos compatíveis selecionados, será exibida uma mensagem dizendo que os apps do sistema não serão instalados nesses dispositivos.

Para obter mais informações, consulte Software_Updates.

Atribuindo um dispositivo a um novo usuário

Pode ser necessário provisionar novamente um dispositivo registrado existente para um novo usuário, caso a função do usuário ou o seu relacionamento anterior com a empresa tenham mudado. Essas etapas ajudam a evitar aposentar e registrar novamente o dispositivo.

Procedimento:

1. Navegue até o dispositivo na **página Dispositivos**.
2. Clique no nome do dispositivo para exibir a página de detalhes do Dispositivo.
3. Clique no ícone **Atribuir ao usuário**  .
4. Comece a digitar o nome do usuário no campo **Pesquisar usuário**... .
5. Selecione o usuário desejado.
6. Clique em **Atribuir ao usuário**.
   O dispositivo será provisionado para aquele usuário.

Você pode perceber que em cenários baseados em usuário e baseados em licença, é possível atribuir um dispositivo a um usuário que excedeu o limite do dispositivo atribuído. Isso acontece porque a intenção do recurso de limite do dispositivo é limitar o registro de dispositivos para oferecer suporte aos cenários Traga Seu Próprio Dispositivo (BYOD).

Tanto na licença baseada em dispositivo quanto na licença baseada em usuário, impor o limite do dispositivo é uma ação inconsequente. Para as licenças baseadas em dispositivo, o custo para o cliente final não é alterado, pois o número total de dispositivos no sistema permanece o mesmo. Para licenças baseadas em usuário, a ausência dessa verificação beneficia o cliente. Por exemplo, considere cinco usuários, U1 a U5 com cinco dispositivos cada um. Com a licença baseada em usuário, seriam necessárias cinco licenças. Se ao invés disso, dois dos dispositivos de U4 e U5 fossem movidos para U1 e U2, então o número de licenças necessárias CAIRIA de cinco para três.

Imposição de registro do dispositivo

Os dispositivos precisam se comunicar com o Ivanti Neurons for MDM (fazer check-in) para receber e fornecer informações. Os registros são programados em intervalos regulares. Você também pode solicitar que um dispositivo faça o registro sob demanda. Forçar o registro de um dispositivo pode acelerar o processo de aplicação de **configurações**[1], atualização de **políticas**[2] etc.

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione os dispositivos.
3. Clique em **Ações**.
4. Selecione **Forçar check-in**.
5. É possível clicar no link do nome do dispositivo para ir para a página de detalhes do Dispositivo e, depois, clicar no ícone **Forçar registro**  e clicar **OK**.

Se houver falha no lado do dispositivo ao processar o comando de instalação da configuração durante o check-in, o Ivanti Neurons for MDM não tentará reinstalar automaticamente a configuração no dispositivo durante os check-ins posteriores. O administrador deve tentar instalar a configuração manualmente na página de detalhes do dispositivo. Para isso, acesse a guia Configuração, selecione a configuração do erro e clique em **Tentar instalação novamente**.

[1]collections of settings that you send to devices.

[2]sets of requirements and compliance actions defined for devices.

Como localizar um dispositivo

Se você habilitou o recurso Localizar para um dispositivo, poderá exibir a última localização conhecida desse dispositivo. Você deve editar a configuração de privacidade para ativar a coleta de dados de localização e aplicar a configuração ao dispositivo para ativar esse recurso. O dispositivo também deve suportar esse recurso, e o usuário deve concordar em compartilhar seus dados de localização.

Procedimento

1. Navegue até o dispositivo na página **Dispositivos** .
2. Clique no link na coluna **Nome**.
3. Na guia **Visão Geral**, clique no link em **Localização do dispositivo**.

Os seguintes detalhes são exibidos na página:

Nome do campo	Descrição
Localizado por último em	Exibe a data e o horário em que o dispositivo foi localizado pela última vez.
Coordenadas	Exibe a latitude (posição norte-sul) e a longitude (posição leste-oeste) do dispositivo.

Também é possível encontrar o mapa de localização do dispositivo exibido na página.

Como bloquear um dispositivo

Você pode acionar o bloqueio de tela em um dispositivo. O bloqueio pode funcionar de forma diferente em diferentes dispositivos.

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione o dispositivo.
3. Clique em **Ações**.
4. Selecione **Bloquear**.
5. Alternativamente, é possível clicar no link do nome do dispositivo para acessar a página de detalhes do dispositivo e, depois, clicar no ícone **Bloquear** e em **OK**.
6. Para aplicativos AppConnect Android, o comando Bloquear bloqueia o usuário fora do contêiner e também bloqueia o dispositivo. Os usuários podem fazer login de novo no dispositivo e no aplicativo AppConnect usando a senha do dispositivo e a senha do AppConnect, respectivamente.
7. Para dispositivos iOS 7, insira uma mensagem e um número de telefone para a tela (opcional). Essas opções podem fornecer aos usuários informações sobre o motivo pelo qual o dispositivo foi bloqueado e o número para ligar para desbloqueá-lo.
8. Para dispositivos macOS, o usuário será solicitado a inserir um PIN de 6 dígitos como senha para acessar o dispositivo. Para realizar o bloqueio da tela, o usuário do dispositivo precisará:
    1. Inserir o PIN.
    2. Marcar a caixa de seleção para confirmar o bloqueio do dispositivo.
    3. Clicar em **Sim, enviar o comando de trava**.

    No macOS, o usuário pode adicionar uma mensagem de tela de bloqueio opcional e o número de telefone durante a configuração da senha de bloqueio do dispositivo.

9. Para dispositivos ChromeOS, quando você executa uma operação de bloqueio, a janela pop-up "Bloquear o dispositivo pode exigir que o usuário insira uma senha de acesso" aparece na tela. Clique em **Bloquear**, e o status do dispositivo será atualizado para **Desabilitação enviada**. O status atualizado ficará visível após a sincronização periódica do dispositivo.

Métodos alternativos de bloquear um dispositivo:

- O usuário de um dispositivo pode executar a ação de bloqueio a partir do Portal de autoatendimento.
- Um administrador pode executar a ação de bloqueio a partir do Portal do administrador.

Gerenciar dispositivos no modo perdido da Apple

Esta seção contém os seguintes tópicos:

Aplicável para: dispositivos iOS 10.3 ou superior supervisionados

É possível colocar um dispositivo supervisionado no modo perdido pelo Ivanti Neurons for MDM. Isso significa que você relata o dispositivo como perdido para os servidores da Apple, permitindo recuperar a última localização gravada do dispositivo, bem como desabilitar o modo perdido se o dispositivo for encontrado.

Habilitar o modo perdido

É possível relatar um dispositivo como perdido para os servidores da Apple colocando-o em modo perdido. Depois de colocar um dispositivo em modo perdido:

- Se o dispositivo for desativado, não será possível desabilitar o modo perdido.
- Se o dispositivo for apagado, não será é possível localizá-lo ou rastreá-lo.

Procedimento

1. Acesse **Dispositivos**.
2. Marque a caixa de seleção do dispositivo.
3. Selecione **Ações > Apenas iOS > Modo perdido**.
4. Na seção Modo de dispositivo perdido, selecione a opção **Ativar modo perdido** para colocar o dispositivo iOS em modo perdido.

Executar ações no modo perdido

Depois de habilitar o modo perdido, é possível executar as seguintes ações na seção Modo de dispositivo perdido:

- **Mensagem push/Número de telefone para iPhone**
  - Insira uma mensagem a ser exibida na tela bloqueada do dispositivo perdido.
  - Insira um número de contato para ser exibido na tela bloqueada do dispositivo perdido. Se alguém encontrar o dispositivo, poderá ligar para o número e relatar isso.
- Bloquear dispositivo
- **Atualizar localização do dispositivo**

  Se o dispositivo for apagado, não será possível localizá-lo.

- **Reproduzir som do modo perdido**

  O som será reproduzido até o dispositivo ser removido do modo perdido ou um usuário desativar o som no dispositivo.

Desabilitar o modo perdido

Se um dispositivo no modo perdido for recuperado ou o modo perdido foi habilitado por engano, desabilite esse modo.

Se o dispositivo perdido for desativado a partir do Ivanti Neurons for MDM, desativar o modo perdido não funcionará.

Procedimento

1. Acesse **Dispositivos**.
2. Marque a caixa de seleção do dispositivo.
3. Selecione **Ações > Apenas iOS > Modo perdido**.
4. Na seção Modo de dispositivo perdido, desmarque a opção **Modo perdido ativado para o dispositivo**.

Solicitação de logs de depuração

Você pode solicitar registros de depuração a dispositivos iOS, MacOS e Android de trabalho gerenciados, para fins de solução de problemas. Usando o comando "Request debug logs" na página de Dispositivos, as ações e sucesso ou falha de um evento são capturados nos registros de auditoria.

Este recurso requer os seguintes clientes:

- Dispositivos com iOS exigem o Go 5.3.0 para iOS ou versões mais recentes com suporte. Para dispositivos que migraram do Core para o Ivanti Neurons for MDM, este recurso exige o Mobile@Work 12.2.0 para iOS ou versões mais recentes com suporte.
- Dispositivos macOS exigem o Mobile@Work para macOS 1.5 ou versões mais recentes com suporte.
- Dispositivos gerenciados de trabalho com Android exigem o Go 65 para Android ou versões mais recentes com suporte.

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione o dispositivo e clique no link do nome para acessar a página de detalhes do Dispositivo.
3. Clique no ícone .
4. Selecione **Solicitar registros de depuração** e clique em **OK**.

Quando a solicitação é enviada e os registros estão prontos no dispositivo, uma notificação é enviada ao administrador e exibida nos registros do dispositivo. Também é possível clicar no link para fazer download dos registros do dispositivo.

Como desativar um dispositivo

Desativar um dispositivo encerra o relacionamento dele com o Ivanti Neurons for MDM. Você deve desativar um dispositivo se:

- o usuário sair da empresa
- o usuário substituiu o dispositivo
- for necessário desfazer as tarefas de gerenciamento concluídas (começar novamente)

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione o dispositivo.
3. Clique em **Ações** (canto superior direito).
4. Selecione **Desativar**.
5. É possível clicar no link do nome do dispositivo para ir para a página de detalhes do Dispositivo e, depois, clicar no ícone .
6. Selecione **Aposentar** e clique em **OK**.

Renunciar à propriedade de um dispositivo

Aplicável a dispositivos Android no modo Perfil de trabalho em dispositivo de propriedade da empresa.

Renunciar à propriedade de um dispositivo no Work Profile em modo de dispositivo de propriedade da empresa remove o perfil de trabalho e o dispositivo do Ivanti Neurons for MDM, sem afetar aplicativos e dados pessoais. O usuário final poderá então usar o dispositivo como um dispositivo pessoal com total acesso a todos os controles e definições do dispositivo.

O dispositivo precisa ser removido do Toque zero do Google ou do portal do Knox Mobile Enrollment.

Você deve renunciar a propriedade de um dispositivo se:

- o usuário sair da empresa
- o usuário substituiu o dispositivo

Procedimento

1. Acesse **Dispositivos** > **Dispositivos**.
2. Selecione o dispositivo.
3. Clique na **página de detalhes do Dispositivo** e no ícone .
4. Selecione **Renunciar à propriedade**.

Como apagar um dispositivo

Apagar um dispositivo remove todos os dados e faz com que o ele volte às configurações predefinidas de fábrica.

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione o dispositivo.
3. Clique em **Ações** (canto superior direito).
4. Selecione **Apagar**.
5. Como alternativa, clique no link do nome do dispositivo para acessar a página Detalhes do dispositivo e clique no ícone . Selecione **Apagar** e clique em **OK**.
6. (Opcional, aplicável a dispositivos iOS 11 ou superior) Selecione a opção **Preservar plano de dados**.
7. (Opcional, aplicável a dispositivos iOS 11.3 ou superior) Selecione a opção **Ignorar configuração de proximidade**.
8. Para dispositivos macOS, você pode enviar um PIN de 6 dígitos ao dispositivo como senha. O usuário será então solicitado a inserir o PIN no dispositivo para acessá-lo. Para continuar com a ação de apagamento, o usuário do dispositivo precisará:
   a. Inserir o PIN.
   b. Marcar a caixa de seleção para confirmar a ação de apagamento do dispositivo.
   c. Clicar em **Sim, apagar este dispositivo**.
9. Em dispositivos ChromeOS, quando você executa uma operação de apagamento na página **Detalhes do dispositivo** ou **Listagem de dispositivos**, a janela pop-up "Apagar um dispositivo faz com que ele retorne às configurações de fábrica, o que pode resultar na perda dos dados. A ação de apagamento difere conforme a plataforma." aparece na tela.
   a. Marque a caixa de seleção "Compreendo que o apagamento não pode ser desfeito" para confirmar a ação de apagamento do dispositivo.

b. Clique em **Apagar** para apagar o dispositivo.

O status do dispositivo muda para "**Apagamento enviado**". O status atualizado ficará visível após a sincronização periódica do dispositivo.

Em dispositivos Android Enterprise, você pode executar a ação **Apagar** mesmo depois que o dispositivo for reinicializado e permanecer bloqueado.

Dispositivos Android que estejam no estado **Apagamento pendente** podem ser excluídos usando-se a opção **Excluir dispositivo**, presente na página **Detalhes do dispositivo**. Depois que um dispositivo é excluído, ele perde a conexão com o servidor e se torna não conforme. Portanto, o usuário deve inscrever novamente o dispositivo após realizar a redefinição de fábrica.

Como excluir um dispositivo

Após desativar um dispositivo, é possível excluí-lo. Ao excluí-lo, ele é removido de todas as páginas. Você pode excluir um dispositivo somente se seu status for Desativado ou Desativação pendente.

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Navegue até o dispositivo.
3. Clique no link na coluna **Nome**.
4. Clique no link **Excluir dispositivo** (painel esquerdo).
5. Leia o aviso exibido.
6. Se você ainda quiser excluir o dispositivo, selecione a caixa de seleção para confirmar.
7. Clique em **Excluir**.

Como desbloquear um dispositivo

Esta seção contém os seguintes tópicos:

Para desbloquear um dispositivo:

Você pode limpar o bloqueio de tela em um dispositivo. O desbloqueio pode funcionar de forma diferente em diferentes dispositivos.

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Selecione os dispositivos.
3. Clique em **Ações**.
4. Selecione **Desbloquear**.
5. Alternativamente, é possível clicar no link do nome do dispositivo para acessar a página de detalhes do dispositivo e, depois, clicar no ícone **Desbloquear**  e em **OK**.

Desbloquear dispositivos Android

Quando um comando Desbloquear é recebido, o aplicativo Android tenta redefinir a senha. A tabela a seguir explica como desbloquear dispositivos Android em diferentes modos de dispositivo:

	Administrador de dispositivo	Proprietário do dispositivo	Proprietário do perfil
Android 7 e superior	Desbloquear é ignorado no caso de dispositivos de administrador de dispositivo. A senha do dispositivo não é redefinida como vazia ou "0000"	É necessário apagar a senha do dispositivo ou defini-la como "0000", caso o apagamento da senha do dispositivo não funcione. Em seguida, deve-se solicitar para o usuário definir uma nova senha do dispositivo, caso exista uma configuração de senha.	Redefina a senha como "0000" e, caso haja uma configuração de Desafio de trabalho (Work Challenge), o usuário será obrigado a definir um novo desafio de trabalho segundo as restrições do Desafio de trabalho (Work Challenge).
Android 6 e anterior	É possível apagar a senha do dispositivo ou defini-la como "0000", caso o apagamento da senha não funcione. O usuário será solicitado a configurar uma nova senha caso haja uma configuração de senha de dispositivo. Exemplo: No Samsung S7, mediante o comando Desbloquear, a senha do dispositivo é apagada.		Não há suporte para desbloquear o perfil e redefinir a senha no dispositivo.

Em dispositivos Android Enterprise, você pode executar a ação de dispositivo **Desbloquear** mesmo depois que o dispositivo for reinicializado e permanecer bloqueado.

Desbloquear AppConnect para apps Android

Para apps AppConnect, o comando **Desbloqueio do AppConnect** ajuda a desbloquear os recipientes que foram bloqueados por conta de usuários tentarem efetuar login várias vezes com senhas incorretas. Essa ação não desbloqueia o dispositivo.

Desbloquear um dispositivo iOS

Ao receber um comando Desbloquear, o aplicativo iOS remove a senha do dispositivo. Se a configuração da senha especificar que é necessária uma nova senha, o usuário do dispositivo deverá configurar uma nova senha, conforme as regras definidas na configuração da senha. O usuário deve fazer essa alteração dentro de 60 minutos ou o aplicativo forçará o usuário a configurar a nova senha.

Desbloquear dispositivos ChromeOS

Quando um dispositivo ChromeOS é selecionado e a opção **Desbloquear** é acionada, uma janela pop-up aparece na tela: "O desbloqueio poderá apagar a senha existente para permitir que o usuário acesse o dispositivo. O desbloqueio varia de acordo com a plataforma." Clique em **Desbloquear**, e o status do dispositivo será atualizado para "Desbloqueio enviado". O status atualizado ficará visível após a sincronização periódica do dispositivo.

Reiniciar ou desligar dispositivos

Esta seção contém os seguintes tópicos:

Aplicável para: Android 7.0+ (dispositivos gerenciados), iOS 10.3+ (iOS e tvOS) supervisionado, macOS 10.13+ e dispositivos Windows 10+

Os administradores podem reiniciar ou desligar um dispositivo supervisionado com iOS ou tvOS de forma individual a partir da página de detalhes do dispositivo ou em massa a partir da página de lista de dispositivos.

Reiniciar um dispositivo

Procedimento

1. Acesse **Dispositivos**.
2. Navegue até o dispositivo.
3. Clique no link na coluna **Nome**.
4. Clique no botão **Ações**.
5. Clique em **Reiniciar/desligar dispositivo**.

   Os dispositivos não suportados não podem ser reiniciados.

6. Leia o aviso exibido.
7. (Opcional) Selecione a opção de limpar a senha do dispositivo na reinicialização. Se a senha não for apagada, o dispositivo precisará de senha e não será conectado ao Wi-Fi após a reinicialização.
8. Selecione **Reiniciar dispositivo** se ainda não estiver selecionado.

9. Se ainda quiser reiniciar o dispositivo, clique em **Enviar ao dispositivo**. Caso contrário, clique em **Cancelar**.

> Para dispositivos Android, os administradores podem visualizar a informação sobre quando o dispositivo foi reiniciado em **Tempo de atividade**, na página Detalhes do dispositivo.

É possível reiniciar vários dispositivos suportados na página de lista de **Dispositivos**. Para isso, selecione os dispositivos, clique em **Ações > Reiniciar/desligar dispositivo** e siga as instruções na tela.

Desligar um dispositivo

Procedimento

1. Acesse **Dispositivos**.
2. Navegue até o dispositivo.
3. Clique no link na coluna **Nome**.
4. Clique no botão **Ações**.
5. Clique em **Reiniciar/desligar dispositivo**.

> Os dispositivos não suportados não podem ser reiniciados.

6. Leia o aviso exibido.
7. Selecione **Desligar dispositivo**.
8. Se ainda quiser desligar o dispositivo, clique em **Enviar ao dispositivo**. Caso contrário, clique em **Cancelar**.

É possível desligar vários dispositivos suportados na página de lista de **Dispositivos**. Para isso, selecione os dispositivos, clique em **Ações > Reiniciar/desligar dispositivo** e siga as instruções na tela.

Como apagar as Senhas de Restrições (somente iOS)

Você pode apagar as senhas de restrições configuradas pelo usuário em dispositivos iOS 8 supervisionados. Esta ação está disponível apenas para dispositivos ativos.

Procedimento

1. Acesse Dispositivos > Dispositivos.
2. Selecione a entrada para o dispositivo.
3. Selecione Ações > Apagar Senhas de Restrições.
4. Quando solicitado, confirme a ação.

Como excluir uma associação Sentry de um dispositivo

A associação do Sentry aos dispositivos é feita para tunelamento de aplicativos ou sistema de e-mail habilitado por ActiveSync, que controla o acesso de e-mail nos dispositivos. Se necessário, qualquer dispositivo que esteja associado ao Sentry poderá ser removido de sua associação da seguinte maneira:

Procedimento

1. Acesse **Dispositivos.**
2. Na coluna **Nome**, clique no link do dispositivo para o qual você deseja excluir a associação Sentry.
3. Clique na guia **Sentry**.
4. Na coluna **Ações** , clique em **Excluir**.

Como atribuir atributos personalizados aos dispositivos

Você pode designar atributos de dispositivo personalizados, como ID interno, a um ou mais dispositivos. Cada atributo tem um valor correspondente que você pode usar para tarefas como criar configurações e grupos de dispositivos. Depois de criar atributos personalizados, você pode atribuí-los a dispositivos. Para mais informações sobre como gerenciar atributos, consulte "Atributos" na página 1164.

Procedimento

1. Faça login no Portal Administrativo.
2. Acesse **Dispositivos**.
3. Selecione um ou mais dispositivos.
4. Clique em **Ações**.
5. Selecione **Atribuir atributos personalizados**.
6. Selecione *uma* das opções a seguir:
    - Forçar a designação (substituição) de todos os atributos, mesmo que quaisquer valores existentes sejam encontrados.
    - Substituir apenas se o valor estiver vazio e ignorar os atributos com valores existentes.
7. Selecione os atributos que deseja atribuir e insira seus valores (valores vazios não são permitidos).
8. Clique em **Atribuir**.

Os **Atributos personalizados do dispositivo** com seus valores podem ser exportados para o formato CSV na página **Detalhes do dispositivo**.

Como remover atributos personalizados dos dispositivos

Proceda com cuidado, pois esta ação não poderá ser revertida. Para remover atributos personalizados de um ou mais dispositivos:

Procedimento

1. Acesse **Dispositivos**.
2. Selecione um ou mais dispositivos.
3. Clique em **Ações**.
4. Selecione **Remover atributos personalizados**.
5. Selecione os atributos que deseja remover.
6. Clique em **Remover**.

Sincronização e busca de feedback de aplicativo

Você pode enviar uma solicitação para um aplicativo instalado em dispositivos Android para obter os detalhes do status atual da configuração do aplicativo. Quando uma solicitação é enviada, você recebe um relatório de feedback de configuração do aplicativo para o dispositivo.

Procedimento

1. Acesse **Dispositivos**.
2. Clique no dispositivo para o qual você deseja enviar a solicitação.
3. Clique em **Ações**.
4. Selecione **Sincronizar e buscar feedback de aplicativo**. A solicitação é enviada para a sincronização e busca o feedback de configuração do aplicativo. O campo Última sincronização de feedback do aplicativo ao lado do campo Último registro do cliente será atualizado.
5. Na guia **Aplicativos instalados**, clique no link **Exibir detalhes** do aplicativo na coluna **Feedback do aplicativo**. A janela **Feedback do aplicativo** é exibida.
   Chave - fornece informações detalhadas e o posicionamento das configurações relatadas (na configuração Aplicativo gerenciado do app) com base no feedback recebido dos aplicativos.
   Marcação de hora - data e hora da chave.
   Severidade - especifica a severidade da chave. Exemplo: "Informação", "Erro".
   Mensagem - tipo de mensagem recebida do feedback de configuração do aplicativo. Exemplo: "Falha".
   Dados - detalhes dos dados recebidos do feedback de configuração do aplicativo.

Exibição do feedback de configuração do aplicativo para o App Catalog

Você pode visualizar o relatório de feedback de configuração do aplicativo para um aplicativo específico do App Catalog.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione um aplicativo que você deseja visualizar os detalhes.

3. Clique na guia **Feedback de configuração do aplicativo**. A coluna **Contagem de dispositivo** exibe o número de dispositivos (hyperlink) para cada chave do relatório de feedback de configuração do aplicativo.

4. Clique no número de hyperlink dos dispositivos para visualizar os seus detalhes. Por exemplo, ao clicar no hyperlink 5, são exibidos os detalhes de 5 dispositivos. Os detalhes a seguir são exibidos para uma combinação de "Chave" e "Severidade" que é exibida acima da tabela:
   Endereço de e-mail - especifica o nome de usuário. Ao clicar no link do nome do usuário, você é direcionado para a guia **Aplicativos instalados** em **Dispositivos > Detalhe do dispositivo**.
   Tipo de dispositivo - especifica o modelo do dispositivo.
   SO - Número de versão do SO Android.
   Número de série - número de série do dispositivo.
   Marcação de hora - data e hora da última atualização.
   Mensagem - tipo de mensagem recebida do feedback de configuração do aplicativo. Exemplo: "Falha".
   Dados - detalhes dos dados recebidos do feedback de configuração do aplicativo.

Você pode visualizar as notificações de erro de feedback de configuração do aplicativo para o dispositivo Android clicando no ícone de campainha (canto superior direito) ou na página **Painel > Notificações**. Clique no link de notificação para navegar até a guia **Feedback de configuração do aplicativo** e visualizar o relatório de feedback do aplicativo.

O relatório de feedback de configuração do aplicativo será removido e não será exibido quando o dispositivo for apagado ou desativado. O trabalho em segundo plano executado a cada 24 horas limpa os dados com mais de 7 dias.

Redefinir o PIN

Aplicável a: dispositivos móveis do Windows 8 e 10

O administrador pode redefinir o PIN para um dispositivo móvel do Windows. Um novo PIN será gerado para este dispositivo. Este recurso pode ser útil em situações como quando o usuário sai da organização sem redefinir o PIN de um dispositivo de propriedade da empresa.

Procedimento

1. Acesse **Dispositivos**.
2. Clique no nome do usuário ao qual o dispositivo está associado para visualizar a página de detalhes do dispositivo.
3. Na seção Geral, na linha do PIN, clique em **Redefinir**.
4. Na janela Redefinir PIN, selecione a caixa de seleção para confirmar a redefinição do PIN.
5. Clique em **Sim, prosseguir**.

Esse processo pode demorar alguns minutos. Verifique se o dispositivo está LIGADO. Na página de detalhes do dispositivo, clique em **Exibir** para visualizar o PIN recém-atribuído após a redefinição.

Configuração da senha do firmware

Aplicável a: macOS 10.13 ou a versões mais recentes com suporte.

O administrador pode configurar ou atualizar a senha do firmware (EFI) de um dispositivo com macOS. A senha do firmware impede a inicialização do dispositivo com macOS de qualquer dispositivo de armazenamento interno ou externo diferente do disco de inicialização selecionado pelo usuário do dispositivo. Como resultado, ele também impede o uso de diversas combinações de teclas de inicialização.

Procedimento:

1. Acesse **Dispositivos**.
2. Para configurar ou alterar a senha do firmware de um único dispositivo:
    a. Clique no nome do usuário ao qual o dispositivo está associado para visualizar a página de detalhes do dispositivo.
    b. Na seção Geral, expanda **Senha do firmware** e clique em **Configurar senha** ou em **Configurar/Alterar senha do firmware** no menu Ações do dispositivo.
    c. As seguintes informações são exibidas nesta seção:
        a. **Senha:** senha ou uma lista de senhas prováveis.

> Quando o administrador configura a senha do firmware, o comando é enviado ao dispositivo. Se o dispositivo não responder no prazo, a senha será armazenada temporariamente e exibida neste campo. A nova senha não entrará em vigor até a confirmação e reinicialização do dispositivo. Até lá, todas as senhas prováveis são exibidas. Depois que o dispositivo é reinicializado e a alteração da senha é confirmada, todas as senhas desprezadas são apagadas.

        b. **Alteração pendente:** indica se a alteração da senha está pendente.
        c. **Status do comando:** indica se a alteração da senha foi bem-sucedida ou se ocorreu uma falha.

d. **Permitir OptionROMs:** indica se ROMs opcionais devem ser ativados. Por padrão, a configuração é Não.

3. Para configurar ou alterar a senha do firmware de mais de um dispositivo:

   a. Selecione os dispositivos.

   b. No menu Ações, clique em **Configurar/Alterar senha do firmware**.

4. Insira a senha atual e a nova senha.
   Se for a primeira vez, a senha atual pode ser deixada em branco.
   Para redefinir a senha, deixe o campo de nova senha em branco.

5. Clique em **Salvar**.

Somente os dispositivos com versões compatíveis do macOS serão atualizados com a nova senha. Os dispositivos incompatíveis serão ignorados.

Como emitir uma nova chave de recuperação pessoal

Aplicável a: dispositivos macOS com Mobile@Work para macOS 1.66 ou versões mais recentes com suporte.

Ao migrar de outras soluções MDM para Ivanti Neurons for MDM, os administradores podem solicitar que o SO emita uma nova Chave de recuperação pessoal (PRK) após o registro, se uma PRK tiver sido emitida antes do registro. Isso permite que a chave seja armazenada em Ivanti Neurons for MDM.

Você pode visualizar o log de Trilhas de auditoria para as atividades de PRK da seguinte maneira:

1. Vá até **Painel** > **Trilhas de auditoria**.
2. No filtro Tipo, selecione **Chave de recuperação pessoal**. As entradas de PRK serão exibidas na categoria Gerenciamento de dispositivos e em atividades como "Chave de recuperação pessoal visualizada".

Pré-requisito

Distribua as seguintes configurações para os dispositivos antes de executar este procedimento:

- Configuração de Mobile@Work para macOS.
- Configuração de Chave de recuperação do FileVault.

Procedimento

1. Entre em contato com o Suporte para solicitar que o script gere uma nova PRK no dispositivo.
2. Crie um atributo personalizado do dispositivo com o nome "deviceprk", usado no script.
3. Carregue o script para o repositório em **Administrador** > **Todos os scripts**. Enquanto isso, selecione o atributo personalizado "deviceprk".
4. Crie um grupo de dispositivos dinâmico para dispositivos para os quais a PRK não foi recuperada da solução antiga do MDM. Selecione as regras do grupo de dispositivos desta maneira: "**Platform=macOS** e **Criptografia ativada é igual a Sim** e **Chave de recuperação pessoal do macOS garantida é igual a Não** e **Tipo de chave de recuperação do macOS é igual a Pessoal**".
5. Crie uma configuração Script do Mobile@Work para macOS na qual você pode selecionar o script PRK no repositório. Distribua a configuração para o novo grupo de dispositivos.

6. Agende o script para ser executado uma vez por dia ou conforme desejado. Esse script solicitará a senha do usuário a cada execução. Por padrão, o período de tempo limite para a execução do script é de 60 segundos. Recomendamos estender o período de tempo limite na configuração correspondente Mobile@Work para macOS ao definir o campo **Tempo máx. de execução** em 300 segundos.

- A chave descriptografada está disponível na página de detalhes do dispositivo na seção Status de criptografia do dispositivo. Clique em **Visualizar** ao lado do campo Criptografia ativada FileVault.

- Ao obter a PRK, o dispositivo sai do grupo de dispositivos. Dessa forma, a configuração do script não será mais aplicável e será excluída do dispositivo.
- Depois que o MDM recuperar a chave de recuperação de um dispositivo usando o script, o script será desinstalado do dispositivo.

Definir ou alterar o bloqueio de recuperação

Aplicável a: macOS 11.5+

O administrador pode definir ou alterar o bloqueio de recuperação para a reinicialização de dispositivo para dispositivos macOS executando no Apple Silicon. Um bloqueio de recuperação evita a inicialização dos dispositivos macOS em modo de recuperação, a menos que uma senha seja inserida.

Procedimento:

1. Acesse **Dispositivos**.
2. Para definir ou alterar o bloqueio de recuperação para reinicialização:
    a. Clique no nome de exibição do usuário ao qual o dispositivo está associado para visualizar a página de detalhes do dispositivo. Execute uma das seguintes etapas:
    b. Na seção **Visão geral**, expanda **Bloqueio de recuperação** e clique em **Definir senha** ou em **Alterar senha**. Ou clique nas reticências em **Ações** e clique em **Definir/Alterar o bloqueio de recuperação**.
    c. Na caixa de diálogo **Definir/Alterar o bloqueio de recuperação**, faça o seguinte:
        a. **Senha atual**: insira a senha atual aqui. Deixe o campo vazio se você estiver definindo a senha pela primeira vez.
        b. **Senha**: insira a senha que você deseja definir.
        c. **Confirmar senha**: insira novamente a senha que você deseja definir.
3. Clique em **Definir/Alterar o bloqueio de recuperação**.

Em Visão geral, o **Bloqueio de recuperação habilitado** mostra o status da senha do Bloqueio de recuperação.

Os administradores também podem apagar a senha removendo a senha existente e clicando em **Definir/Alterar o bloqueio de recuperação**.

Aplicativos

Esta seção contém os seguintes tópicos:

App Catalog

Esta seção contém os seguintes tópicos:

Use a página Catálogo de Aplicativos para gerenciar seu catálogo de aplicativos.O App Catalog lista os aplicativos móveis disponibilizados para seus usuários. Isso inclui apps que os usuários podem baixar de lojas de aplicativos públicas e apps que você pretende distribuir usando o Ivanti Neurons for MDM (aplicativos internos). Apps habilitados para AppConnect, GoClient para iOS e M@W para macOS também estão disponíveis como apps empresariais na página do App Catalog, simplificando assim o processo de importação desses apps para configuração e distribuição. Em dispositivos Apenas MAM, os usuários do iOS deverão selecionar o certificado para autenticação do acesso aos apps quando abrirem o App Catalog.

MacBooks com chipset M1 da Apple oferecem suporte a apps VPP do iPhone e do iPad. Somente o administrador pode inserir os apps VPP do iPhone e do iPad suportados. Essa opção não está disponível para os usuários instalarem do App Catalog.

Para os locatários do Ivanti Neurons for MDM com dispositivos Android, se o Android Enterprise não estiver habilitado até o final de março de 2021, os administradores não serão capazes de procurar aplicativos com os nomes. A comunicação sobre essa mudança é exibida com uma mensagem de banner ao acessar a página do App Catalog. Essa mensagem de banner continua a ser exibida até que o Android Enterprise seja ativado nesses locatários e até que a opção "Não mostrar isso novamente" não seja selecionada.

- O método de Instalação silenciosa de aplicativo não está disponível para apps macOS públicos. Os aplicativos macOS também podem ser implementados por meio do Apps and Books da Apple, via licenças de dispositivos e por meio do método de Instalação silenciosa de aplicativos em inscrições.
- Ao carregar o aplicativo Go no servidor do Ivanti Neurons for MDM, se houver necessidade de selecionar a opção **Converter para aplicativo gerenciado**, você também precisará habilitar a opção **Instalar no dispositivo**.
- O App Catalog e a instalação de aplicativos não são compatíveis com dispositivos Sonim XP5s.
- O Android não permite que apps com privilégios ativos de administrador sejam desinstalados. Para desinstalar esse aplicativo, acesse **Configurações de dispositivo > Segurança > Administradores de dispositivos** e desative os privilégios de Administrador de dispositivo. Depois, desinstale o aplicativo.
- Apps Android internos podem ser carregados se o aplicativo estiver compactado ou ofuscado.
- Apps públicos não são compatíveis com iPads compartilhados.
- Devido a uma limitação da Apple para apps iOS Business-to-Business (B2B) disponíveis no App Catalog, as descrições e capturas de tela dos apps não estão disponíveis na guia **Detalhes**.
- Quando você procurar um app no App Catalog ou no portal do administrador, os resultados da pesquisa tomarão com base **Nome do Aplicativo**, **Comentário**, **Descrição**, **Versão de Exibição** e **Novidades**. Se os dados do aplicativo pesquisado corresponderem a algum desses campos, serão exibidos como resultado na pesquisa.

Licenciamento de recursos do aplicativo

Os seguintes recursos do Catálogo de aplicativos exigem licenciamento adicional:

- Instalação/desinstalação silenciosa de aplicativos:Silver licença
- Configuração por aplicativo: Gold licença

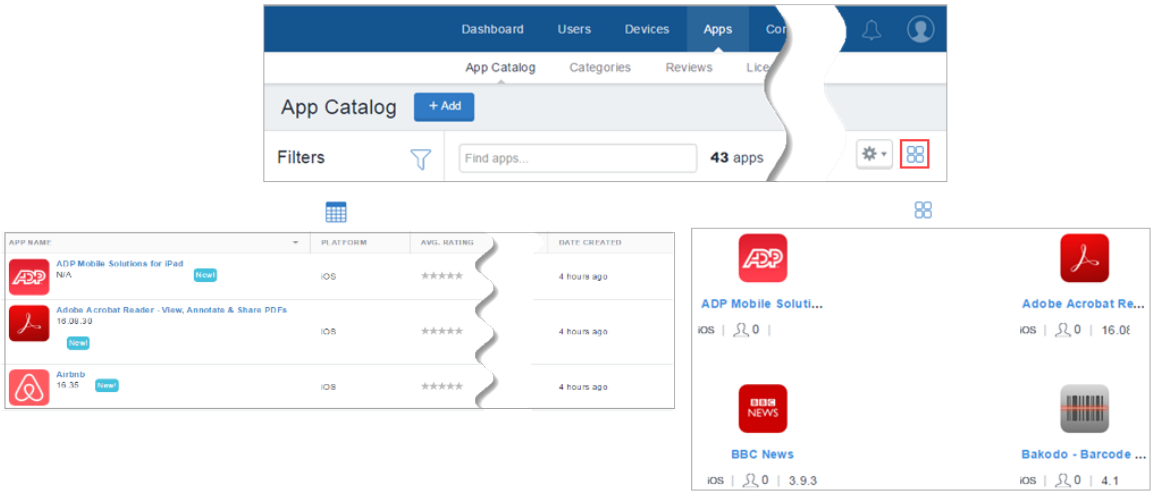
- Configuração personalizada do AppConnect: Licença Gold
- Configuração personalizada do Android Enterprise: licença Silver

Se um dispositivo Android estiver no modo de quiosque:

Somente apps internos podem ser instalados enquanto o dispositivo estiver no modo de quiosque. Você pode instalar apps públicos, mas o dispositivo deve sair do modo quiosque antes que os apps sejam instalados. Além disso, você pode limitar os apps disponíveis para uso em dispositivos no Modo de quiosque apenas aos apps aprovados ou permitidos por sua empresa. Nos dispositivos que usam o Android 4.1, se um aplicativo aprovado iniciar um aplicativo não incluído na lista de permitido, o aplicativo será iniciado e, em seguida, minimizado rapidamente. Nos dispositivos que usam o Android 5.0, o aplicativo não aprovado iniciado de um aplicativo permitido permanecerá disponível.

Alternar entre a visualização de lista e grade

Clique no ícone de Grade ou Lista no lado direito da tela do Catálogo de aplicativos.



Adicionando o aplicativo da Google Play Store para Android Enterprise

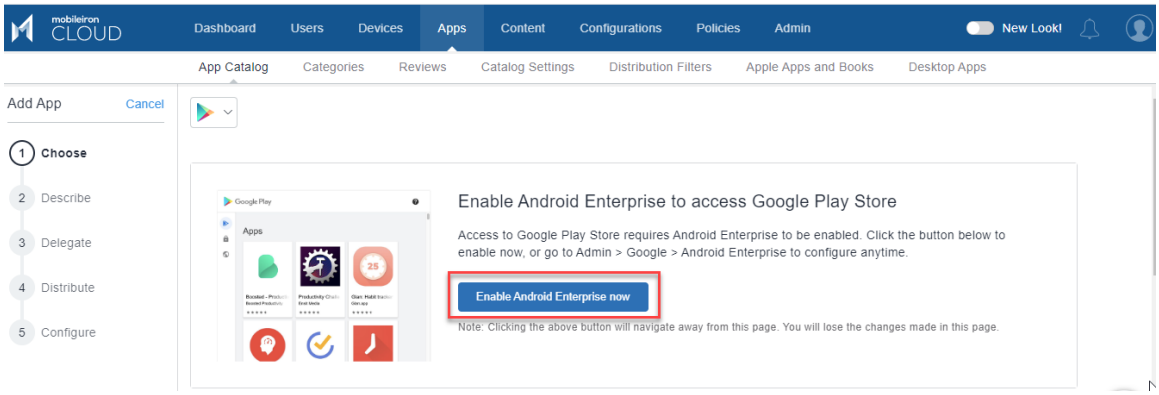
- Você pode adicionar um aplicativo da Google Play Store ao App Catalog e disponibilizá-lo aos usuários. Para adicionar um aplicativo da Google Play Store no Android Enterprise, é necessário aprovar a inclusão do aplicativo no App Catalog.

- O layout da Google Play Store para dispositivos Android Enterprise tem uma página inicial para dispositivos migrados que é gerenciada do Core e tem um link rápido para o Ivanti Neurons for MDM que exibe todos os aplicativos gerenciados a partir dele. A partir da versão 80 do Ivanti Neurons for MDM, ao migrar dispositivos Android Enterprise do Core para o Ivanti Neurons for MDM, somente os aplicativos que são comuns entre o Catálogo de Aplicativos do Core e do Ivanti Neurons for MDM são listados na Google Play Store do perfil de trabalho do dispositivo. Você pode clicar no botão Ivanti Neurons for MDM para visualizar a lista de todos os aplicativos disponíveis no Catálogo de Aplicativos do Ivanti Neurons for MDM.

O layout da Google Play Store para dispositivos Android Enterprise tem uma página inicial para dispositivos migrados que é gerenciada do Core e tem um link rápido para o Ivanti Neurons for MDM que exibe todos os aplicativos gerenciados a partir dele. A partir da versão 80 do Ivanti Neurons for MDM, ao migrar dispositivos Android Enterprise do Core para o Ivanti Neurons for MDM, somente os aplicativos que são comuns entre o Catálogo de Aplicativos do Core e do Ivanti Neurons for MDM são listados na Google Play Store do perfil de trabalho do dispositivo. Você pode clicar no botão Ivanti Neurons for MDM para visualizar todos os aplicativos disponíveis no Catálogo de Aplicativos do Ivanti Neurons for MDM.

Pré-requisito

- Você deve habilitar o Android Enterprise para acessar e adicionar aplicativos da Google Play Store ao App Catalog.



Procedure

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **Adicionar** (topo superior esquerdo).

   Selecione Google Play na lista suspensa para buscar um aplicativo na Google Play Store. O Google Play iFrame é exibido quando o Android Enterprise está inscrito.

3. Procure pelo aplicativo no campo Buscar e clique no aplicativo.
4. Clique em **APROVAR** para aprovar que o aplicativo seja disponibilizado a usuários. Uma janela de confirmação é exibida com os detalhes do acesso fornecido ao aplicativo. Clique em **APROVAR**.

   Para desaprovar um aplicativo anteriormente aprovado, clique em **DESAPROVADO**.

5. Selecione uma das seguintes opções para lidar com a solicitação de permissão de novo aplicativo:

Opção	Descrição
Configurações de aprovação	
Manter aprovado quando o aplicativo solicitar novas permissões	Permite que os usuários instalem o aplicativo atualizado
Revogar permissão deste aplicativo quando ele solicitar novas permissões	Remove o aplicativo da loja até que seja reaprovado.
Configurações de aprovação	
Adicionar assinante	Insira o endereço de email para o qual enviar notificações quando os apps que você aprovou solicitarem novas permissões.

6. Clique em **SALVAR**.

Adicionando um aplicativo de uma loja pública

Você pode adicionar um aplicativo de uma app Store pública no App Catalog e disponibilizá-lo aos usuários.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **Adicionar** (topo superior esquerdo).
3. Escolha o aplicativo que você deseja:
   a. Selecione a app store pública.
   b. Insira o nome do aplicativo.
   c. Selecione o aplicativo da lista.
   d. Clique em **Avançar**.
4. Descreva o aplicativo para os usuários:
   a. Adicione ou remova categorias.
   b. Insira uma descrição opcional.
   c. Clique em **Avançar**.
5. Defina uma distribuição para o aplicativo:
   a. Selecione uma opção de distribuição.
   b. Expanda a seção **Opções avançadas e configuração do aplicativo**.

      Use as diretrizes a seguir para concluir as opções:

Configuração	O que fazer
Instalar no dispositivo	Selecione essa opção para iniciar a instalação imediatamente após a inscrição. O usuário deverá confirmar a instalação do aplicativo, exceto sob as seguintes condições: • O dispositivo é um dispositivo iOS supervisionado para instalações novas e atualizações de aplicativos. • O dispositivo é um dispositivo iOS sem supervisão para atualizações de aplicativos. • Os usuários que se registraram no programa Apps and Books. • O dispositivo é um dispositivo Samsung Knox e a opção de instalação silenciosa abaixo foi selecionada. Para os apps públicos do iOS, quando instalados pela primeira vez no dispositivo, o App Catalog exibe o botão "Reinstalar" que permite que o usuário instale o aplicativo novamente. A reinstalação será realizada se a versão do aplicativo no dispositivo for diferente da versão na app Store do iOS.
Não exibir o aplicativo no App Catalog do usuário final	Selecione essa opção caso não queira que o usuário veja o aplicativo no catálogo de aplicativos no dispositivo.

Configuração	O que fazer
Definir prioridade de instalação de aplicativos	Selecione Alta, Média ou Baixa para definir a prioridade da instalação de aplicativos durante a integração do usuário. Apenas aplicativos de alta prioridade são instalados durante a integração do usuário.
Suspender reenvio de aplicativo após um número definido de tentativas com falha (somente iOS)	Coloque a chave seletora na posição LIGADO para suspender o reenvio do aplicativo após o número definido de falhas na tentativa de reenvio, usando as configurações a seguir: **Parar reenvio após** – Informe após quantas tentativas de reenvio com falha o reenvio deve ser interrompido. Os valores informados devem estar dentro do intervalo de **1** a **999** **Tentativas com falha e tentar novamente após** – Informe quantas horas após a falha no reenvio ocorrerá a nova tentativa de reenvio. Os valores informados devem estar dentro do intervalo de **3** a **48** horas.
(Android somente) Instalar silenciosamente em dispositivos Samsung Knox	Esta opção não se aplica a apps públicos.

Configuração	O que fazer
(Somente iOS e macOS) Habilitar VPN por aplicativo para esse aplicativo	Selecione essa opção para usar uma configuração de VPN por aplicativo com esse aplicativo. Selecione a configuração VPN por aplicativo a ser utilizada na lista suspensa. Para o macOS, selecione apenas a configuração VPN por aplicativo do Tunnel.
(somente iOS) Impedir backup no iCloud e iTunes	Selecione essa opção para que o backup dos dados relacionados a esse aplicativo não seja feito no iCloud e no iTunes.
(somente iOS) Remover aplicativos em cancelamento de registro	Selecione esta opção para remover esse aplicativo quando o dispositivo não for mais gerenciado pelo Ivanti Neurons for MDM.
(somente iOS) AppConnect Configuração Personalizada	Para Aplicativos habilitados por AppConnect, insira as chaves e os valores que especificam suas preferências de configuração personalizada. Consulte a documentação do aplicativo para obter informações sobre as chaves disponíveis.
iOS 7+ Configurações de Aplicativos Gerenciados	Insira chaves e valores definidos para esse aplicativo como um aplicativo gerenciado iOS 7+. Consulte a documentação do aplicativo para obter informações sobre as chaves suportadas.

Os aplicativos do Android Enterprise terão opções diferentes.

c. Clique em **Avançar**

d. Selecione uma opção de promoção:

- Não qualificado
- Lista de qualificados
- Banner

e. Clique em **Concluído**.

Ao pesquisar um aplicativo do Windows no App Catalog, você pode buscar a correspondência mais próxima usando as opções **Nome do aplicativo** ou **ID da AppStore** na lista suspensa:

- **Nome do aplicativo** - selecione esta opção e forneça o nome do aplicativo
- **ID da AppStore** - selecione esta opção e forneça o ID da AppStore

A pesquisa por ID da AppStore não aceita aplicativos Win32 da loja (IDs de aplicativo começando com "X").

Adicionando um aplicativo interno

É possível carregar um aplicativo interno no catálogo de aplicativos com os seguintes formatos de arquivos. O upload de um arquivo grande pode demorar vários minutos. O número de versões de aplicativo interno é limitado a 100. Se esse número for excedido, o sistema Ivanti Neurons for MDM eliminará as versões mais antigas do aplicativo. O status de upload e eliminação do aplicativo é listado e está visível na página Trilhas de auditoria.

O inventário de apps MIP retornado pelo Mobile@Work pode estar incorreto para alguns apps. O Mobile@Work pode falhar em detectar o status de instalação de apps que não estão instalados em locais padrão. Para esses apps, adicionar um script de detecção ajudará a identificar o estado correto do aplicativo no dispositivo. O Mobile@Work determinará a presença do aplicativo se o código de saída do script de detecção for 0. Para quaisquer outros códigos de saída, o aplicativo será determinado como não instalado. Com base nos apps detectados, o Mobile@Work prepara o relatório de inventário para o dispositivo.

- IPA (iOS)
- MIP (aplicativo Packager para macOS)
- PKG (macOS)

- APK (Android)
- APPX, APPXBUNDLE, EXE e MSI (Windows)

Em aplicativos como PKG com scripts ou DMGs contendo PKG com scripts, o Mobile@Work para macOS detecta apenas solicitações de instalação bem-sucedidas. Ele não informará se o aplicativo foi excluído ou se os scripts que estavam instalados foram removidos. Portanto, o servidor Ivanti Neurons for MDM não poderá reenviar um comando de instalação. Se a conexão for interrompida durante o download dos apps, tente instalar o aplicativo novamente fazendo o registro. Para aplicativos MIP, mesmo se o aplicativo for removido do dispositivo instalado pelo PKG ou DMG, tendo o PKG o script incluso, o Mobile@Work não instalará o aplicativo MIP se a entrada do PKG existir na pasta de recibos do dispositivo cliente.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **Adicionar** (topo superior esquerdo).
3. Arraste o arquivo do aplicativo até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo em seu sistema e clique em **Confirmar**.
4. Clique em **Avançar** (inferior direito).

5. Descreva o aplicativo para os usuários e configure os apps de pré-requisito:

   a. Adicione categorias.

   b. Ao adicionar um pacote do macOS, se o arquivo de pacote contiver mais de um aplicativo (por exemplo, pacotes do Microsoft Office e Cisco AnyConnect), os apps primários selecionados serão usados para identificar que o pacote está instalado. O VPN por aplicativo, se configurado, será aplicado a esses apps.

   c. Insira uma descrição opcional.

   d. **Código do produto MSI**: ao carregar os apps MSI, o código do produto do aplicativo MSI é preenchido automaticamente neste campo.

   e. **URL de substituição:** insira a URL de uma fonte opcional para permitir o download do aplicativo de uma fonte diferente, ou para permitir a obtenção de arquivos grandes, como mídia de instalação do Microsoft Office, em uma rede local (HTTP e HTTPS). Esta opção exige acesso a uma rede interna segura e sincronização manual de um servidor alternativo em que os apps estejam armazenados. Não insira um valor a menos que você tenha estabelecido a infraestrutura necessária. Você pode editar esse valor ao editar as configurações do aplicativo específico.

      - Para apps iOS, os URLs de substituição do aplicativo devem estar somente nos formatos HTTP ou HTTPS.
      - Para apps Android e macOS, os URLs de substituição devem estar somente no formato HTTPS.
      - Para apps macOS, o URL deve terminar com a extensão, que é .pkg.

   f. **Linha de comando** (Apenas para apps MSI do Windows 32-bit): insira uma chave de linha de comando opcional para especificar informações adicionais que não fazem parte do pacote ao implantar os arquivos MSI. Por exemplo: para gravar registros de instalação em um arquivo de saída, é possível inserir "/log output.txt" neste campo. Isso criará o arquivo.txt de saída na pasta C:\Windows\System32. Por padrão, a opção /qn da linha de comando para instalação silenciosa é preenchida automaticamente durante o upload do aplicativo MSI.

O nome do pacote do aplicativo MSI a ser carregado não deve ser adicionado como parte dos argumentos da linha de comando. Se for adicionado, o upload ficará restrito até que o nome do pacote do aplicativo seja removido dos argumentos da linha de comando. Uma lista de todas as opções de linha de comando compatíveis é fornecida no link adicional. Este link estará visível no modo de visualização e edição do aplicativo.

g. Somente .EXE para Win32: instalados por meio do Bridge usando o modo Admin PowerShell. A funcionalidade Bridge será usada automaticamente, se disponível.

   - Atualizar a versão para manter a consistência entre a **Versão de exibição** e a **Versão do pacote**
   - Localização do instalador (.EXE)
   - Parâmetros de linha de comando do instalador: é obrigatório um argumento para executar o arquivo silenciosamente (por exemplo, /SILENT ou /VERY SILENT)
   - Execução do instalador como usuário: para instalar usando as credenciais do usuário, selecione a opção "Executar como usuário"

h. No caso de apps Packager para macOS, configure os aplicativos de pré-requisito (opcional). Consulte Compreensão dos aplicativos internos Packager para macOS para obter uma visão geral da funcionalidade do aplicativo de pré-requisito.

i. **URL de lançamento**: insira a URL personalizada para iniciar o aplicativo no AppStation. Necessário somente ao adicionar apps que não são AppConnect para distribuição em uma implantação somente MAM com AppStation e aplicável somente a apps iOS.

j. Configure a delegação de aplicativo.

Após delegar um aplicativo de pré-requisito e ele se tornar um aplicativo de requisito para o aplicativo do espaço que não é padrão, não será possível reverter a delegação do aplicativo a menos que você remova antes o relacionamento de pré-requisito.

k. Clique em **Avançar**.

l. Clique em **Avançar**.

6. (Opcional) Adicione capturas de tela do aplicativo.

7. (Opcional) Adicione ou substitua ícones para o aplicativo (aplicativos iOS, MacOS e Windows).

8. Clique em **Avançar**.

9. No caso de apps Packager para macOS, defina ou selecione os scripts de instalação que serão executados antes e/ou após a instalação do aplicativo. Selecione um ou ambos os scripts a seguir digitando na caixa de busca ou clicando no link para ver a lista de scripts. Clique em **Avançar**.

   - **Scripts pré-instalação** – Digite o nome do script que será executado antes da instalação do aplicativo. Os scripts pré-instalação serão executados ou haverá novas tentativas de execução até que o status de execução bem-sucedida seja recebido do cliente. O comando de instalação do aplicativo será enviado apenas depois disso. Você pode visualizar o status de execução do script na guia **Registros** da página de detalhes dispositivo.

   - **Scripts pós-instalação** – Digite o nome do script que será executado após a instalação do aplicativo.

   - **Desinstalar scripts**: insira o nome do script que o servidor envia para um dispositivo quando ele detectar que um aplicativo não é mais distribuído para o dispositivo.

   - **Scripts de detecção**: insira o nome do script que o servidor envia a um dispositivo para detectar o aplicativo. O resultado do script de detecção do aplicativo se sobrepõe ao resultado do inventário padrão do aplicativo no dispositivo. Independentemente de se o aplicativo é distribuído ao dispositivo ou não, o script de detecção de todos os apps será enviado ao dispositivo para avaliar a existência dos apps no dispositivo.

     Um script de detecção de amostra é mostrado abaixo:

     ```
     #!/bin/bash
     app_name="Name of the App"
     count="$(system_profiler SPApplicationsDataType | grep "$app_name" -c)"
     echo "$app_name count $count"
     if [ $count -ge 1 ]
     then
      echo "$app_name is installed"
     else
      echo "$app_name is not installed"
      exit 1
     fi
      exit 0
     ```

   Você pode criar os scripts na página **Administrador > Todos os scripts**. Ao fazer upgrade do aplicativo, você pode optar por copiar os scripts do aplicativo mais antigo e executá-los no aplicativo atualizado. Se você pular esta seção, poderá configurar scripts editando o aplicativo posteriormente.

10. Defina uma distribuição para o aplicativo:

a. Selecione uma opção de distribuição.

b. Expanda a seção **Opções avançadas e configuração do aplicativo**.

c. Use as diretrizes a seguir para concluir as opções:

Configuração	O que fazer
Instalar no dispositivo	Selecione essa opção para iniciar a instalação imediatamente após a inscrição. O usuário deverá confirmar a instalação do aplicativo, exceto sob as seguintes condições: • O dispositivo é um dispositivo iOS supervisionado. • O dispositivo é um dispositivo Samsung Knox e a opção de instalação silenciosa abaixo foi selecionada.
Não exibir o aplicativo no App Catalog do usuário final	Selecione essa opção caso não queira que o usuário veja o aplicativo no catálogo de aplicativos no dispositivo.

Definir prioridade de instalação de aplicativos	Selecione Alta, Média ou Baixa para definir a prioridade da instalação de aplicativos durante a integração do usuário. Apenas aplicativos de alta prioridade são instalados durante a integração do usuário.

Suspender reenvio de aplicativo após um número definido de tentativas com falha (somente iOS)	Coloque a chave seletora na posição LIGADO para suspender o reenvio do aplicativo após o número definido de falhas na tentativa de reenvio, usando as configurações a seguir: **Parar reenvio após** – Informe após quantas tentativas de reenvio com falha o reenvio deve ser interrompido. Os valores informados devem estar dentro do intervalo de **1** a **999** **Tentativas com falha e tentar novamente após** – Informe quantas horas após a falha no reenvio ocorrerá a nova tentativa de reenvio. Os valores informados devem estar dentro do intervalo de **3** a **48** horas.

(Android somente) Instalar silenciosamente em dispositivos Samsung Knox	Selecione essa opção caso não queira que seja solicitado ao usuário confirmar a instalação nos dispositivos Samsung Knox.
(Somente iOS e macOS) Habilitar VPN por aplicativo para esse aplicativo	Selecione essa opção para usar uma configuração de VPN por aplicativo com esse aplicativo. Selecione a configuração VPN por aplicativo a ser utilizada na lista suspensa. Para o macOS, selecione apenas a configuração VPN por aplicativo do Tunnel.
(somente iOS) Impedir backup no iCloud e iTunes	Selecione essa opção para que o backup dos dados relacionados a esse aplicativo não seja feito no iCloud e no iTunes.

(somente iOS) Remover aplicativos em cancelamento de registro	Selecione esta opção para remover esse aplicativo quando o dispositivo não for mais gerenciado pelo Ivanti Neurons for MDM.
(somente iOS) AppConnect Configuração Personalizada	Para Aplicativos habilitados por AppConnect, insira as chaves e os valores que especificam suas preferências de configuração personalizada. Consulte a documentação do aplicativo para obter informações sobre as chaves disponíveis.
iOS 7+ Configurações de Aplicativos Gerenciados	Insira chaves e valores definidos para esse aplicativo como um aplicativo gerenciado iOS 7+. Consulte a documentação do aplicativo para obter informações sobre as chaves suportadas.

d. Clique em **Avançar**.

11. Selecione uma opção de promoção:

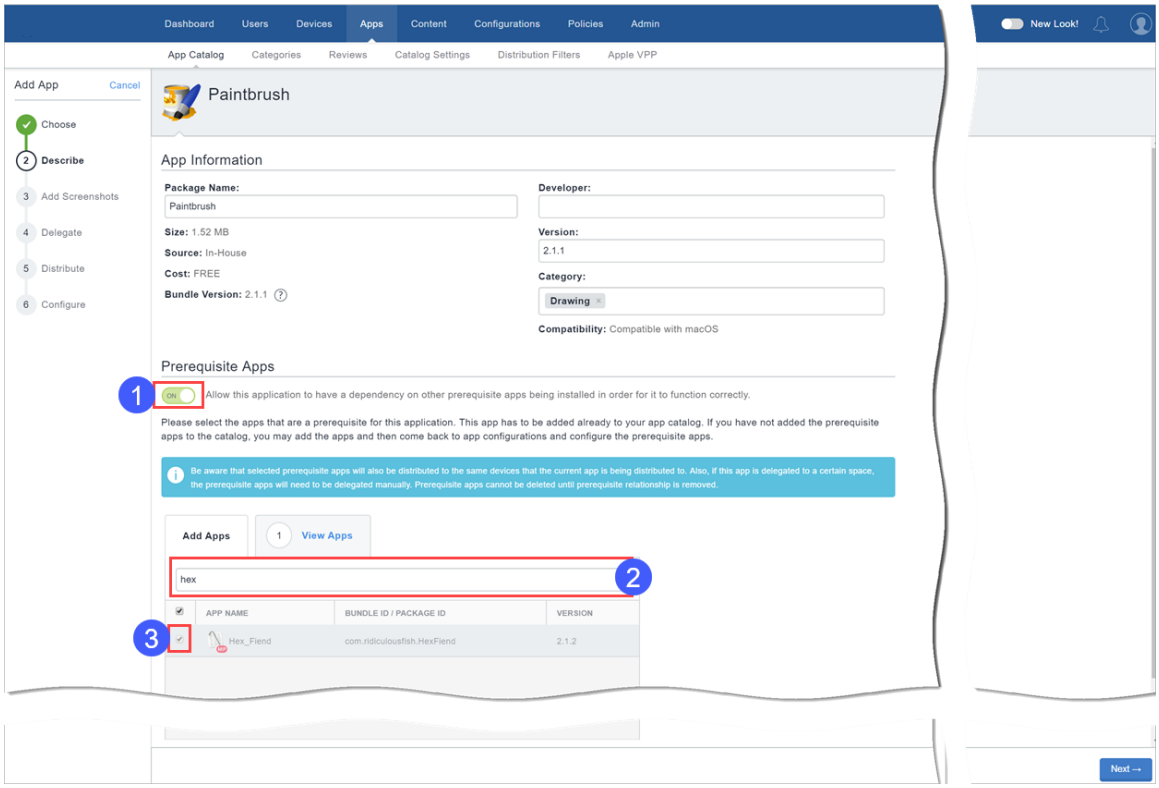
- Não qualificado
- Lista de qualificados

- Banner

12. Clique em **Concluído**.

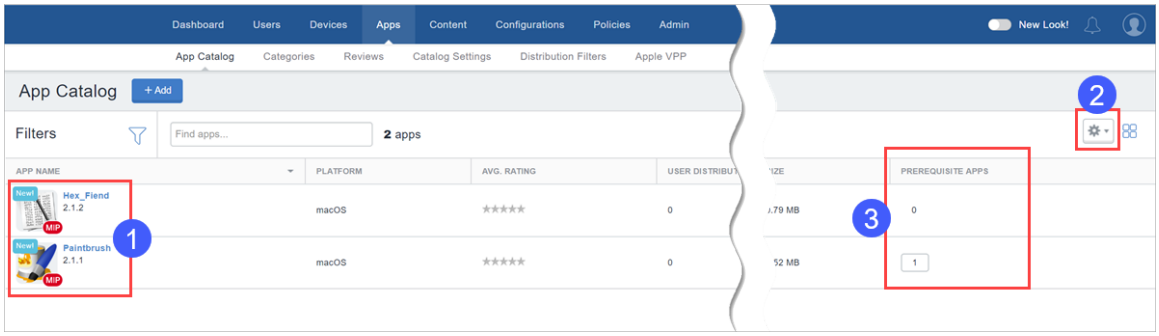
Compreensão dos apps internos Packager para macOS

Ao importar aplicativos internos Packager para macOS, o administrador pode ativar 1 o recurso Apps de pré-requisito para realizar uma busca 2 e selecionar 3 aplicativos de pré-requisito que devem ser instalados em clientes antes que o aplicativo que o administrador está importando possa ser instalado.



Uma vez importado, o aplicativo interno Packager para macOS aparecerá no App Catalog com o símbolo MIP exibido 1 abaixo. Você poderá então usar as configurações de coluna, 2, para adicionar a coluna APPS DE PRÉ-REQUISITO, 3, para ver rapidamente os apps com dependências, ou seja, que têm apps de pré-requisito.

- Você pode buscar e selecionar aplicativos MIP, não MIP e públicos (aplicativos Apps and Books e públicos da App Store no macOS) como aplicativos de pré-requisito.
- Os usuários precisam aceitar a licença do Apps and Books para que os aplicativos obrigatórios do Apps and Books sejam instalados silenciosamente.
- Para aplicativos pré-requisitos públicos não Apps and Books, os administradores precisam distribuir explicitamente os aplicativos públicos e o usuário precisa instalar os aplicativos públicos. Os aplicativos públicos (aplicativos Apps and Books e não Apps and Books) precisam ser importados para o App Catalog para que apareçam na lista de aplicativos de pré-requisito. A coluna Origem indica o tipo de aplicativo de pré-requisito.
- O registro MDM é necessário para instalar um aplicativo interno não MIP que possui apps de pré-requisitos não MIP.
- Os usuários precisam instalar manualmente aplicativos de pré-requisito públicos não Apps and Books.
- Se o token de Apps and Books for removido ou se a licença estiver esgotada, os aplicativos Apps and Books selecionados como aplicativos de pré-requisito e, desse modo, o aplicativo principal não será instalado. O administrador precisa seguir uma melhor prática para informar os usuários com antecedência sobre qualquer uma dessas circunstâncias para aplicativos Apps and Books.



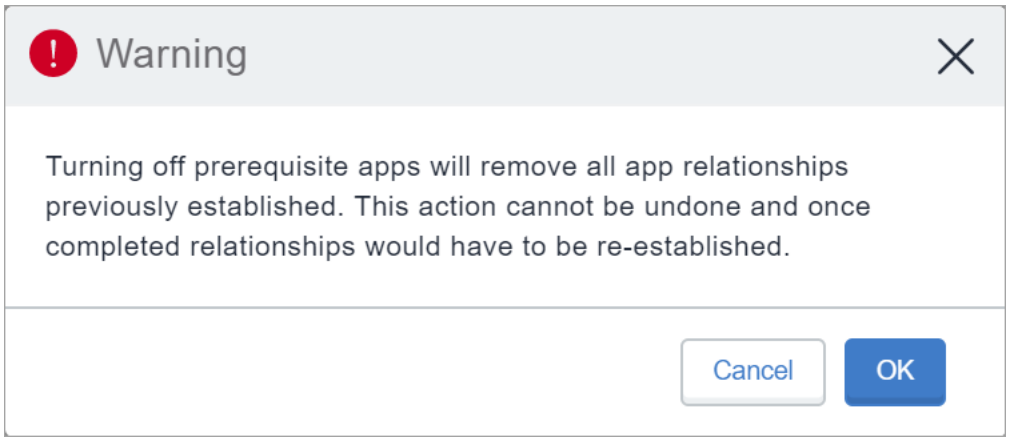
Os apps de pré-requisito também estão disponíveis como apps independentes para serem baixados pelo usuário quando distribuídos explicitamente. Se o usuário tentar desinstalar um aplicativo de pré-requisito:

- O próximo registro do dispositivo assegura que o aplicativo de pré-requisito seja instalado novamente.
- O aplicativo de pré-requisito será desinstalado se não houver apps principais dependentes no mesmo dispositivo.

- Se o aplicativo de pré-requisito não for explicitamente distribuído, o aplicativo de pré-requisito será desinstalado juntamente com o aplicativo principal.
- Se o aplicativo de pré-requisito for explicitamente distribuído, o aplicativo de pré-requisito permanecerá no dispositivo.
- Se o aplicativo de pré-requisito tiver um aplicativo dependente, o aplicativo de pré-requisito permanecerá no dispositivo.

Desativando o recurso apps de pré-requisitos

Ao interagir com apps com dependências e apps de pré-requisito e, por exemplo, atualizar, excluir ou deletar tais apps, você encontrará solicitações do sistema orientando sobre como o status de pré-requisito ou a dependência do aplicativo pode impactar as ações que você deseja executar. Por exemplo, quando você tentar desligar o recurso Apps de pré-requisito para um aplicativo, a seguinte solicitação aparece:



- Se você desativar o recurso Apps de pré-requisito para um aplicativo, os detalhes sobre os apps de pré-requisito serão apagados. Isso inclui a autorização e desautorização dos apps de pré-requisito dos subespaços.
- No Apps@Work, o botão de instalação não aparece para apps dependentes cujos apps de pré-requisito já não estejam instalados no cliente hospedado.
- Nos dispositivos de usuários, quando um usuário tenta instalar um aplicativo interno com dependências, os apps de pré-requisito serão instalados (se ainda não estiverem instalados) primeiramente seguidos pelo aplicativo principal, o que pode levar alguns minutos. A lista de apps dependentes é exibida para o usuário juntamente com o status de suas instalações.

Autorização e desautorização dos apps de pré-requisito dos espaços

- Os apps de pré-requisito vinculados a um aplicativo (aplicativo principal) são autorizados automaticamente quando o aplicativo principal é autorizado em um subespaço.
- Se o aplicativo principal estiver desautorizado em um subespaço, os apps de pré-requisito também são desautorizados nos locais que os apps não são distribuídos explicitamente. No entanto, os apps de pré-requisito que são vinculados a mais de um aplicativo principal não estão desautorizados.
- Se os apps de pré-requisito são autorizados explicitamente, então, eles não são desautorizados automaticamente.

Delegando permissões de dispositivo para aplicativos internos do Android Enterprise

É possível atribuir permissões delegadas a apps internos que podem ser aplicadas a dispositivos gerenciados do Android Enterprise.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. No **App Catalog**, selecione o aplicativo para o qual deseja delegar permissões de dispositivo.
3. Clique na guia **Configurações de aplicativo**.
4. Nas Permissões delegadas (aplicativo interno do Android corporativo), selecione as permissões necessárias para as seguintes ações nos aplicativos:

   Somente a implantação COSU usa AMAPI. Consulte a seção AMAPI para obter mais informações.

   - **Configurar permissões do tempo de execução de aplicativos de terceiros**
   - **Ocultar e suspender apps de terceiros**
   - **Gerenciar certificados**
   - **Gerenciar configurações de apps**
   - **Gerenciar desinstalação do aplicativo de bloqueio**
   - **Gerenciar a ativação de apps de sistema**
   - **Gerenciar seleção de certificado** (sem suporte no modo AMAPI)

- **Gerenciar retenção de apps desinstalados** (sem suporte no modo AMAPI)
- **Gerenciar coleção de registros de rede** (sem suporte no modo AMAPI)
- **Gerenciar coleção de registros de segurança** (sem suporte no modo AMAPI)
- **Gerenciar instalação de apps existentes** (sem suporte no modo AMAPI)
- **Instalar e remover pacotes** (sem suporte no modo AMAPI)

A opção de instalar e remover pacotes está disponível em todos os dispositivos compatíveis com o modo Proprietário do dispositivo Android (7.0 ou posterior). Outras permissões delegadas valem apenas para o Android 8.0 ou posterior.

5. Configure as opções de distribuição, selecionando **Todos com o aplicativo**, **Nenhum** ou **Personalizado**.
6. Clique em **Salvar**.

Exibindo o status do perfil de provisionamento para os apps internos do iOS

Exiba o status do perfil de provisionamento na página App Catalog para os apps internos do iOS. A dica de ferramenta ao lado do nome do perfil exibe o número de dias para a expiração do perfil. Esse status pode ser útil para verificar quando os perfis de provisionamento vão expirar para os apps internos.

O status é útil para a resolução de problemas de apps que não são instalados porque o perfil está expirado. Os apps seriam instalados, mas não abririam nem seriam inicializados se não houvesse um perfil de provisionamento adequado.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique no ícone de engrenagem no canto superior direito para exibir as colunas.
3. Selecione **Perfil de provisionamento** para exibir a coluna da lista de apps na página App Catalog.

Os detalhes do Perfil de provisionamento também estão disponíveis na página de detalhes do aplicativo na seção Configurações do perfil de provisionamento.

Atualizando o perfil de provisionamento para os apps internos do iOS

O perfil de provisionamento é aplicado a um aplicativo interno iOS específico. Os detalhes do perfil de provisionamento de um aplicativo estão disponíveis na página de detalhes do aplicativo. Para que um aplicativo interno do iOS seja iniciado no dispositivo, é necessário haver um perfil de provisionamento que não tenha expirado. Para atualizar um perfil de provisionamento caso tenha expirado, carregue o perfil na página de detalhes do aplicativo.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique no aplicativo cujo perfil de provisionamento é necessário atualizar. A página de detalhes do aplicativo é exibida.
3. Clique em **Editar**.
4. Na seção **Perfil de provisionamento**, clique em **Escolher arquivo**.
5. Selecione o arquivo de perfil de provisionamento para carregar (extensão de arquivo .mobileprovision) e clique em **Salvar**.

Implementar apps internos no Google Play

Faça upload de seus aplicativos internos no canal privado da Google Play e importe-os no Ivanti Neurons for MDM para implementação em dispositivos compatíveis com Android Enterprise.

Procedimento

1. Faça login no console de apps privados do Goople: https://play.google.com/apps/publish.
2. Clique em **Todos os apps** no menu à esquerda.
3. Clique em **Criar novos aplicativos** e insira um nome para o aplicativo.
4. Clique em **Carregar APK** para enviar o arquivo .apk que você gerou.

5. Clique em **Armazenar lista**:
    - Insira uma descrição breve e uma descrição completa.
    - Carregue uma captura de tela para todas as abas.
    - Carregue um ícone de alta resolução.
    - Carregue um ícone gráfico de recursos (gráfico.png)
    - Insira as informações necessárias para Categorização, detalhes de Contato e Política de privacidade.
    - Complete o questionário para classificar o aplicativo.
6. Clique em **Preço e distribuição**.
   Se todas as informações obrigatórias tiverem sido inseridas, a opção Pronto para publicar será exibida na parte superior da página.
7. Vá para a guia Aplicativos no Ivanti Neurons for MDM.
8. Clique em **Atualizar Catálogos disponíveis** para sincronizar os seus apps privados.

Pode levar horas para publicar o seu aplicativo.

Adicionando um aplicativo da Web para dispositivos Android Enterprise

Um aplicativo da Web é um link para um site que é instalado no dispositivo como um atalho. Os aplicativos da Web se comportam de maneira semelhante a qualquer outro aplicativo, o que significa que o aplicativo da Web pode ser distribuído da mesma forma que um aplicativo. Ele é exibido no App Catalog e pode ser instalado pelos usuários como qualquer outro aplicativo. No entanto, os aplicativos da Web podem ter apenas uma versão e não oferecem suporte para a instalação silenciosa. Os aplicativos da Web usam clipes da Web e são instalados no dispositivo como configurações, mas se comportam como aplicativos.

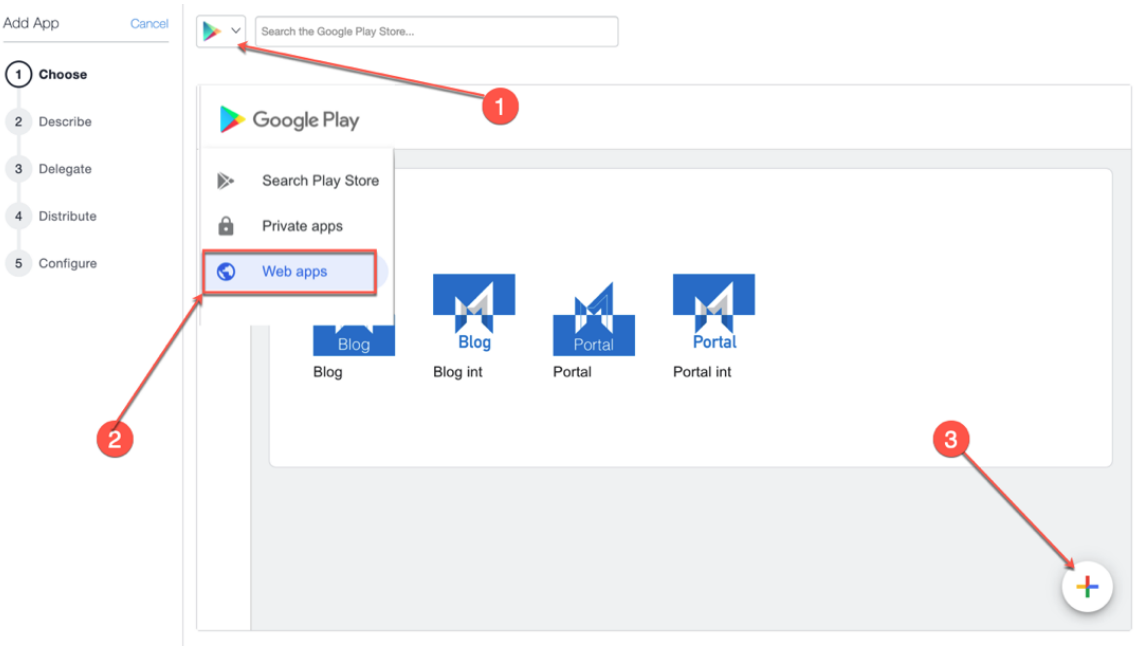
Configure um clipe da Web como um aplicativo no App Catalog para disponibilizar o aplicativo da Web no App Catalog para os usuários. O clipe da Web pode ser definido como uma configuração, mas uma configuração pode ser distribuída somente por um administrador. Os usuários podem optar por instalar o aplicativo da Web em seus dispositivos ou por não instalá-lo, mas os usuários não podem optar por não instalar a configuração de um clipe da Web.

No Android corporativo, um aplicativo da Web é um formulário incorporado de aplicativo da Web executado no Google Chrome dentro do Work Profile. Ele pode ser combinado com soluções VPN ou SSO no Android corporativo. Após a criação de um aplicativo da Web, ele funciona como qualquer outro aplicativo Android, que você pode distribuir conforme necessário. Os aplicativos da Web para que sejam executados requerem que o Chrome seja instalado no Work Profile do dispositivo de propriedade da empresa.

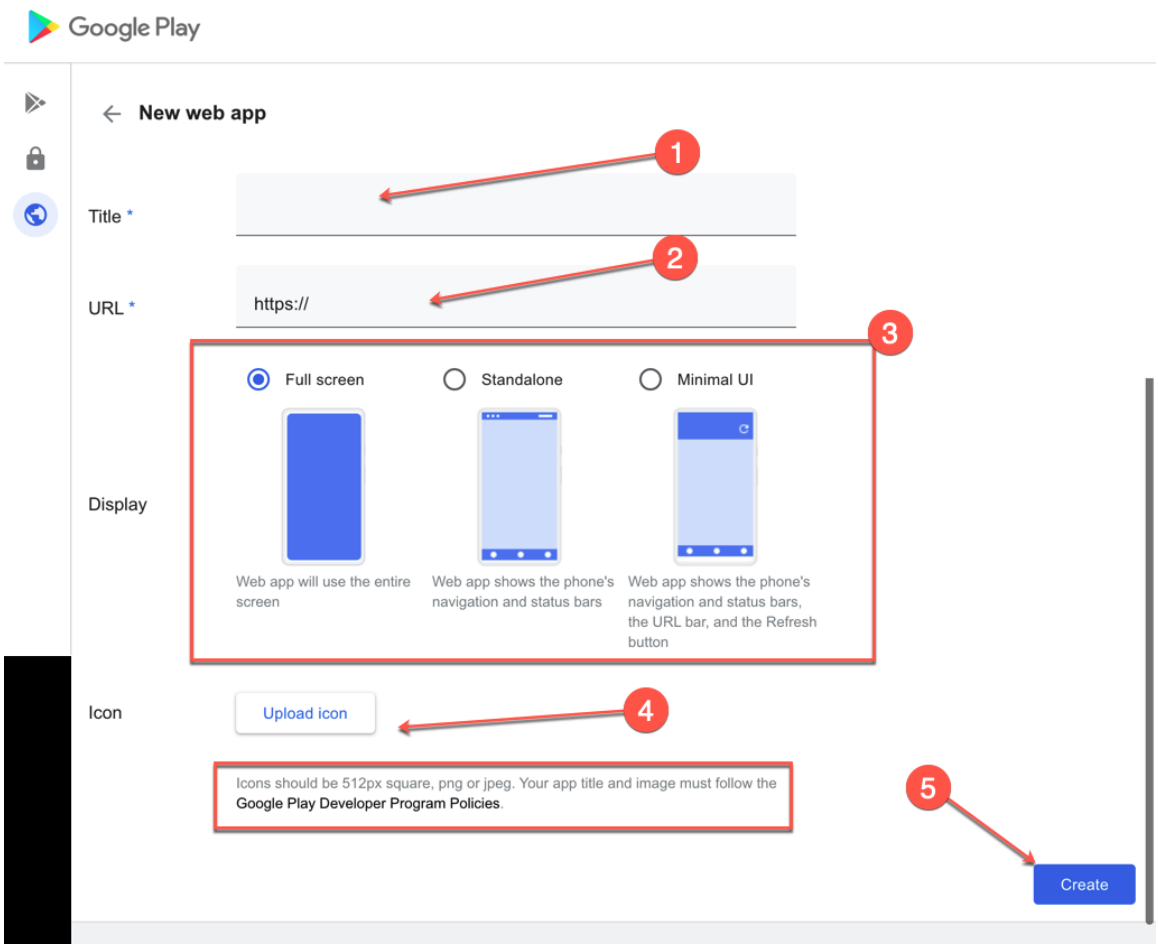
Se houver algum problema com o uso desse recurso, os administradores podem entrar em contato com o suporte.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **+ Adicionar** (canto superior esquerdo).
3. Selecione **Google Play** na lista suspensa para buscar um aplicativo no Google Play Store. O Google Play iFrame será exibido se o Android corporativo estiver registrado.
4. Clique em **Apps da Web**.



5. Descreva o aplicativo para os usuários:



   a. Nome ou título do aplicativo.

   b. URL do aplicativo.

   c. Tipo de exibição para o aplicativo da Web.

   d. Ícone de carregamento, que pode ser uma imagem PNG ou JPEG quadrada de 512 pixels.

6. Clique em **Criar**. Aguarde a publicação do aplicativo no iFrame. Isso pode demorar alguns minutos. Você pode fechar e retornar depois.

7. Após a publicação do aplicativo da Web, importe-o para o App Catalog para distribuição. Clique no ícone do aplicativo da Web.

8. Role para baixo e clique em **Selecionar**.
9. Adicione categorias e uma descrição opcional.
10. Clique em **Avançar**.
11. Selecione uma das opções a seguir para delegação do aplicativo:
    - Delegar este aplicativo a todos os espaços.
    - Não delegar este aplicativo a todos os espaços.
12. Clique em **Avançar**.
13. Selecione uma opção de distribuição para o aplicativo.
14. Clique em **Concluir**.

Após adicionar um aplicativo da Web, é possível editá-lo sempre que necessário. Para isso:

1. Na página **App Catalog**, clique no nome do aplicativo da Web existente.
2. Clique em **Editar** para editar os campos do aplicativo da Web.

Adicionando um aplicativo da Web em dispositivos com iOS

Um aplicativo da Web é um link para um site que é instalado no dispositivo como um atalho. Os aplicativos da Web se comportam de maneira semelhante a qualquer outro aplicativo, o que significa que o aplicativo da Web pode ser distribuído da mesma forma que um aplicativo. Ele é exibido no App Catalog e pode ser instalado pelos usuários como qualquer outro aplicativo. No entanto, os aplicativos da Web podem ter apenas uma versão e não oferecem suporte para a instalação silenciosa. Os aplicativos da Web usam clipes da Web e são instalados no dispositivo como configurações, mas se comportam como aplicativos.

Configure um clipe da Web como um aplicativo no App Catalog para disponibilizar o aplicativo da Web no App Catalog para os usuários. O clipe da Web pode ser definido como uma configuração, mas uma configuração pode ser distribuída somente por um administrador. Os usuários podem optar por instalar o aplicativo da Web em seus dispositivos ou por não instalá-lo, mas os usuários não podem optar por não instalar a configuração de um clipe da Web.

Se houver algum problema com o uso desse recurso, os administradores podem entrar em contato com o suporte.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **+ Adicionar** (canto superior esquerdo).
3. Clique em **Apps da Web**.
4. Descreva o aplicativo para os usuários:
    a. Nome do aplicativo.
    b. URL do aplicativo.
    c. Tipo de plataforma.
    d. Ícone do aplicativo.
    e. Adicione ou remova categorias.
    f. Tela inteira – Selecione para exibir o aplicativo da Web como um aplicativo de tela cheia.
    g. Removível – Selecione para permitir a remoção do aplicativo da Web.
    h. Clique em **Avançar**.
5. Selecione uma das opções a seguir para delegação do aplicativo:
    - Delegar este aplicativo a todos os espaços.
    - Não delegar este aplicativo a todos os espaços.
6. Clique em **Avançar**.
7. Selecione uma opção de distribuição para o aplicativo.
8. Clique em **Concluir**.

Editando um aplicativo web

Após adicionar um aplicativo da Web, é possível editá-lo sempre que necessário.

Procedimento

1. Na página **App Catalog**, clique no nome do aplicativo da Web existente.
2. Clique em **Editar** para editar os campos do aplicativo da Web.

Implantação lenta de aplicativos

A configuração de implantação lenta permite aos administradores implantar novas versões de aplicativos nos dispositivos de forma automática e gradual. A opção Usar método de distribuição de implementação lenta fica disponível quando você implementa a versão subsequente do aplicativo. O portal administrativo do Ivanti Neurons for MDM permite editar aplicativos mesmo quando a implementação lenta está pausada.

Depois que a implantação lenta for definida para uma versão, ela será aplicável às versões subsequentes com a mesma porcentagem definida na última vez. Você pode pausar a distribuição de um aplicativo se a distribuição estiver definida como 100%. No entanto, se você definir a meta de distribuição para 100%, deverá definir manualmente a porcentagem da meta de distribuição para a próxima versão, pois a interface do usuário redefine a porcentagem para 0%.

Procedimento

1. Vá até **App Catalog**, **Apps**, selecione uma das opções de modo de distribuição.
2. Selecione a opção **% personalizada de dispositivos no resumo da seleção (Implementação lenta)**.
3. Nas **configurações de implementação lenta**, arraste o controle deslizante para a **Especificar % de destino de distribuição**.
4. Clique em **Confirmar**, depois clique em **Concluído**. O status da versão mais recente do aplicativo é exibido. A página App Catalog indica o status IMPLANTAÇÃO LENTA na tabela.

Se você não conseguir executar tarefas na página do **App Catalog,** pode ser que você não tenha as permissões necessárias. Você precisa da função Gerenciamento de Aplicativo e Conteúdo.

Usando a pesquisa avançada

Você pode usar a opção Pesquisa avançada para pesquisar um aplicativo com base em regras, a fim de identificar e visualizar os aplicativos com critérios específicos. Essas regras podem ser construídas usando os operadores apropriados, como "igual", "é menor que", "é maior que", "é igual a" e "é diferente de". As opções de regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). Os aplicativos que atendam às regras são exibidos abaixo da seção.

Os valores dos atributos personalizados usados em Pesquisar diferenciam maiúsculas de minúsculas.

Procedimento

1. Na página App Catalog, clique no link **Pesquisa avançada**. O assistente Pesquisa Avançada é exibido.
2. Clique em uma das opções a seguir:

- **Qualquer**: os aplicativos precisam atender a pelo menos uma das regras
- **Todas**: os aplicativos precisam atender a todas as regras

3. Crie uma regra que defina os critérios de busca. **Exemplo**: Capacidade APNS igual a Sim.
4. (Opcional) Clique em **+** para criar regras adicionais.
5. Clique em **Pesquisar**. A lista dos aplicativos que correspondem os critérios de pesquisa é exibida.

Carregando as consultas de pesquisa

Você pode visualizar a lista das consultas de pesquisa salvas.

Procedimento

1. Clique em Pesquisa avançada e, em seguida, clique no ícone da pasta. A lista das consultas de pesquisa criadas é exibida na seção **Consulta carregada**, e os seguintes detalhes são exibidos.
   - **Nome da consulta** - O nome da consulta carregada.
   - **Conteúdo da consulta** - Exibe o conteúdo sobre as regras que definem a consulta de pesquisa.
   - **Ações** - Selecione a ação a ser executada na consulta.
2. Clique em **Carregar consulta** na coluna **Ações** para exibir a lista de aplicativos que correspondem aos critérios definidos na consulta carregada.
3. Clique em **Excluir** para excluir uma consulta carregada.

Tópicos relacionados

- "Funções do usuário" na página 142
- "Exclusão de apps do App Catalog" na página 382
- "Implantando dependências de aplicativo" na página 414

Apps@Work (iOS, Android, Windows e macOS)

O Apps@Work é uma vitrine de apps corporativos que facilita a distribuição segura de software e aplicativos. O Apps@work está disponível para dispositivos iOS, Android, macOS e Windows. A vitrine corporativa Apps@Work está integrada nos clientes Go app e Mobile@Work para iOS, Android e macOS. Para dispositivos Windows, é um aplicativo autônomo nativo. Esta seção contém os seguintes tópicos:

Apps@Work para iOS

A appstore nativa do Apps@work é implantada automaticamente com o cliente Go. Nenhuma ação do administrador é necessária. A guia Apps@work é exibida na barra de tarefas do cliente Go. O usuário final pode acessar essa guia para visualizar e instalar os aplicativos aprovados pela empresa. Para mais informações, consulte "Recursos da loja de aplicativos Apps@Work para iOS" na página 339.

As notificações de usuário final do Apps@Work iOS para atualizações de aplicativos ficam habilitadas por padrão. Se quiser mudar as configurações, consulte o tópico **Notificações** em "Configurações do catálogo" na página 409.

Clientes existentes com o Webclip Apps@Work para iOS

Clientes que tenham o antigo webclip do Apps@Work para iOS implantado não receberão o Catálogo de Aplicativos Integrado Nativo por padrão. Se você quiser fazer a transição para o catálogo nativo do Apps@Work para iOS e remover o webclip Apps@Work dos dispositivos, execute as seguintes etapas:

Enviar as configurações por push

O administrador deve enviar a configuração Catálogo de Aplicativos para Cliente Nativo aos dispositivos para disponibilizar o Apps@Work como uma experiência de appstore nativa a partir do aplicativo cliente Go. Para mais informações, consulte "Trabalhando com configurações" na página 445.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá para **Configurações** > Filtrar e selecione **Serviços do cliente**. Todas as configurações do cliente são listadas.
3. Selecione **Catálogo de aplicativos para cliente nativo**. A página de configuração Catálogo de Aplicativos para Cliente Nativo é aberta.
4. Clique no ícone **Editar distribuição**. A página Editar Distribuição é aberta.
5. Selecione uma das opções a seguir:
   - **Todos os dispositivos**
   - **Nenhum dispositivo** - se não quiser distribuir a nenhum dispositivo
   - **Personalizada** - permite selecionar dispositivos, grupos de dispositivos, usuários e grupos de usuários
6. Após a distribuição da configuração, o usuário deve atualizar a versão do cliente Go para 83 ou superior. A guia Apps@Work agora está visível no cliente Go app.

> A configuração não pode ser enviada a dispositivos registrados usando iReg porque o cliente Go não está disponível no dispositivo. Você deve instalar o cliente Go app para receber o catálogo de aplicativos nativo. Para mais informações, consulte "Registro de dispositivo (iOS, macOS e Android)" na página 222.

Remover Webclip do Apps@Work para iOS

Os usuários que receberam o Webclip Apps@Work e já migraram para a experiência nativa do Apps@Work podem remover o webclip do Apps@Work para iOS.

Procedimento

1. Vá até **Configurações**.
2. Filtre a Configuração – **Catálogo de Aplicativos Apple**.
3. Clique em **Editar**.
4. Em **Distribuição** selecione **Distribuição para nenhum dispositivo**.
5. Clique em **Salvar**.

Apps@Work para Android

A appstore nativa do Apps@work é implantada automaticamente com o cliente MI Go. Nenhuma ação do administrador é necessária. A guia Apps@work é exibida na barra de tarefas do cliente Mi Go. O usuário final pode acessar essa guia para visualizar e instalar os aplicativos aprovados pela empresa. Para mais informações, consulte "Administrador – Android Enterprise" na página 1403.

macOS Apps@Work

O Apps@work para macOS está integrado ao cliente macOS M@W. Depois que o dispositivo for registrado no Ivanti Neurons for MDM, o cliente será exibido como Apps@Work. Para locatários recém-criados, a configuração do Webclip Catálogo de Aplicativos Apple não será enviada ao dispositivos macOS. Se necessário, o administrador pode distribuir a configuração do Webclip Apps@work aos dispositivos macOS. Para obter mais informações, consulte "Configurar dispositivos macOS" na página 20.

Distribuir apps macOS

- A Ivanti oferece suporte à distribuição de aplicativos macOS por meio do protocolo Apple MDM e usando o aplicativo Mobile@Work. Os administradores podem escolher usar uma ou ambas as seguintes abordagens:
  - Protocolo MDM da Apple – Os administradores podem carregar apenas formatos PKG específicos (formato de distribuição) como apps internos e também podem distribuir a partir da Mac App Store (o suporte a licença de Apps e Books da Apple é incluído). No entanto, essa abordagem não permite que os administradores distribuam DMG e outros formatos PKG.
  - Aplicativo Mobile@Work para macOS - como uma maneira de distribuir apps a usuários, os administradores podem usar o aplicativo MobileIron Packager (MIP) para converter qualquer arquivo PKG, DMG ou .app em um arquivo MIP. Carregue o arquivo MIP no Ivanti Neurons for MDM como um aplicativo interno
- Você pode baixar o utilitário a partir do site de downloads de software.
- Os administradores podem usar o Mobile@Work para distribuir apps internos que estejam no formato DMG, PKG ou .app. Para apps que estejam disponíveis apenas na Mac App Store, os administradores podem continuar usando recursos de MDM nativos da Apple, o que inclui recursos de licença de Apple Apps e Books. Para obter mais informações, consulte "Configurar dispositivos macOS" na página 20.

Apps@Work para Windows

O Apps@Work é um aplicativo nativo autônomo que pode ser baixado da Microsoft Store ou ser enviado diretamente a partir do Ivanti Neurons for MDM. Ele possibilita o uso de aplicativos públicos e internos do Windows em dispositivos Windows 10 no Ivanti Neurons for MDM. O Apps@Work é instalado silenciosamente nos dispositivos Windows 10 compatíveis. Para obter mais informações, consulte "Configuração do aplicativo" na página 354.

Usando o Apps@Work para Windows

O Apps@Work possibilita o uso de aplicativos públicos e internos do Windows em dispositivos Windows 10 no Ivanti Neurons for MDM. O Apps@Work é instalado silenciosamente nos dispositivos Windows 10 compatíveis.

Autenticação de certificado do Apps@Work

Para usar a autenticação de certificado com o Apps@Work para Windows:

1. Vá para **Administrador > Windows > Autenticação de Certificado do Apps@Work**.
2. Alterne a configuração para **ATIVADO**.

   Alternar a configuração para **DESATIVADO** obriga o uso de nome de usuário e senha.

O SAML não é compatível com o Apps@Work para Windows.

Para configurar um aplicativo do Apps@Work:

1. Selecione um aplicativo do Windows.
2. Clique na guia **Configuração de aplicativo**.
3. Clique em **Instalar no dispositivo**.
   A configuração do aplicativo interno do Windows pode ser definida para instalação silenciosa ou instalação pelo Apps@Work. Apps públicos não podem ser definidos para instalação silenciosa.
4. Também é possível optar por exibir ou ocultar os apps no catálogo do Apps@Work.
   Esta opção diz respeito somente a apps internos.

5. Clique na guia **Promoção**.

> O Apps@Work atualmente não suporta promoção de banner, então as opções disponíveis são **Em destaque** e **Sem destaque**.
> Apenas a opção **Promoção** é exibida para aplicativos públicos.

Recursos da loja de aplicativos Apps@Work para iOS

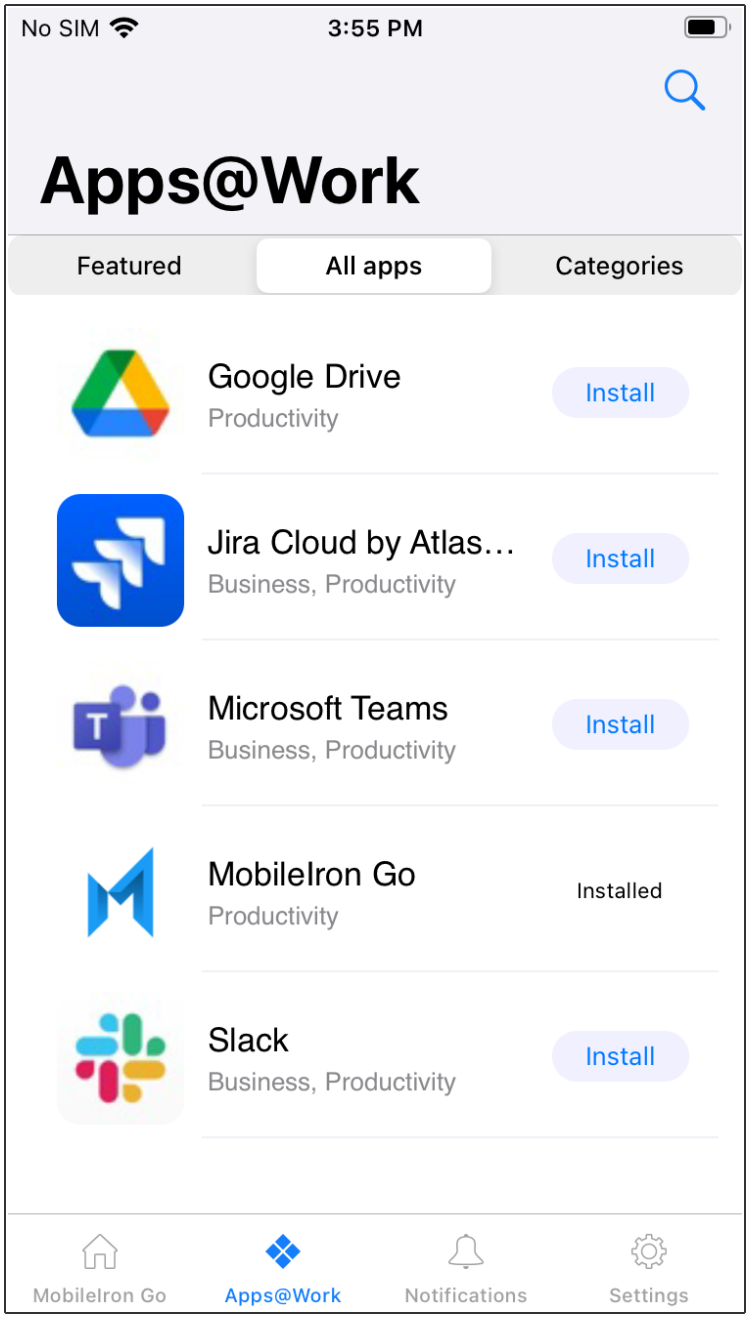
A guia Apps@Work tem os seguintes recursos:

- " Acesse a guia Apps@Work no aplicativo Go" abaixo
- "Pesquisar" na página 341
- " Instalando um aplicativo - estados de botão" na página 343
- "Aplicativos e banner em destaque" na página 347
- "Notificação de atualização de aplicativo" na página 349
- "Configurações - Meus Dispositivos" na página 349

Acesse a guia Apps@Work no aplicativo Go

Procedimento

1. Faça login no Go app em seu dispositivo iOS.
2. Toque no ícone **Apps@Work**. Duas guias padrão estão disponíveis: Todos os aplicativos e Categorias.



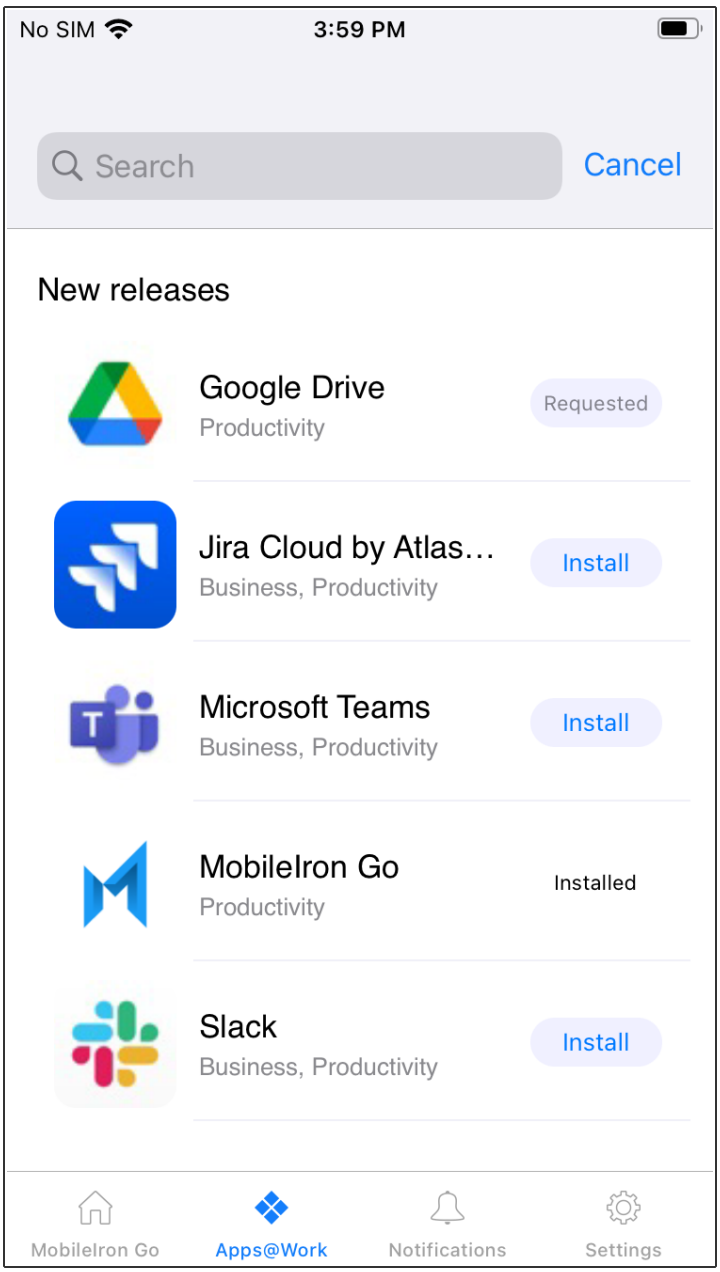
3. Toque na guia **Todos os aplicativos**. A guia Todos os aplicativos lista todos os aplicativos em ordem alfabética.
4. Toque na guia **Categorias**. A guia Categorias exibe apenas as categorias que possuem aplicativos, da seguinte forma:
    - Cada categoria exibe o número de aplicativos presentes nela.
    - A linha MyApps na guia Categorias é um item de lista que contém todos os aplicativos instalados. A linha MyApps será sempre a primeira categoria, e as demais categorias estarão listadas em ordem alfabética.
    - Quando nenhum aplicativo está instalado, a lista MyApps exibe Nenhum.
    - Quando você clica em uma categoria, todos os aplicativos específicos dela são listados com a opção Instalar. Clique em **Instalar** para instalar cada aplicativo individualmente; ou em **Instalar tudo** para instalar todos os aplicativos da categoria. Você será solicitado a permitir a instalação de cada aplicativo.

Pesquisar

Procedimento

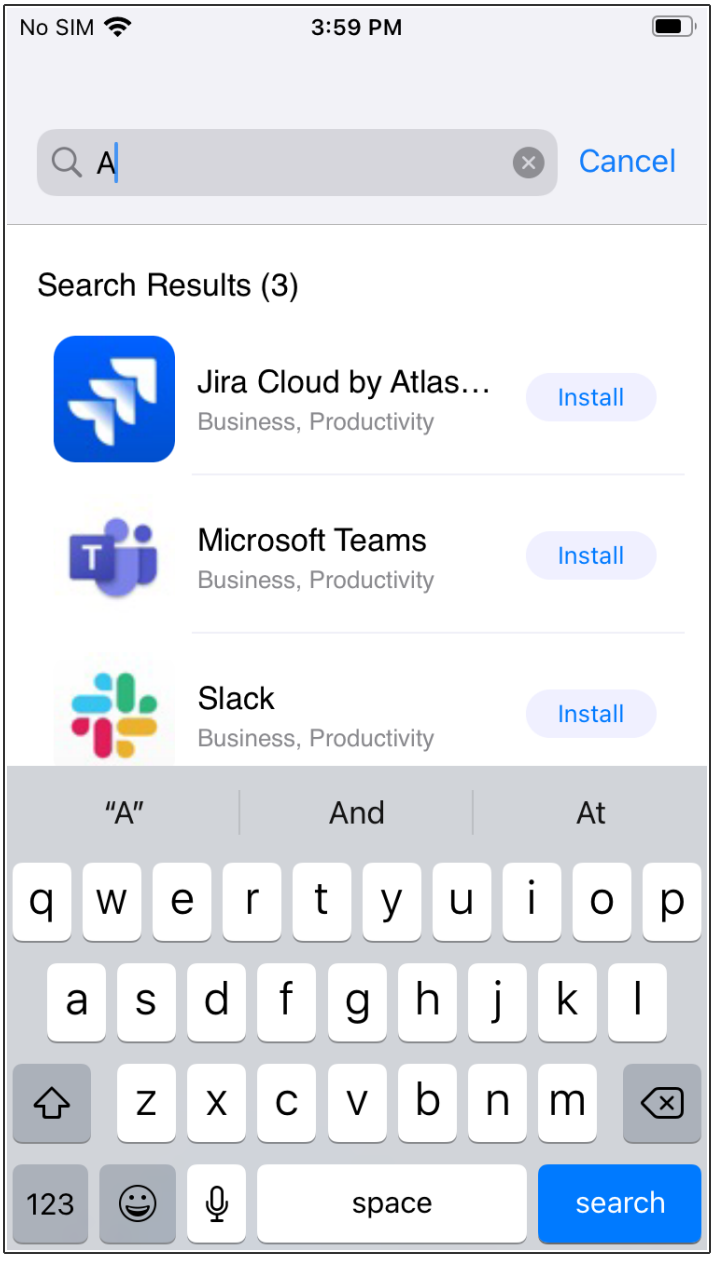
1. Faça login no Go app em seu dispositivo iOS.
2. Toque no ícone **Apps@Work**.
3. Toque no ícone de pesquisa (lente) para pesquisar o seguinte:

- **Novos lançamentos:** uma lista de aplicativos recém-lançados aparece se nenhum texto é digitado na barra de pesquisa



- Digite algum texto, e o campo de pesquisa irá prever e exibir dinamicamente os aplicativos correspondentes.
- A contagem de resultados da pesquisa é exibida como subtítulo

- Você também pode tocar no botão **Instalar** para instalar um aplicativo sem navegar até a página de detalhes.



Instalando um aplicativo - estados de botão

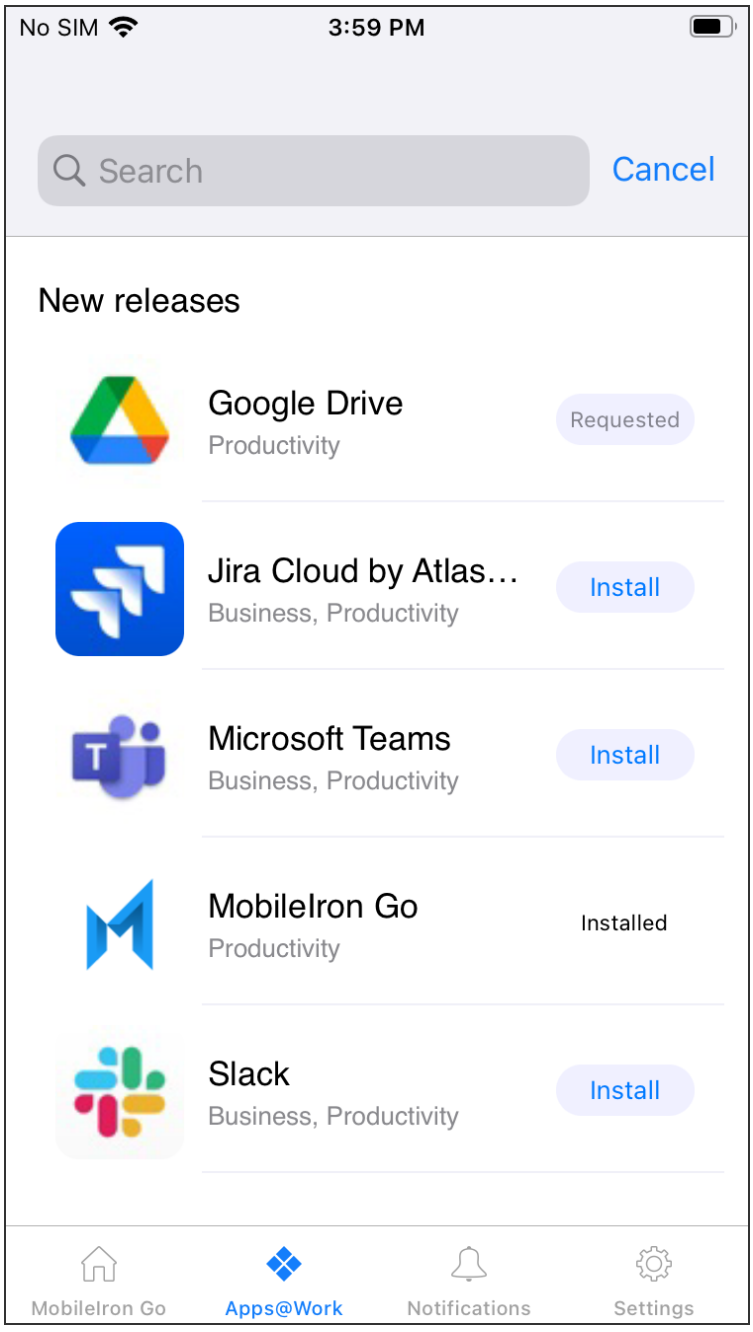
Como a instalação do aplicativo exige que o servidor processe a solicitação e envie o aplicativo ao dispositivo, o botão de instalação não exibirá o progresso em tempo real. O botão de instalação percorre os estados Instalar > Solicitado > Instalado.

Procedimento

1. Faça login no Go app em seu dispositivo iOS.
2. Toque no ícone **Apps@Work**.

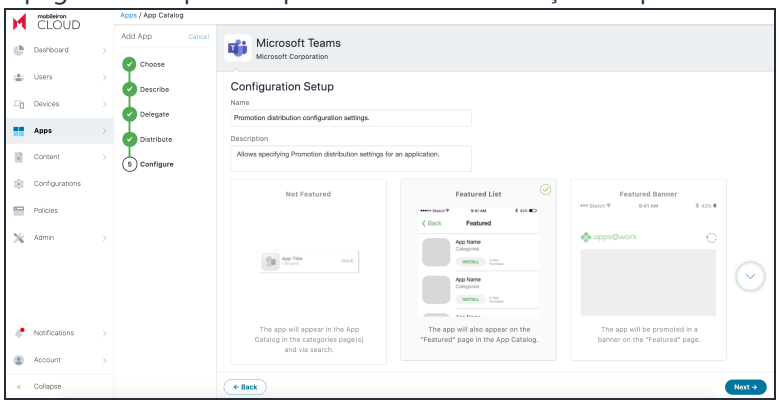
3. Toque em **Instalar**, e as notificações de status aparecem da seguinte forma:
    - Primeiro, aparece uma mensagem de alerta indicando que uma instalação foi solicitada.
    - Toque no botão Solicitado. Uma mensagem de alerta é exibida.

    O status Instalado não é um botão.



Aplicativos e banner em destaque

A guia Em destaque fica visível com base na configuração enviada pelo administrador. A guia Em destaque é a página inicial padrão quando não há atualizações disponíveis.

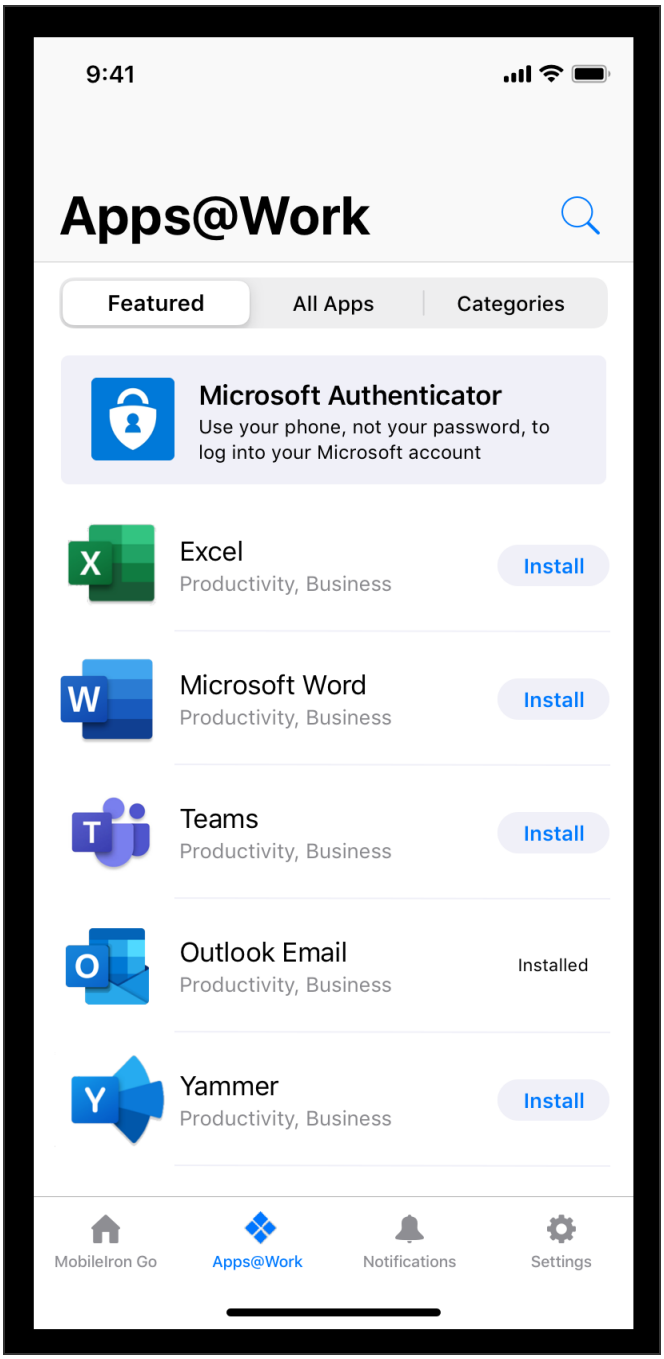


Procedimento

1. Faça login no Go app em seu dispositivo iOS.
2. Toque no ícone **Apps@Work**.

3. Toque na guia **Em destaque**.

   - O Banner de Aplicativo em Destaque exibe um aplicativo no banner.
   - Aplicativo em Destaque contém uma lista de todos os aplicativos em destaque.

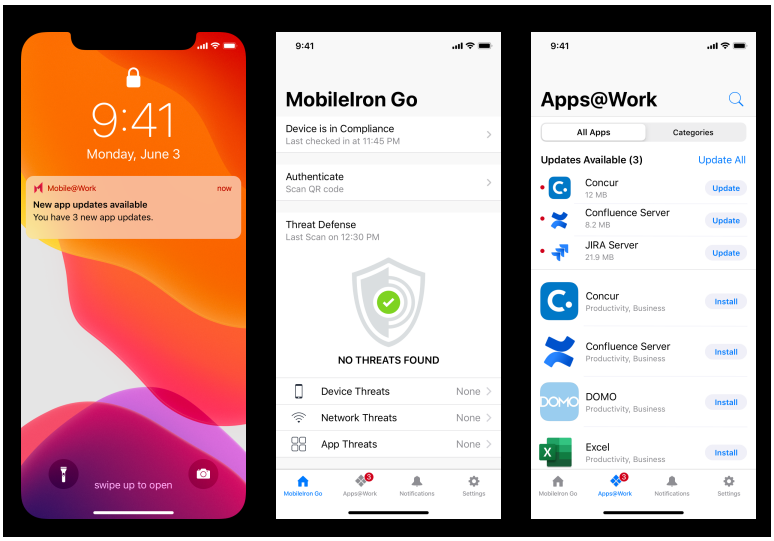


Notificação de atualização de aplicativo

O usuário final é notificado no dispositivo quando há alguma atualização de aplicativo disponível. A notificação contém o número de aplicativos que possuem atualizações disponíveis. Quando o usuário clica na notificação, o Apps@Work é aberto.

Procedimento

1. Faça login no Go app em seu dispositivo iOS. O ícone Apps@Work exibe a contagem de aplicativos com atualizações pendentes.
2. Toque na notificação de atualização de aplicativo; você será redirecionado para a guia Todos os aplicativos no Apps@Work. As seguintes indicações são exibidas:
   - A subseção Atualizações Disponíveis na guia Todos os Aplicativos exibe a contagem dos aplicativos que estão disponíveis para atualização.
   - Um ícone de ponto vermelho é exibido para cada aplicativo que requer atualização.



Configurações - Meus Dispositivos

Procedimento

1. Faça login no Go app em seu dispositivo iOS.
2. Toque no ícone **Configurações**.
    - A guia Meus Dispositivos está disponível em Configurações.
    - Meus Dispositivos agora está listado como um item de linha em Autenticar.

Visualizando detalhes do aplicativo

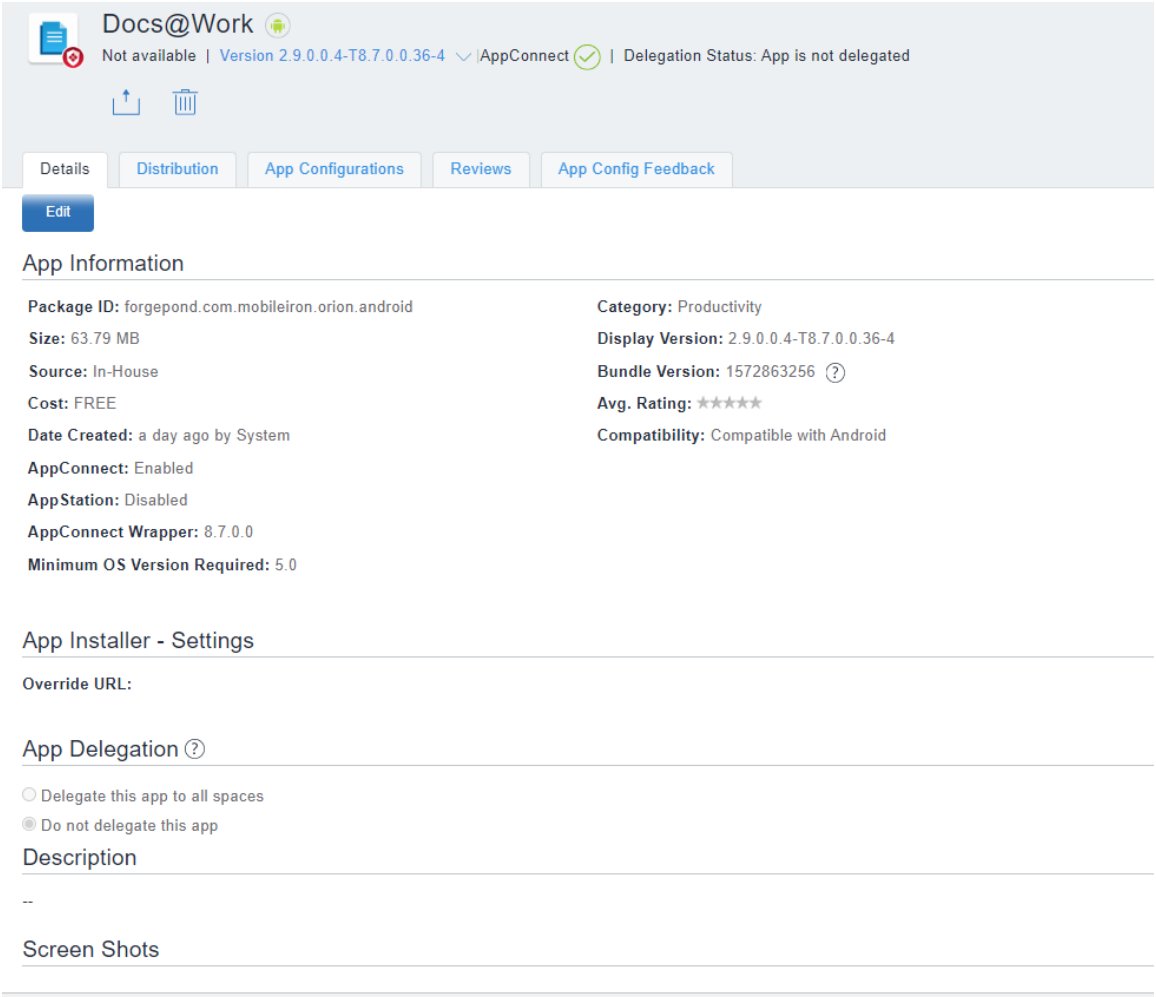
É possível fazer uma busca detalhada no App Catalog até os detalhes do aplicativo sobre qualquer um dos apps do catálogo. Na página de detalhes do aplicativo, são exibidos detalhes como Versão de display (por exemplo, 1.5.0), Versão do pacote (por exemplo, 1.5.0.42) e Versão mínima do SO exigida (por exemplo, 5.0 para Android).

Aplicativos que não atendem à versão especificada no campo de Versão mínima do SO exigida não são exibidos no catálogo Apps@Work. Portanto, esses apps não estão disponíveis para ser distribuídos aos dispositivos. O campo de Versão mínima do SO exigida também é exibido como parte das Trilhas de auditoria para os aplicativos.

Procedimento

1. Clique em **Apps**.
2. Clique em **Catálogo de aplicativos**.
3. Selecione o aplicativo.

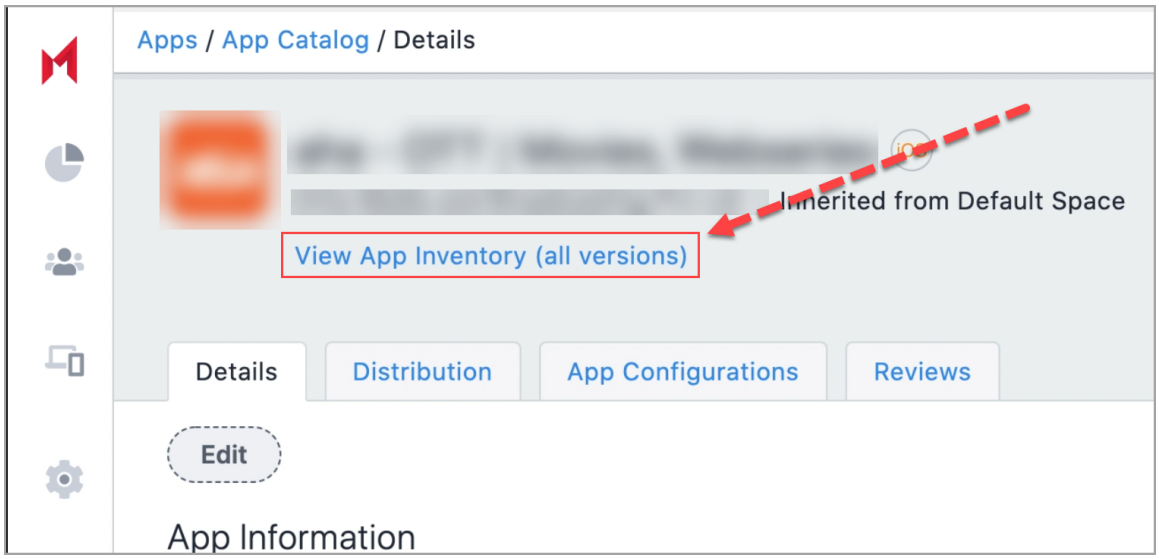
   A janela Detalhes do Aplicativo é exibida. Uma janela de amostra para sua referência:



- Para apps internos do iOS, é possível verificar a **Data de expiração do perfil de provisionamento** na página de detalhes do aplicativo.
- Informações do aplicativo mostram **Permitir instalação do aplicativo em dispositivos M1 na distribuição** como uma opção para todos os apps VPP do iOS e do iPadOS. O administrador deve habilitar a opção **Permitir instalação do aplicativo em dispositivos M1 na distribuição** somente para apps VPP do iOS ou do iPad que possam ser instalados em dispositivo macOS M1. Somente após habilitar essa opção é que o administrador poderá ver os dispositivos macOS M1 durante a instalação do aplicativo. A configuração de aplicativo gerenciado é compatível com aplicativos VPP do iOS em dispositivos Mac M1.
- Um botão de alternância para **Apps de pré-requisito** é adicionado em Detalhes do dispositivo. Os administradores podem selecionar essa opção e adicionar apps como pré-requisitos de um aplicativo principal.

Visualizando informações de inventário do aplicativo na página de detalhes do aplicativo

Para exibir informações do inventário de aplicativos, clique em **Exibir inventário de aplicativos (todas as versões)** para ver em **Dispositivos > Inventário de aplicativos** uma lista filtrada pelo ID de pacote desse aplicativo.



Configuração do aplicativo

Esta seção contém os seguintes tópicos:

A configuração do aplicativo permite personalizar a instalação, a promoção e a distribuição de cada aplicativo que você implementa nos dispositivos de seus usuários. Os aplicativos podem ser seus próprios aplicativos internos, de uma loja pública ou do Ivanti Neurons for MDM. Você tem a flexibilidade de implementar os apps para vários usuários e grupos diferentes, com nomes e configurações exclusivos personalizados especificamente para cada destinatário. O número de versões de aplicativo interno é limitado a 100. Se esse número for excedido, o sistema Ivanti Neurons for MDM eliminará as versões mais antigas do aplicativo. O status de upload e eliminação do aplicativo é listado e está visível na página Trilhas de auditoria.

Quando você altera os valores para a configuração do aplicativo de um aplicativo no app catalog ou no perfil de configuração do aplicativo gerenciado. São necessários um ou dois registros de dispositivo para receber os novos valores de configuração.

Licenciamento de recursos do aplicativo

Os seguintes recursos requerem licença adicional:

- Instalação/desinstalação silenciosa de aplicativos:Silver licença
- Configuração por aplicativo: Gold licença
- Configuração personalizada do AppConnect: Licença Gold

Para ter vários pacotes de aplicativo, é necessário gerenciar bem o grupo, pois o SO do Windows não poderá definir os tipos de dispositivos no futuro. Nesse caso, a única maneira de instalar a versão correta do aplicativo é se o administrador usar o grupo correto para o aplicativo correto.

Etapas de configuração comuns a vários apps

Conclua estas etapas primeiro e, em seguida, prossiga com as etapas de configuração para cada aplicativo que você deseja implementar. É possível projetar várias configurações do mesmo aplicativo e dar a cada uma um nome exclusivo. Cada configuração pode ter seus próprios níveis de distribuição e promoção de acordo com a estratégia de implementação. O número de versões de aplicativo interno é limitado a 100. Se esse número for excedido, o sistema Ivanti Neurons for MDM eliminará as versões mais antigas do aplicativo. O status de upload e eliminação do aplicativo é listado e está visível na página Trilhas de auditoria. Você pode implementar um aplicativo para no máximo 100 usuários, Grupo de usuários, Dispositivos ou Grupo de dispositivos de uma só vez. Você pode selecionar um aplicativo para adicionar ao catálogo de aplicativos. Ivanti Neurons for MDM tem um processo assíncrono para enviar o comando de solicitação de instalação/atualização de aplicativos iOS. Quando você usa o comando Enviar solicitação de instalação/atualização, o portal administrativo do Ivanti Neurons for MDM exibe uma mensagem informando que:

- o processo continuará a ser executado em segundo plano
- o processo está concluído
- status: se o processo foi bem-sucedido ou ocorreu algum erro

Procedimento

1. Acesse **Apps > Catálogo de apps** e clique em **+Adicionar**.
2. Use o menu suspenso para selecionar a App Store, o Google Play ou sua própria loja interna de aplicativos, e escolha um aplicativo para adicionar ao catálogo.
   Dependendo do seu acordo de licença, aplicativos também podem estar disponíveis para inclusão em seu catálogo.
3. Como opção, edite a categoria do aplicativo.
4. Como opção, adicione uma breve descrição do aplicativo no campo **Descrição**.
5. Clique em **Avançar**.

6. Escolha um nível de distribuição para esta configuração do aplicativo:
    - **Para todos** – O aplicativo é adicionado a todos os dispositivos de usuário compatíveis.
    - **Para ninguém** – O aplicativo é preparado para distribuição posteriormente.
    - **Distribuição personalizada** – Selecione qualquer uma das opções a seguir:
        - **Usuário/Grupos de usuários** – O aplicativo é distribuído apenas para os usuários ou grupos de usuários que você escolher.
          Clique na guia **Usuários** para selecionar os usuários.
          Clique na guia **Grupos de usuários** para selecionar os grupos de usuários.
        - **Dispositivo/Grupos de dispositivos** – O aplicativo é distribuído apenas para os dispositivos ou grupos de dispositivos que você escolher
          Clique na guia **Dispositivos** para selecionar os dispositivos.
          Clique na guia **Grupos de dispositivos** para selecionar os grupos de dispositivos.
7. Clique em **Avançar**.

Como configurar opções de instalação

Você pode selecionar as opções da configuração de instalação.

Procedimento

1. Clique em **Instalar definições de configuração do aplicativo** ou clique no ícone **+** para adicionar outra configuração para exibir a página **Definição da configuração**.
2. Insira um nome para a configuração no campo **Nome**.
3. Como opção, insira uma breve descrição da configuração de instalação no campo **Descrição**.
4. Selecione a opção **Configurações de instalação do dispositivo**.
5. Selecione uma das opções a seguir:
    - **Requer instalação no dispositivo**
    - **Instalar apenas uma vez no registro do dispositivo**

6. Selecione as seguintes opções:
   - **Instalar silenciosamente em dispositivos com área de trabalho Samsung Knox e Zebra** (somente Android)
   - **Não exibir o aplicativo no catálogo de aplicativos do usuário final**.
   - **Modo de atualização de aplicativo** (compatível também com dispositivos AMAPI). (Somente Android)
     Use esta opção para atualizar um aplicativo para a versão mais recente usando um dos três modos a seguir:
     - **Padrão:** este modo é selecionado quando você seleciona a opção Modo de atualização de aplicativo. Neste modo, a atualização ocorre dentro de 24 horas a partir do momento da disponibilidade do aplicativo.
     - **Adiar por 90 dias:** se você selecionar este modo de atualização, poderá adiar as atualizações do aplicativo por 90 dias. Após 90 dias, os apps são atualizados automaticamente com base em outras configurações feitas na configuração do Managed Google Play.
     - **Alta prioridade:** se você selecionar este modo de atualização e o dispositivo do usuário estiver on-line, o aplicativo será atualizado imediatamente após ser disponibilizado na Google Play Store.
   - **Definir prioridade de instalação do aplicativo** - consulte o tópico Configurando a prioridade do aplicativo para obter mais detalhes:
7. Você pode encontrar opções de configuração adicionais, dependendo do aplicativo selecionado. Essas opções podem incluir a capacidade de adicionar diversos pares de Chave e Valor. Nesses casos, clique em **+ Adicionar** para inserir pares de chave e valor. Para mais informações, consulte **Adicionando um aplicativo de uma loja pública** no "App Catalog" na página 301.
8. (macOS 11+) Selecione as opções para instalar e configurar os aplicativos como aplicativos gerenciados:
   - **Instalar como aplicativo gerenciado**
   - **Converter para aplicativo gerenciado**

> No macOS 12.0+, o suporte para aplicativo gerenciado está disponível para dispositivos registrados do usuário.

Configurando a prioridade do aplicativo

Você pode definir a ordem em que os aplicativos são recebidos no dispositivo quando ele é registrado pela primeira vez (especificamente, dentro dos primeiros 20 minutos após a data e hora de registro) e os aplicativos necessários estão sendo instalados. Você pode priorizar o download de aplicativos específicos antes de outros aplicativos. Por exemplo, priorizar o download de aplicativos Tunnel e E-mail antes de outros aplicativos não críticos. Esta funcionalidade é aplicável a aplicativos públicos e privados. Os aplicativos obrigatórios são passados na frente dos aplicativos dependentes.

Esse recurso é suportado em dispositivos iOS (exceto AppStation para iOS), Android (exceto Android corporativo), MacOS (aplicativos PKG internos e aplicativos Apple Apps e Books) e Windows.

Esse recurso está disponível para dispositivos de registro. Por padrão, todos os aplicativos são definidos para prioridade Média. Durante esse processo, o usuário pode optar por instalar manualmente qualquer aplicativo do catálogo, mesmo que tal aplicativo concorra por recursos na instalação e possa entrar na fila antes de aplicativos de alta prioridade.

No caso de aplicativos do Windows, o aplicativo Bridge tem a prioridade mais alta que a de todos os outros aplicativos.

Veja a seção anterior, "Configurando opções de instalação" para o procedimento para definir a prioridade de um aplicativo usando a opção **Configurar prioridade de instalação do aplicativo**. Você pode definir prioridade Alta, Média ou Baixa para um aplicativo. Os aplicativos com a mesma prioridade serão instalados sem uma ordem específica. A prioridade do aplicativo não é usada durante as atualizações do aplicativo, quando o usuário já tiver instalado o aplicativo.

Selecionando configurações de gerenciamento de aplicativos Apple

Estas configurações se aplicarão apenas a este aplicativo e substituirão todas as configurações globais selecionadas em **Apps > Configurações do catálogo**. Para selecionar as configurações de **Gerenciamento de aplicativos Apple**.

Procedimento

1. Clique nas **configurações do Apple Apps** ou clique no ícone **+** para adicionar outra configuração para exibir a página **Definição da configuração**.
2. Insira um nome para a configuração no campo **Nome**.
3. Insira uma breve descrição da configuração no campo **Descrição**.

4. Selecione ou desmarque uma ou mais das seguintes opções em **Configurações de Gerenciamento Apple**:
    - **Impedir backup no iCloud e iTunes**
    - **Remover aplicativos mediante cancelamento do registro**
    - (iOS 14.0+) **Permitir remoção e descarregamento deste aplicativo** – você pode desmarcar esta opção para evitar que um usuário remova e descarregue um aplicativo gerenciado.
    - (Opcional) Adicione uma **Configuração de Aplicativo Gerenciado Apple**
5. Clique em **Atualizar**.

Seleção dos níveis de promoção do aplicativo

Você pode definir o nível de promoção do aplicativo.

Procedimento

1. Clique em **Definições de configuração de distribuição de promoção** ou clique no ícone **+** para adicionar outra configuração para exibir a página **Configuração da promoção**.
2. Insira um nome para os ajustes de configuração de distribuição de promoção no campo **Nome**.
3. Como opção, insira uma breve descrição da configuração no campo **Descrição**.
4. Selecione o nível de promoção que você deseja que o aplicativo receba: **Não destacado**, **Lista de destacados**, ou use um **Banner de destaque**. Caso **Não destacado** seja selecionado, o aplicativo não aparecerá na lista.
5. Clique em **+ Adicionar descrição** para inserir uma breve descrição da configuração.
6. Como opção, altere a distribuição da configuração.
7. Clique em **Concluído** para salvar a configuração do aplicativo.

Configurar regras de tráfego do AppTunnel

Use a configuração AppTunnel para definir as regras de tráfego para permitir o acesso a serviços usando Sentry.

Para obter informações sobre como adicionar uma configuração AppTunnel, consulte "Adição de uma configuração AppTunnel" no *Guia do AppConnect para Ivanti Neurons for MDM*.

Configurando o aplicativo gerenciado

Procedimento

1. Clique no ícone **+** para abrir a página de configuração.
2. Clique em **+ Adicionar descrição** para inserir uma breve descrição da configuração.
3. Clique em **+ Adicionar** para inserir uma chave e um valor.
4. Escolha um nível de distribuição.
5. Clique em **Avançar**.

Como configurar um VPN para cada aplicativo usando VPN por aplicativo

Procedimento

1. Clique no ícone **+** para abrir a página de configuração.
2. Insira um nome para o VPN deste aplicativo no campo **Nome**.
3. Clique em **+ Adicionar descrição** para inserir uma breve descrição da configuração.
4. Clique na opção **Habilitar VPN por aplicativo para este aplicativo** e selecione uma configuração VPN por aplicativo.
5. (Opcional) No caso de aplicativos macOS, insira a string **Requisito designado** no formato identificador "\%s\". Por exemplo, identificador "com.google.Chrome". Use este campo para permitir que um aplicativo macOS de múltiplos pacotes use uma VPN por aplicativo, como o Tunnel.
6. Escolha como **distribuir esta configuração de aplicativo**.
7. Clique em **Avançar**.

Como usar a configuração de aplicativos gerenciados Apple

Usando a Configuração de aplicativos gerenciados Apple, é possível definir configurações específicas para o aplicativo gerenciado instalado. Um aplicativo pode ter alguns parâmetros de configuração implementados ou restringidos pelo desenvolvedor. Para aplicativos com tais restrições, suas opções de configuração podem ser limitadas. Você pode configurar aplicativos gerenciados pela Apple.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione um aplicativo.
3. Clique na guia **Configurações de aplicativo**.
4. Clique em **configuração de aplicativos gerenciados Apple** ou clique no botão **+**.
   Na configuração de aplicativos gerenciados Apple, há algumas definições de configuração padrão.
5. Clique em **Adicionar** para adicionar outra configuração, se necessário. Como alternativa, clique no nome da configuração para editá-la.
6. Em **Fonte de configuração**, selecione qualquer opção de **Tipo de fonte**

   - **Comunidade de AppConfig**: esta opção está disponível apenas para apps cuja especificação de configuração está disponível no repositório da comunidade. Se essa opção estiver disponível, ela será selecionada por padrão.
   - **Usar a especificação .xml**: selecione esta opção para fazer upload do esquema do aplicativo e enviar uma versão específica da configuração do aplicativo. Clique em **Escolher arquivo** para carregar o arquivo .xml. Certifique-se de que o arquivo .xml contenha o ID e a versão do pacote. Se o ID do pacote no arquivo não corresponder ao ID do pacote do aplicativo, será exibida uma mensagem de erro.

   a. **Nenhum**: selecione essa opção caso não queira aplicar nenhum esquema ao aplicativo. Esta opção é selecionada por padrão, caso a opção **Comunidade de AppConfig** não esteja disponível.
   O arquivo .xml carregado é exibido na seção **Fonte de configuração**. Clique no ícone Excluir para excluir o arquivo .xml carregado.

7. Nas **Configurações de aplicativos gerenciados Apple**, é possível definir as opções de configuração para inserir pares de chave-valor.

   - **+Adicionar**: clique em **+Adicionar** para adicionar os pares de chave-valor à configuração do aplicativo gerenciado e recuperar a identidade do nome de registro pelo Go client durante o registro de dispositivo da Apple ou iReg.
     Você pode selecionar os tipos de dados (String, Inteiro, Booleano, Long Float, Duplo, Data, String Array, Integer Array, Double Array, Float Array, Long Array) para os pares de valores-chave.

     Adicione os seguintes pares de chave-valor à configuração do aplicativo gerenciado para recuperar a identidade do nome de registro pelo Go client durante o registro de dispositivo da Apple ou iReg:

Chave	Valor	Tipo
registration.username	${userEmailAddress}	STRING
registration.token	${zeroTouchClientRegistrationNonce}	STRING
registration.token.expirationSeconds	${zeroTouchClientRegistrationNonceExpiresAtSeconds}	STRING
registration.url	${clientRegistrationUrl}	STRING

   - **Usar .plist**: os arquivos .plist contêm múltiplos pares de chave-valor a serem carregados em massa. Clique em **Escolher arquivo** para fazer upload do arquivo .plist. Os dados plist validados serão exibidos na tabela **Configurações de aplicativos gerenciados Apple**.

     Arquivos plists com dicionários aninhados são inválidos.

8. Clique em **Atualizar** para salvar as entradas.

Clonar definições de configuração de aplicativos

Você pode clonar as definições de configuração de um aplicativo gerenciado para aplicá-las em outros dispositivos. Você pode até renomear e fazer algumas alterações nas configurações clonadas.

Android

Você pode clonar definições de configuração em dispositivos Android.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione o aplicativo do qual você deseja clonar as definições de configuração.
3. Clique em **Configurações do aplicativo**.
4. Na seção **Resumo de Configurações do Aplicativo**, você encontrará a lista de configurações (**Configurações gerenciadas para Android**, **Instalar no dispositivo**, **Promoção**, **Permissões de dispositivo delegadas** e **Versão do Google Play**) disponíveis para dispositivos Android.
5. Clique em qualquer uma das configurações disponíveis.
6. Em **Ações**, clique em **Clonar** para iniciar o processo de clonagem.
7. Por padrão, o nome da configuração clonada será <Cópia de nome da configuração clonada>. No entanto, você pode modificar o nome digitando um nome de sua escolha na caixa **Nome**.
8. (Opcional) Digite algum texto sobre a configuração clonada na caixa **Descrição**.
9. Clique em **Continuar**.

Uma janela de confirmação aparece indicando que a clonagem das definições de configuração do aplicativo foi concluída. Você pode visualizar a versão clonada no Resumo de Configurações de Aplicativo e dentro do aplicativo clonado.

iOS

Você pode clonar as definições de configuração de apps gerenciados em dispositivos iOS.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione o aplicativo do qual você deseja clonar as definições de configuração.
3. Clique em **Configurações do aplicativo**.

4. Na seção **Resumo de Configurações do Aplicativo**, você encontrará a lista de configurações (**Instalar no dispositivo**, **Configurações de aplicativo Apple**, **Promoção**, **Configuração personalizada do AppConnect**, **Túnel de aplicativo**, **Configuração de aplicativo gerenciado Apple** e **VPN por aplicativo**) disponíveis para dispositivos iOS.
5. Clique na configuração específica que você deseja clonar.
6. Em **Ações**, clique em **Clonar** para iniciar o processo de clonagem.
7. Por padrão, o nome da configuração clonada será <Cópia de nome da configuração clonada>. No entanto, você pode modificar o nome digitando um nome de sua escolha na caixa **Nome**.
8. (Opcional) Digite algum texto sobre a configuração clonada na caixa **Descrição**.
9. Selecione uma fonte de configuração na lista **Tipo de fonte**.
10. Na seção **Configurações de Aplicativos Gerenciados Apple**, insira **Chave**, **Valor** e selecione **Tipo** na lista.
    Para obter informações sobre **Chave**, **Valor** e **Tipo**, consulte **Usando a Configuração de Aplicativos Gerenciados Apple**.
11. Clique em **Continuar**.
    Uma janela de confirmação aparece indicando que a clonagem das definições de configuração do aplicativo foi concluída. Você pode ver a versão clonada na seção **Configuração de Aplicativos Gerenciados Apple**.

Windows

Você pode clonar configurações de aplicativo em dispositivos Windows:

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione o aplicativo do qual você deseja clonar as definições de configuração.
3. Clique em **Configurações de aplicativo**.
4. Na seção **Resumo das Configurações de Aplicativo**, você encontrará as configurações **Instalar no dispositivo** e **Promoção**.
5. Clique na configuração específica que você deseja clonar.

6. Em **Ações**, clique em **Clonar** para iniciar o processo de clonagem.
7. Por padrão, o nome da configuração clonada será <Cópia de nome da configuração clonada>. No entanto, você pode modificar o nome digitando um nome de sua escolha na caixa **Nome**.
8. (Opcional) Digite algum texto sobre a configuração clonada na caixa **Descrição**.
9. Clique em **Continuar**.

Uma janela de confirmação aparece indicando que a clonagem das definições de configuração do aplicativo foi concluída. Você pode visualizar a versão clonada no Resumo de Configurações de Aplicativo e dentro do aplicativo clonado.

Escolha de apps do Windows 10 para seu catálogo interno

Escolha os apps para adicionar ao seu catálogo de aplicativos internos. Aplicativos internos, da Microsoft Store e da Microsoft for Business são compatíveis com o Windows 10. O Windows 10 reforça a conformidade diretamente no dispositivo baseado nos apps que você escolheu para permitir ou proibir.

O intervalo de registro do Windows 10 ocorre uma vez a cada 60 minutos por padrão. Você pode executar um registro de dispositivo forçado para obter uma atualização do status do dispositivo e do aplicativo.

Estas ações são compatíveis:

- Upload de novos apps
- Instalação silenciosa
- Instalar manualmente a partir de Apps@Work
- Adição de uma nova versão do aplicativo
- Exclusão de um aplicativo

Estes formatos são compatíveis:

- APPX
- APPXBUNDLE
- MSI Win32 ajustado – aplicativo Win32 pré-agrupado

- MSIX (compatível com dispositivos Windows 10 RS5 e superior)
- .EXE (usando bridge)

O aplicativo **Ivanti Neurons Agent** está disponível no **Catálogo de Aplicativos** para dispositivos **Windows**. O administrador pode implantar o aplicativo **Ivanti Neurons Agent** como um aplicativo interno, e esse aplicativo pode ser distribuído de acordo nos dispositivos Windows.

Configurar aplicativos do Windows 10

Procedimento

1. Clique em **Dispositivos** na barra de navegação principal.
2. Selecione um dispositivo Windows 10 que você tenha registrado no Ivanti Neurons for MDM.
3. Clique em **Apps > Catálogo de aplicativos**.
4. Selecione um aplicativo.
5. Use o menu suspenso **Ações** para adicionar ou excluir o aplicativo do seu catálogo.
   Como alternativa, adicione uma nova versão do aplicativo.
   - Clique no menu suspenso **Ações**.
   - Selecione **Adicionar nova versão**.
   - Acesse o catálogo e selecione uma nova versão do aplicativo.
   - Clique em **Atualizar e Salvar** para visualizar a tela Informações do aplicativo.
6. Use o menu suspenso **Versão** para escolher qual versão usar.
7. Clique em **Editar** para começar a alterar os detalhes.
   - Edite a **Categoria** se necessário.
   - Insira uma **Descrição** se necessário.
   - Adicione capturas de tela se necessário.
8. Clique em **Salvar**.

9. Clique na guia **Distribuição** e clique em **Editar** para começar a fazer alterações no nível de distribuição.
10. Clique em **Salvar**.
11. Clique na guia **Configurações do aplicativo** para visualizar um resumo da configuração atual.
12. Insira a descrição do aplicativo, se necessário.
13. Clique em **Instalar no dispositivo** na página de resumo de configurações do aplicativo.
    A instalação silenciosa é o padrão e não pode ser alterado.
14. Clique em **Promoção** no painel de navegação esquerdo e, em seguida, clique em **Definições de configuração da distribuição da promoção** para alterar o nível de promoção.
    - Clique em **Editar** para alterar os ajustes do nível de promoção.
    - Insira um nome para a configuração.
    - Insira uma descrição para a configuração.
    - Selecione um nível de promoção.
    - Clique em **Atualizar** para salvar as alterações.
15. Clique na guia **Análises** para exibir informações sobre análises.
    Exporte os dados de revisão para uma planilha, se necessário.

Edição das definições de configuração de aplicativo no Windows 10

Procedimento

1. Clique em **Políticas** > **Configuração**.
2. Clique em **+Adicionar**.
3. Selecione **Controle de aplicativos do Windows** para exibir a tela **Criar configuração de controle de aplicativos do Windows**.
4. Digite um **Nome** e uma **Descrição** para a configuração.

5. Defina o tipo de aplicativo como:
    - Permitido (Listado como permitido) – Somente estes apps são permitidos. Estes apps são instalados de forma silenciosa se já não estiverem presentes no dispositivo.
    - Não permitido (Listado como bloqueado) – Se estiverem presentes no dispositivo, esses apps serão bloqueados se iniciados.
6. Especifique a definição Regras para o Tipo e Identificador de Aplicativo.
7. Clique em **Pesquisar Apps** para exibir a tela **Pesquisar Aplicativos do Windows 10**.
8. Insira o nome do aplicativo para pesquisar na Windows Store.
9. Selecione o aplicativo das escolhas exibidas para adicioná-lo ao Identificador de Aplicativos.
10. Como alternativa, use o menu suspenso Tipo de aplicativo para definir um caminho no Identificador de aplicativo para permitir ou proibir apps que usem um caminho especificado ou bloquear todos os apps instalados neste caminho.
    O tipo de aplicativo **Publisher/PFN Equals** é aplicável ao Windows 10 Mobile, e o Windows 10 Desktop é compatível com PFN. **EXE/Win32 Equals** é aplicável apenas para o Windows Desktop.
11. Clique em **Avançar**.
12. Selecione um nível de distribuição.
    - **Todos os dispositivos**.
    - **Nenhum dispositivo**.
    - **Personalizado** - para inserir os usuários ou grupos que vão receber aplicativo.
13. Clique em **Concluído**.
14. Você pode editar as definições de Regra para selecionar o Tipo de aplicativo e especificar o Identificador do aplicativo.
    - Clique no menu suspenso **Ações**.
    - Selecione **Adicionar nova versão**.
    - Selecione a nova versão do aplicativo.
    - Clique em **Atualizar e Salvar** para visualizar a tela **Informações do aplicativo**.

Configurando a opção Reinicializar dispositivo após a instalação para Windows

Você pode configurar um dispositivo para se reinicializar após a instalação de um aplicativo usando a opção **Reinicializar dispositivo após a instalação**.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione qualquer aplicativo específico do Windows na lista.
3. Vá para **Configurações do aplicativo > Instalar no dispositivo > Instalar definição de configuração do aplicativo**.
4. Clique em **Editar** e ative a opção **Reiniciar dispositivo após a instalação**.
5. Selecione o horário no qual deseja reinicializar o dispositivo.
6. Clique em **Atualizar**.

   O dispositivo será reinicializado no horário agendado.

No caso de aplicativos públicos e aplicativos da Microsoft Store for Business (MSB), você precisa definir a configuração **Instalar silenciosamente em dispositivos Windows** como ATIVADO na seção **Configurações do aplicativo**.

Instalação de apps usando o Apps@Work

Para instalar um aplicativo usando o Apps@Work:

1. Clique no aplicativo **Apps@Work**.
   O seu endereço de e-mail administrador e servidor URL são preenchidos automaticamente na caixa de diálogo para fazer login ao Apps@Work.
2. Insira a sua senha e clique em Entrar para exibir a página de apps.

3. Selecione um aplicativo para instalar. Não será possível instalar apps com dependências em apps de pré-requisito se estes já não estiverem instalados no cliente.
   No Apps@Work para dispositivos iOS, há a opção de clicar no botão **Instalar todos** para instalar todos os apps. Essa opção está disponível nas telas **Novas versões**, **Apps em destaque** e **Categorias**.

   > Os aplicativos Apps and Books não serão instalados se a respectiva licença não for aceita anteriormente.

4. Clique em **Atualizar e Salvar** para visualizar a tela **Informações do aplicativo**.

Tópicos relacionados:

- "App Catalog" na página 301

Como atribuir atributos personalizados aos aplicativos

Depois de criar atributos personalizados, você pode atribuí-los a um ou mais aplicativos. Cada atributo tem um valor correspondente que você pode usar para tarefas, tais como criar grupos de aplicativos. Para mais informações sobre como gerenciar atributos, consulte "Atributos" na página 1164.

Criar e atribuir um atributo personalizado a um aplicativo individual

Você pode atribuir um atributo personalizado a um aplicativo individual.

Procedimento

1. Faça login no Portal Administrativo.
2. Navegue até **Aplicativos** > **Catálogo de aplicativos**.
3. Selecione um aplicativo e clique em **Atributos**.
4. Clique em **+Adicionar novo** e selecione um valor no menu suspenso **Nome do atributo**.
5. Especifique o valor do atributo no campo **Valor**.
6. Clique em **Salvar**. O atributo personalizado é adicionado ao aplicativo.

Atribuir um atributo personalizado a vários aplicativos

Você pode atribuir atributos personalizados a um ou mais aplicativos. Quando você seleciona vários aplicativos, o atributo personalizado é aplicado a todas as versões do aplicativo. Você pode selecionar um aplicativo específico, acessar a guia Atributos e alterar os detalhes do atributo personalizado para uma versão específica do aplicativo.

Procedimento

1. Faça login no Portal Administrativo.
2. Navegue até **Aplicativos** > **Catálogo de aplicativos**.
3. Marque as caixas de seleção em um ou mais aplicativos.
4. Clique em **Ações**.
5. Selecione **Atribuir atributos personalizados**. O assistente Atribuir Atributos Personalizados a Aplicativos é exibido.
6. Selecione *uma* das opções a seguir:
   - Forçar a designação (substituição) de todos os atributos, mesmo que quaisquer valores existentes sejam encontrados.
   - Substituir apenas se o valor estiver vazio e ignorar atributos com valores existentes.
7. Marque as caixas de seleção em um ou mais atributos.
8. Especifique o valor nos campos Valor (valores vazios não são permitidos).
9. Clique em **Atribuir**. O atributo personalizado é atribuído a todas as versões dos aplicativos selecionados.
10. (Opcional) Se quiser alterar o atributo personalizado para determinada versão do aplicativo, selecione a versão do aplicativo na lista suspensa de versões e clique em Editar.

Os **Atributos Personalizados de Aplicativos** e os valores deles podem ser usados para criar relatórios e ser exportados em formato CSV na página **Detalhes do dispositivo**.

Configurações gerenciadas para Android

Esta seção contém os seguintes tópicos:

Se o Ivanti Neurons for MDM estiver habilitado para Android Enterprise, a configuração do Android Enterprise estará disponível para uso por aplicativo.

Uso de configurações gerenciadas do Android Enterprise

1. Clique em **Apps**.
2. Clique em **Catálogo de aplicativos**.
3. Selecione um aplicativo no qual deseja definir a configuração do Android Enterprise.
4. Clique em **Configurações do aplicativo**.
5. Clique em **Configurações gerenciadas para Android**.
6. Forneça um nome para a configuração.
7. Como opção, forneça uma descrição.
8. Use os campos de Configurações gerenciadas para definir o comportamento dessas configurações :

Configuração	Descrição
Impede os apps de compartilhar widgets entre perfis	Permitir bloqueio de apps de compartilhamento de widgets entre perfis somente se o aplicativo não for instalado silenciosamente. Deixe desativado para permitir que apps confiáveis implementados no perfil do Android Enterprise exibam widgets na tela inicial de modo que os usuários possam acessar as informações sem precisar efetuar login.
Bloqueia a desinstalação do aplicativo pelo usuário	Permite bloquear a desinstalação do aplicativo pelo usuário após o Ivanti Neurons for MDM instalar silenciosamente o aplicativo.

Código de versão mínima	Definir um código de versão mínimo necessário para o aplicativo substituir o comportamento de atualização padrão. Se o código de versão do aplicativo atualmente instalado no dispositivo for menor que o código de versão mínimo especificado, o aplicativo será atualizado imediatamente para a versão mais recente.
Início automático na instalação	Selecione essa opção se desejar iniciar um aplicativo automaticamente após a instalação. Este recurso está disponível apenas se o aplicativo for recém-instalado no dispositivo e não for uma atualização de versão. No caso de Work Profile ou Work Profile em dispositivos de propriedade da empresa, o aplicativo Go deve estar ativo e em primeiro plano. Devido a limitações no Android 10+, somente um aplicativo será iniciado automaticamente se o usuário enviar vários apps no caso do Work Profile e do Work Profile em dispositivos de propriedade da empresa.

Configurações gerenciadas

O administrador pode controlar os campos de configuração de aplicativo que podem ou não ser enviados aos dispositivos. Em geral, os valores padrão são definidos no momento de enviar as configurações aos diferentes dispositivos. Na seção Configurações Gerenciadas, no parâmetro **Enviar ao dispositivo**, selecione **Enviar todas as configurações** ou **Enviar somente configurações com valores definidos**.

Cada configuração de aplicativo Android Enterprise exibe o botão Habilitar certificado para cada campo de texto e, quando clicado, o campo de texto é substituído por uma lista suspensa de certificados. Quando configurados, esses certificados são aplicados silenciosamente, sem qualquer interação com o usuário.
Um campo habilitado para certificado existente pode ser alterado para habilitado para texto clicando-se no mesmo botão ao lado do campo. Um campo habilitado para texto alterado para um campo habilitado para certificado pode voltar a ser um campo habilitado para texto clicando-se no mesmo botão. (Campos suspensos padrão não podem ser alterados de volta para campos habilitados para texto.)

Se não houver certificados de ID configurados no locatário, e quando alterado de texto para menu suspenso usando o botão Ativar para certificado, apenas a opção "Nenhum" será mostrada na lista suspensa.

9. Clique em **Gerenciar permissões** para selecionar e configurar as permissões de tempo de execução para os aplicativos que visam a API 23 ou superior e o Android 6.0 ou superior.
   Somente as permissões perigosas apropriadas ao aplicativo específico estão listadas para seleção. A lista completa de permissões perigosas (como ler seus contatos, localizar contas no dispositivo, gravar registro de chamadas e assim por diante) está em https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.

   - As permissões são aplicadas somente quando o aplicativo solicita permissões.
   - As permissões não são aplicadas se os usuários já tiverem aceitado ou negado permissões anteriormente.

   Os direitos que podem ser designados a cada permissão incluem:

   - Concessão automática;
   - Negação automática. Use essa configuração com cautela;
   - Padrão/global.

10. Configure as opções de distribuição, selecionando **Todos com o aplicativo**, **Nenhum** ou **Personalizado**.
11. Clique em **Salvar**.

Restrições e permissões para aplicativos internos

O administrador pode definir algumas restrições de aplicativos e restringir ou conceder permissões para aplicativos internos. Essa funcionalidade estava disponível apenas para aplicativos públicos. Mas agora ela foi estendida para os aplicativos internos.

O administrador deve reenviar os aplicativos internos para ter os recursos **Restrições de aplicativo** e **Permissões** disponíveis neles. Recomenda-se excluir o aplicativo existente antes de carregar uma nova versão.

Procedimento

1. Acesse **Apps** > **Catálogo de aplicativos**.
2. Selecione um aplicativo **Interno** na lista.
3. Clique em **Configurações de aplicativo**.
4. Clique em **Configurações gerenciadas para Android**.
5. Clique em **Adicionar**.

   A seção **Restrições de aplicativo** aparece na tela.
6. Insira os valores desejados nas restrições disponíveis.
7. Selecione **Gerenciar permissões**.

   A janela **Selecionar permissões** aparece na tela.
8. Selecione as permissões necessárias na lista e clique em **Selecionar**.
9. Na seção **Permissões de tempo de execução**, defina os valores para as permissões selecionadas.
10. Na seção **Distribuir essa configuração de aplicativo**, escolha uma das seguintes opções de **Distribuição de aplicativo**:
    - **Todos com o aplicativo**
    - **Ninguém**
    - **Personalizada**
11. Clique em **Salvar**.

    As restrições e permissões selecionadas serão aplicadas nos aplicativos internos.

Configurando o Gmail com o Android Enterprise

Você poderá implantar o Gmail em dispositivos Android Enterprise se tiver configurado o Ivanti Neurons for MDM para Android Enterprise. Para configurar o Gmail com o Android Enterprise

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione o aplicativo do Gmail para o qual deseja definir a configuração do Android Enterprise. A seção Definições de configuração é exibida.

3. Forneça um nome para a configuração.
4. Como opção, forneça uma descrição.
5. Use os campos **Configurações gerenciadas** para definir o comportamento dessas configurações:

> As opções **Expandir tudo** e **Recolher tudo** estão disponíveis apenas para restrições aninhadas ou hierárquicas.

Configuração	Descrição
Enviar ao dispositivo	Enviar todas as configurações - selecione esta opção para ativar todos os botões, incluindo aqueles sem valores Enviar somente configurações com valores definidos - selecione esta opção para habilitar todos os botões com valores definidos e desabilitar os botões das configurações sem valores Em muitos casos, as configurações padrão já estão disponíveis. No entanto, o administrador pode selecionar as configurações necessárias do aplicativo ou editar as variáveis que devem ser enviadas aos dispositivos.
Endereço de e-mail	Insira variáveis de substituição para definir o endereço de e-mail. Normalmente, você insere $emailaddress$. Os UEMs podem usar esse campo para obter credenciais do usuário do Active Directory.
Nome do host ou host	Digite o nome do host para o servidor Active Sync, como nomedohost.empresa.com:443/caminho.
Nome de usuário	Use a variável para o nome de usuário do Active Directory do usuário que pode ser especificado como um nome de usuário direto (janedoe) ou um valor de modelo ($username$).
Tipos de autenticação	Selecione a lista de strings que contêm os tipos de autenticação permitidos.
SSL obrigatório	Quando selecionado, habilita e exige SSL nos números de porta usados com o nome do host.
Confiar em todos os certificados	Selecione apenas se desejar que o aplicativo aceite automaticamente certificados não confiáveis. Use esta opção apenas para depuração ou

Configuração	Descrição
	desenvolvimento ao trabalhar em um ambiente de teste.
Alias do certificado de login	Digite o alias do certificado de login usado para autenticação nos servidores ActiveSync.
Permitir contas não gerenciadas	Selecione esta opção para permitir que os usuários adicionem ou removam qualquer conta do Exchange que não seja a conta especificada nesta configuração gerenciada.
Assinatura de e-mail padrão	Digite a string que compreende a assinatura de e-mail padrão a ser anexada na parte inferior de todo o texto da mensagem de e-mail de saída.
Janela de sincronização padrão	Digite o valor de 0 a 5 que representa a janela de tempo para sincronização com o EAS (Exchange Active Sync).

6. Clique em **Avançar**.
7. Configure as opções de distribuição, selecionando **Todos com o aplicativo**, **Nenhum** ou **Personalizado**.
8. Clique em **Salvar**.

Gerenciamento de apps do Google Play

Você pode definir qual binário do aplicativo Google Play deve ser implementado em grupos ou indivíduos específicos. Essa implementação se aplica a implementações do Android corporativo. O desenvolvedor do aplicativo também deve incluir sua organização na lista de permitidos para que possa implantar apps de canal alfa ou beta.

1. Clique em **Apps**.
2. No **App Catalog**, selecione o aplicativo para o qual definir a configuração de versão do Google Play.
3. Clique na guia **Configurações do aplicativo**.
4. Clique em **Versão do Google Play**.

   A configuração da Versão do Google se aplica somente a aplicativos do Android Enterprise. Por padrão, a opção Produção será aplicada se a configuração da versão do Google não for selecionada para apps recém-adicionados.

5. Clique em **Adicionar**.
6. Forneça um nome para a configuração.
7. Como opção, forneça uma descrição.
8. Selecione uma opção na lista suspensa para escolher o binário que será disponibilizado aos usuários e dispositivos que receberem o aplicativo. As opções são:
   - **Produção**
   - **Alfa**
   - **Beta**

   A opção Produção é aplicada por padrão aos aplicativos que já foram enviados ao dispositivo.

9. Configure as opções de distribuição, selecionando **Todos com o aplicativo**, **Nenhum** ou **Personalizado**.

Personalizado distribui o aplicativo para o grupo de usuários juntamente com o filtro de dispositivo.

10. Clique em **Salvar**.

Priorização da configuração com diversas versões

Quando diversas configurações de versão do Google são adicionadas, é possível priorizar a ordem de aplicação da configuração de versão do Google.

1. Em **Configurações do aplicativo**, clique em **Priorizar configurações**.

   Este botão é exibido somente quando há diversas configurações listadas

2. Nas configurações listadas, arraste e solte a configuração que deve ser aplicada prioritariamente na parte superior da lista.
3. Clique em **Atualizar**.

   Quando a configuração prioritária é excluída, a segunda configuração na lista assume a condição de configuração prioritária.

Exclusão de apps do App Catalog

Você pode excluir apps públicos e internos do Catálogo de aplicativos. Não é possível excluir apps de pré-requisito. É necessário editar os apps para remover os relacionamentos de pré-requisito antes de excluir tais aplicativos. Se o aplicativo estiver instalado nos dispositivos, ele será removido na próxima vez em que esses dispositivos forem registrados. A instalação/desinstalação silenciosa de aplicativos é compatível com dispositivos Samsung e Zebra no modo Administrador do Dispositivo; ou em todos os dispositivos no modo Proprietário do Dispositivo.

No caso de aplicativos internos, uma janela de confirmação aparece na tela. Você precisa selecionar a confirmação de que deseja continuar com a operação Excluir e clicar em **Excluir aplicativo**. Quando você tenta excluir vários aplicativos e alguns deles não podem ser excluídos, aparece na tela uma janela com informações sobre os aplicativos que não podem ser excluídos e o motivo.

As seguintes condições se aplicam quando você tenta excluir um ou mais aplicativos do Catálogo de Aplicativos:

- Se alguma versão do aplicativo interno não puder ser excluída, não será possível excluir nenhuma versão.
- Se alguma versão do aplicativo interno for um aplicativo de pré-requisito, não será possível excluir o aplicativo nem qualquer versão dele.
- Quando você selecionar todos ou alguns dos aplicativos internos para excluí-los do Catálogo de Aplicativos, todas as versões dos aplicativos internos selecionados serão excluídas.
- Um aplicativo interno delegado de um Espaço não pode ser excluído.

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique no link para o aplicativo.
3. Selecione **Ações > Excluir do catálogo**.
4. Leia os avisos que explicam o que acontece ao excluir um aplicativo.

   O aviso explica que as licenças do Apps and Books (iOS) e as revisões do aplicativo (todos os SOs) também serão excluídas.

5. Marque a caixa de seleção "Eu compreendo as consequências da exclusão de um aplicativo" para prosseguir com a operação de exclusão.
6. Clique em **Excluir aplicativo**.

Upgrade de apps internos

Use o procedimento a seguir para atualizar um aplicativo interno:

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione o aplicativo que será atualizado.
3. Selecione **Ações > Adicionar nova versão**.
4. Arraste e solte o aplicativo na área **Carregar aplicativo** ou clique em **Escolher arquivo** para selecioná-lo no seu sistema de arquivos.
5. Selecione uma das opções a seguir, com base no que você deseja fazer com a versão anterior do aplicativo:
   - **Manter a descrição, as capturas de tela, a distribuição, os pré-requisitos de aplicativo e as configurações do aplicativo iguais:** substitui a versão anterior no catálogo de aplicativos.
   - **Alterar a descrição, as capturas de tela, a distribuição, os pré-requisitos de aplicativo ou as configurações do aplicativo**: inclui as duas versões no catálogo de aplicativos.
6. Em **O que há de novo**, insira um texto que explique aos usuários as diferenças da nova versão.

   O texto será exibido no dispositivo quando o usuário selecionar o aplicativo para instalação.
7. Se você escolher alterar as descrições, capturas de tela ou opções de distribuição, conclua essas alterações.
8. Clique em **Concluído**.

   Se você optar por manter as versões mais antigas do aplicativo no catálogo, apenas uma entrada será exibida em **Apps > Catálogo de aplicativos**. O painel à esquerda indicará o número de apps responsáveis pela entrada. Se mais tarde você decidir excluir a versão mais recente, a versão antiga irá substituí-la automaticamente nos dispositivos instalados.

Exibição da lista de versões do aplicativo

Os administradores podem carregar os aplicativos com a mesma versão e diferentes arquiteturas.

ProcedureProcedimento

1. Clique no link para o aplicativo em **Apps > App Catalog.**
2. Clique na guia **Versão**.
   Se houver várias versões do aplicativo no catálogo, será exibida uma lista suspensa com as versões. Se diversos aplicativos com o mesmo número de versão, mas diferentes arquiteturas, forem carregados, o menu suspenso exibe os detalhes da arquitetura compatível. As arquiteturas compatíveis para os aplicativos também são exibidas em **Informações do aplicativo**.

Descoberta do nome do pacote de um aplicativo do Android

Para apps públicos disponíveis na Google Play Store:

1. Use um navegador para localizar o aplicativo na Google Play Store.
2. Selecione o aplicativo.
3. Examine a URL exibida no navegador.

   O nome do pacote está incluído na URL após o id=, conforme mostrado a seguir:

   https://play.google.com/store/apps/details?id=<package name>

Para apps internos e outros apps não disponíveis na Play Store, tente baixar o Visualizador de nome de pacote ou um aplicativo similar na Google Play Store.

Categorias

Esta seção contém os seguintes tópicos:

As categorias descrevem os tipos de apps e ajudam a organizá-los quando os usuários navegam no catálogo de aplicativos.Todos os aplicativos devem ter pelo menos uma categoria atribuída. Uma lista de categorias de aplicativos comuns estará disponível quando você começar a usar o Ivanti Neurons for MDM. Use essa página para gerenciar categorias de aplicativos.

Adição de categorias

Você pode adicionar novas categorias aqui ou ao adicionar um aplicativo no catálogo de aplicativos.

1. Clique em **Adicionar** (canto inferior esquerdo)
2. Digite o nome da categoria.

   As categorias não fazem distinção entre letras maiúsculas e minúsculas, por isso, MEU é a mesma coisa que Meu.
3. Clique em **Salvar**.

Remoção de categorias

- Clique no X ao lado da categoria.

Se você não conseguir executar tarefas na página das **Categorias de aplicativo,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de aplicativo e conteúdo

Filtros de distribuição

Esta seção contém os seguintes tópicos:

Use Filtros de Distribuição para limitar os apps disponíveis para instalação. Os filtros de distribuição permitem que você exiba apenas os apps no catálogo de apps que podem ser usados no dispositivo.

Licença: Silver

Esses filtros estão disponíveis por padrão:

- **Apps com Android corporativo ativado** – Limita a distribuição de aplicativos aos dispositivos com Android corporativo ativado.
- **Apps apenas do iPad** - limita a distribuição de apps apenas para dispositivos iPad.
- **Apps apenas do iPhone** - limita a distribuição de apps apenas para dispositivos iPhone.

Configuração dos filtros de distribuição

1. Vá para **Apps > Filtro de Distribuição**.
   Os filtros de apps padrão e criados estão listados aqui.
2. Clique em **Adicionar** para acessar a caixa de diálogo **Criar Filtro de Distribuição**.
3. Insira o nome e a descrição nos devidos campos.

4. Selecione as definições das regras. Essas regras podem ser criadas usando os operadores aplicáveis, incluindo os operadores "contém", "é menor que", "é maior que", "está no intervalo", "é igual a" e "é diferente de". As regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). Os filtros de distribuição do aplicativo têm os seguintes recursos
   - Acesso bloqueado
   - Capacidade APNS
   - Dispositivo gerenciado Android com Work Profile
   - Android Work habilitado
   - Dispositivos gerenciados de trabalho com Android (Proprietário do dispositivo) ativados
   - Perfil de trabalho do Android ativado em dispositivos de propriedade da empresa
   - Último registro do cliente
   - Cliente registrado
   - Conformidade
   - Ação de conformidade bloqueada
   - Nome do País Atual
   - MCC atual
   - MNC atual
   - Atributo de dispositivo personalizado
   - Atributo LDAP personalizado
   - Atributo de usuário personalizado
   - Tipo de dispositivo
   - Nome do País de Origem
   - MCC inicial
   - MNC inicial
   - Modo de quiosque
   - Fabricante
   - Versão do SO
   - Propriedade
   - Número de telefone
   - Roaming
   - Status de Secure Apps
   - Supervisionado
   - Sentry bloqueado
   - Registro de usuário registrado
   - Registro de dispositivo automatizado registrado
5. Clique em **Criar Filtro de Distribuição**.

6. Se necessário, selecione um filtro personalizado para atualização.
    a. Clique em **Editar** para exibir a página **Atualizar filtro de distribuição**.
    b. Insira o nome e a descrição nos devidos campos.
    c. Use os menus suspensos para definir as regras do filtro.
    d. Clique em **Atualizar Filtro de Distribuição**.
7. Selecione um aplicativo.
8. Na página de Detalhes do Aplicativo selecione a aba **Distribuição** .
9. Clique em **Editar**.
10. Escolha uma opção de distribuição do aplicativo:
    - **Todos**
    - **Ninguém**
    - **Personalizada**

    A seção Filtro de Distribuição fica visível apenas se a opção de distribuição **Todos** ou **Personalizada** for selecionada.
11. Escolha a opção do filtro de distribuição:
    a. Digite um nome de filtro no campo **Pesquisar os filtros de distribuição existentes**... para localizar um filtro já criado.
    b. Clique em **+Adicionar filtro de distribuição** para adicionar um novo filtro.

Filtros de distribuição podem ser criados ou atribuídos a um aplicativo antes de ser adicionado ao catálogo. Alterações feitas nos Filtros de distribuição afetarão a distribuição dos apps que estão usando o filtro (em todos os Espaços).

Quando o filtro é definido e se a opção **Permitir instalação do aplicativo em dispositivos M1 na distribuição** estiver habilitada, o resultado preenche os dispositivos macOS M1. O aplicativo iOS VPP estará disponível para todos os dispositivos Mac se a opção **Permitir instalação do aplicativo em dispositivos M1 na distribuição** estiver habilitada e o Filtro de distribuição for **Todos** ou **Personalizado**. Filtros de distribuição de atributos relacionados ao macOS não são compatíveis com apps iOS.

Configuração dos filtros de distribuição para o administrador delegado

O administrador delegado pode gerenciar e editar os filtros criados que foram adicionados a apps individuais durante o processo de distribuição no Espaço delegado. Entretanto, o administrador delegado não pode usar os filtros de distribuição criados no Espaço padrão em outro Espaço, mas pode usá-los para apps delegados.

O administrador delegado pode criar, gerenciar e editar filtros de distribuição no Espaço específico a que ele tem acesso. Os filtros de distribuição estão disponíveis somente no Espaço em que foram criados. Os filtros de distribuição de aplicativo não podem ser delegados.

Quando um administrador delegado com a função de gerenciamento de aplicativo e sistema adiciona um aplicativo usando o filtro de distribuição no Espaço delegado, ele pode ver os detalhes dos dispositivos em seu Espaço e dos dispositivos em outros Espaços.

O usuário com função de gerenciamento de sistema ou somente leitura do sistema não poderá criar, atualizar ou excluir filtros de distribuição em nenhum Espaço.

O administrador delegado com função de gerente de aplicativo e conteúdo não pode acessar o filtro de distribuição. Devido a isso, não é possível:

- Criar apps usando filtros de distribuição. Isso acontece quando você está conectado como administrador delegado e adiciona um aplicativo.
- Um administrador delegado somente com a função Apenas leitura de sistema ou superior pode adicionar apps com filtro de distribuição. Um administrador delegado sem a função Gerenciamento de sistema pode adicionar apps sem filtro de distribuição.

O administrador delegado pode filtrar o Status de delegação no catálogo de aplicativos ao selecionar uma das opções a seguir:

- Delegado
- Não delegado

Opiniões

Esta seção contém os seguintes tópicos:

Opiniões são os comentários e as classificações (estrelas) que os usuários dão aos apps no catálogo de aplicativos.As opiniões oferecem informações importantes a você e aos usuários que estão considerando a instalação do aplicativo. Use a página **Opiniões** para visualizar ou excluir classificações e opiniões. Exclua uma opinião ou classificação se ela for antiga ou não apropriada.

- Somente os usuários de dispositivos podem criar e editar as classificações e opiniões do aplicativo.
- Os usuários do dispositivo podem editar, mas não excluir, suas próprias classificações opiniões.
- Somente os administradores podem excluir opiniões do aplicativo.
- As classificações do aplicativo não podem ser excluídas. As classificações (estrelas) fornecidas aos apps permanecem na página **Apps > Catálogo de aplicativos**, mesmo se você desabilitar as classificações e opiniões futuramente para seus usuários.

Exibição de classificações e opiniões

- Acesse **Apps > Opiniões** para ler as classificações (estrelas) e comentários completos para os apps distribuídos.
- Acesse **Apps > App Catalog** e veja a coluna **Classificação média** para o número total de opiniões e classificação média.
- Acesse **Apps > Catálogo de aplicativos**, clique em **Nome do aplicativo** e veja a guia **Opiniões** para classificações e opiniões sobre um aplicativo específico.

Desativação de classificações e opiniões

1. Acesse **Apps > Configurações do catálogo**.
2. Desmarque **Permitir classificações e opiniões no catálogo de aplicativos do usuário final**.
3. Clique em **Salvar**.

Exclusão de opiniões

1. Acesse **Apps > Opiniões**.
2. Selecione a opinião.
3. Clique no botão **Ações** no canto superior direito da página.
4. Selecione **Excluir**.
5. Clique em **Sim** na caixa de diálogo de confirmação **Excluir opinião**.

Se você não conseguir executar tarefas na página **Opiniões,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de apps e conteúdo

Apps and Books da Apple

Esta seção contém os seguintes tópicos:

Licença: Silver

A tela **Apps and Books da Apple** só estará disponível se você tiver configurado o Apps and Books da Apple em suas configurações do App Catalog. Essa tela mostra as licenças de aplicativo que foram compradas para dispositivos Apple por meio do Apps and Books da Apple e quantas foram usadas. Use essa tela para:

- selecionar os aplicativos Apps and Books que serão incluídos no seu catálogo
- distribuir licenças para aplicativos Apps and Books

Para mais informações sobre como distribuir aplicativos com o Apps and Books, consulte o artigo na Comunidade Ivanti, Ivanti Neurons for MDM: How to Distribute Apps with VPP.

Apple Books pode não estar disponível em todos os países ou regiões. Para distribuir licenças para aplicativos pelo Apps and Books da Apple, é necessário inserir o sToken fornecido pela Apple.

Distribuição de licenças de apps em várias contas Apps and Books da Apple em um espaço

- Se o mesmo aplicativo estiver presente em mais de uma conta Apps and Books, a licença será distribuída na ordem de prioridade das contas.
- Se o mesmo aplicativo estiver presente em mais de uma conta Apps and Books e sua licença na conta com prioridade mais alta estiver encerrada, o aplicativo receberá uma licença da conta seguinte na ordem de prioridade, apenas se o usuário ou o dispositivo estiverem presentes na lista de distribuição de licença da conta seguinte.
- Se a prioridade das contas Apps and Books for alterada, não haverá revogação nem reatribuição de licença. O aplicativo receberá uma licença da primeira conta. Se as licenças da primeira conta estiverem encerradas, o aplicativo receberá uma licença da conta seguinte na ordem de prioridade e assim por diante.
- Um usuário tem a opção de revogar todas as licenças de um aplicativo na página do App Catalog. Nesse caso, a licença do aplicativo seria revogada em todas as contas Apps and Books disponíveis.
- Licenças reservadas têm precedência sobre a prioridade das contas Apps and Books.

Distribuição de licença baseada no dispositivo e no usuário

O fato de a licença para um aplicativo ser baseada no dispositivo ou no usuário depende de como você a atribui. Ao atribuir uma licença de aplicativo a um dispositivo, ela se torna uma licença baseada em dispositivo . Ao atribuir uma licença de aplicativo a um usuário, ela se torna uma licença baseada em usuário .

Uma licença é distribuída ao instalar o aplicativo Apps and Books no dispositivo ou quando se emite um token para esse aplicativo. Se não houver licenças disponíveis para o aplicativo, o usuário terá a opção de instalar e pagar pelo próprio aplicativo. Se um usuário já tiver recebido uma licença baseada em usuário para o aplicativo Apps and Books solicitado, o aplicativo será instalado usando a licença existente baseada em usuário em vez da licença Apps and Books.

No caso de iPads compartilhados, o Apps and Books é instalado com base em licenças baseadas em dispositivo, independentemente de as licenças baseadas em dispositivo serem selecionadas ou não.

Uso da opção de licença baseada em dispositivo

Com as licenças baseadas em dispositivo, os usuários não precisam de registro no Apps and Books. Os aplicativos exigidos serão instalados automaticamente. Os dispositivos corporativos supervisionados não precisam lidar com um ID da Apple de propriedade de TI.

Durante seu registro, o dispositivo é identificado pelo número de série e o aplicativo exigido será instalado se houver licenças disponíveis. Se nenhuma licença estiver disponível, o aplicativo não será instalado. Se houver uma licença reservada para um aplicativo, não será feita uma atribuição de licença baseada em dispositivo na instalação do aplicativo.

As atualizações de aplicativos implantados com licença do Apps and Books baseada em dispositivo são controladas pelo administrador.

Para controlar como um aplicativo será atualizado, em **Apps > App Catalog**, navegue até a guia **Configurações do aplicativo/Instalar no dispositivo**. Você poderá selecionar uma atualização imediata que ocorrerá no próximo dispositivo registrado ou poderá escolher que o aplicativo seja atualizado automaticamente quando houver novas versões disponíveis.

Importante: antes de atribuir uma licença baseada em dispositivo a um aplicativo de empresa para empresa (B2B) ou de produtividade, confirme com o desenvolvedor se o aplicativo pode ser licenciado com base no dispositivo.

Uso da opção de licença baseada em usuário

Uma licença baseada em usuário permanece válida para o usuário se ele tiver que trocar de dispositivo em caso de perda ou roubo, ou se o usuário adquirir um dispositivo mais recente. Com licenças baseadas no usuário, o usuário deve primeiro se registrar no Apps and Books da Apple. O registro é uma ação manual que usuário final deve concluir no Catálogo de aplicativo. Aplicativos Apps and Books necessários não serão instalados no dispositivo até que o usuário se registre no Apps and Books.

Se o aplicativo for um Apps and Books exigido e a distribuição de licença for baseada em usuário:

- A instalação exigida do aplicativo não ocorrerá se o usuário não estiver registrado no programa Apps and Books.
- Os aplicativos exigidos poderão ser instalados se o usuário estiver registrado no programa Apps and Books e uma licença estiver disponível.
- Se o usuário estiver registrado no Apps and Books, mas não houver licenças disponíveis, o aplicativo não será instalado.

Adicionando um aplicativo Apps and Books ao catálogo

Procedimento

1. Acesse **Apps > Catálogo de aplicativos**.
2. Selecione um aplicativo e clique em **Adicionar ao catálogo**. Clique em **Avançar**.
3. Como alternativa, adicione uma descrição do aplicativo. Clique em **Avançar**.
4. Selecione uma opção de distribuição. Clique em **Avançar**.
5. Clique na guia **Configuração do aplicativo**.
6. Opcionalmente, selecione **Instalar no dispositivo**. Esta opção de configuração instala o aplicativo sem avisar o usuário em dispositivos iOS supervisionados.
7. Selecione outras opções de configuração, se necessário.

Na página de informações de token seguro Apps and Books, os seguintes detalhes do token são exibidos:

- Data de criação
- Local (se o token contiver essas informações)

- Data de expiração

Adicionando contas Apps and Books

Ivanti Neurons for MDM permite adicionar várias contas de Apps and Books ao adicionar vários tokens seguros de Apps and Books em um único espaço.

Siga estas instruções para adicionar um token seguro do Apps and Books a um espaço:

1. Acesse **Apps > Apps and Books da Apple**.
2. Clique em **+ Adicionar sToken do Apps and Books**.
3. Digite um nome e escolha um arquivo de token.
4. Caso queira, desmarque a opção **Distribuir automaticamente aplicativos Apps and Books a todos os usuários**. Essa opção é selecionada por padrão, caso em que o grupo Todos os usuários é usado para distribuir as licenças de FCFS.
5. Você também pode marcar a opção **Apagar todos os dados da licença do Apps and Books anterior** para remover todas as licenças de aplicativo associadas a este token.
6. Clique em **Salvar**.

Após a adição da conta, uma lista de todas as contas Apps and Books adicionadas é exibida na tabela.

Atualizando um token seguro de Apps and Books

Procedimento

1. Acesse **Apps > Apps and Books da Apple**.
2. Clique no nome da conta de Apps and Books.
3. Na guia Token, clique em **Atualizar sToken** (arquivo .stoken).
4. Digite o nome do token e escolha um arquivo de token.
5. Caso queira, desmarque a opção **Distribuir automaticamente aplicativos Apps and Books a todos os usuários**. Essa opção é selecionada por padrão, caso em que o grupo Todos os usuários é usado para distribuir as licenças de FCFS.

6. Você também pode marcar a opção **Apagar todos os dados da licença do Apps and Books anterior** para remover todas as licenças de aplicativo associadas a este token.
7. Clique em **Atualizar**.

Na guia Token, clique em **Informações de uso da licença de ressincronização de Apps and Books** para realizar uma sincronização completa de todas as informações de aplicativos e licenças do serviço Apps and Books da Apple. Esta ação é necessária apenas quando as informações de alocação de licenças no Ivanti Neurons for MDM não estão corretas. Essa divergência pode ocorrer devido a inconsistências nas APIs do Apps and Books da Apple.

Atualizando a prioridade de uma conta Apps and Books

Administradores podem atribuir uma prioridade a cada conta Apps and Books em um espaço, com base na qual as licenças serão consumidas. As prioridades das contas Apps and Books são usadas para ter um sistema de distribuição de licenças previsível e para solucionar conflitos quando um usuário ou um dispositivo pode receber uma licença do mesmo aplicativo de mais de uma conta.

Procedimento

1. Acesse **Apps > Apps and Books da Apple**.
2. Clique em **Editar prioridade** para o nome da conta Apps and Books.
3. Na janela Editar prioridade, selecione uma nova prioridade.
4. Clique em **Salvar**.

Excluindo um token seguro de Apps and Books

Remover um token seguro de Apps and Books é irreversível e destrutivo. Quando um token é removido:

- Os aplicativos com tokens reservados terão seus tokens removidos.
- Os apps pagos permanecerão no catálogo e os usuários poderão pagar por eles.
- Os aplicativos que foram instalados por usuários finais por meio desta conta corporativa do Apps and Books precisarão mudar para contas pessoais se os usuários quiserem usá-los. Os usuários têm um período de tolerância de 30 dias para fazer isso.

Procedimento

1. Acesse **Apps > Apps and Books da Apple**.
2. Clique no nome da conta de Apps and Books.
3. Na guia Token, clique em **Excluir**.
4. Na janela Excluir token seguro de Apps and Books, selecione a opção **Sim, excluir o token seguro de Apps and Books** para confirmar.
5. Clique em **Excluir**.

Distribuindo licenças para um aplicativo Apps and Books no catálogo

1. Selecione **Apps > Apps and Books da Apple** no menu principal.

   É exibida uma lista de contas Apps and Books. Abaixo de cada conta, é exibida uma lista dos aplicativos comprados por meio do programa Apps and Books.
2. Selecione um aplicativo e clique em **Distribuir licenças**.
3. Escolha uma opção de distribuição, **Ordem de chegada**, **Reservado** ou **Proibido** na seção Licenças do Apps and Books.

Exibição de licenças de aplicativo por usuário

Para visualizar as preferências de licença dos usuários, use a guia Uso de licença.

1. Clique na guia **Usuários**
2. Selecione um usuário.
3. Clique na guia **Uso da licença**.

   Uma lista de aplicativos é exibida com o tipo de licença do Apps and Books e detalhes de atribuição da licença.

Para exibir o uso da licença para cada aplicativo por usuário:

1. Vá para **Usuários** no menu principal do Ivanti Neurons for MDM.
2. Selecione um usuário.

   A guia **Dispositivos** é exibida por padrão.

3. Clique na guia **Uso de licença**.

   Uma lista dos aplicativos instalados no dispositivo do usuário é exibida, incluindo o status da licença. O número de série do dispositivo é listado na coluna Tipo de licença do Apps and Books para licenças baseadas em dispositivo.

   - Nome do aplicativo
   - Versão do aplicativo
   - Custo do aplicativo
   - Data em que o aplicativo foi atribuído
   - Tipo de licença do Apps and Books
   - Ações (Status da licença.)

Você também pode exibir o uso da licença Apps and Books para cada aplicativo:

1. Acesse **Aplicativo > Catálogo de aplicativos** no menu principal do Ivanti Neurons for MDM.
2. Selecione um aplicativo.
3. Clique na guia **Licenças do Apps and Books**, se presente.
4. Clique no nome de uma conta. Somente aplicativos comprados por meio do programa Apps and Books são exibidos nesta guia.

   Uma guia separada para cada tipo de licença do Apps and Books é exibida.

Tipo de licença e registro	Descrição
Ordem de chegada (FCFS) - Você tem a opção de selecionar quais grupos de usuário receberão este tipo de licença.	• Aplicativos solicitados pelo usuário - Os aplicativos que o usuário escolhe instalar. Uma licença baseada em usuário é o padrão • App obrigatórios – Os apps que são obrigatórios e são instalados por uma definição de administrador usando a configuração **Instalar no dispositivo**. Estes apps usam licenças baseadas em dispositivo por padrão.
Reservada	Licenças reservadas têm prioridade sobre as licenças FCFS. Aqui você pode selecionar os usuários ou dispositivos que terão uma licença Reservada para o aplicativo.
Proibido	Insira os usuários que não têm permissão para possuir uma licença para este aplicativo. Este usuário poderá instalar o aplicativo, mas deverá comprá-lo.
Registro de atividade	Exibe o usuário, o tipo de licença Apps and Books atribuída a ele, a data em que ela foi atribuída e a última ação tomada em relação à licença.

Para exibir o uso detalhado da licença para cada aplicativo por dispositivo:

1. Vá para **Dispositivos** no menu principal do Ivanti Neurons for MDM.
2. Selecione um dispositivo.
3. Clique na guia **Apps instalados**.

Uma lista dos apps gerenciados no dispositivo selecionado é exibida, incluindo o status da licença.

- Nome do aplicativo
- Versão do aplicativo
- Plataformas suportadas
- Fonte do aplicativo
- Tamanho do aplicativo
- Tipo de licença do Apps and Books
- Data de relatório (instalação) do aplicativo para apps iOS

Notificações de uso da licença do Apps and Books

As notificações de Apps and Books ajudam a rastrear o uso da licença do Apps and Books. Os limites das notificações são definidos como:

- Uma notificação de informação é emitida quando mais de 50% das licenças foram usados.
- Uma notificação de alerta é emitida quando 70 a 80% das licenças foram usados.
- Uma notificação crítica é emitida quando 90 a 100% das licenças foram usados.
- As notificações são excluídas quando o uso cai para menos de 50%.

Para exibir as informações de licença para cada aplicativo:

1. Clique em **Apps > Apps and Books da Apple**.

   As informações da licença são exibidas, incluindo:

   - O nome do aplicativo.
   - O custo da licença.
   - O número de licenças disponíveis.
   - O número de licenças resgatadas.

2. Acesse **Painel > Notificações** para exibir os detalhes da notificação de licença.

   A página Notificações será exibida.

3. Clique no título da notificação para ver os detalhes. Consulte o Painel para as notificações disponíveis.

Notificações de uso da licença do Apps and Books

Indicador	Severidade	Tipo de notificação	Tipo de componente
50% resgatadas	Informações	Uso da licença	Apps and Books
70% resgatadas	Aviso	Uso da licença	Apps and Books
80% resgatadas	Aviso	Uso da licença	Apps and Books
90% resgatadas	Alerta	Uso da licença	Apps and Books
100% resgatadas	Alerta	Uso da licença	Apps and Books

Visualizando o uso da licença Apps and Books

Os detalhes de uso da licença específicos para um usuário são exibidos na tabela de uso da licença na coluna licença.

1. Clique em um aplicativo.
2. Clique na guia **Uso da licença**.
3. Insira um nome de usuário no campo de busca.

Revogando a licença Apps and Books de um aplicativo

As licenças de Apps and Books são revogadas quando:

- Um dispositivo está inativo (desativado ou apagado).
- O aplicativo Apps and Books é excluído.
- A licença baseada em dispositivo é revogada quando um dispositivo é desativado.
- O token Apps and Books é excluído.

Para revogar uma licença de Apps and Books para um aplicativo:

1. Selecione o aplicativo em **Apps > Catálogo de aplicativos**.
2. Clique na guia **Licenças do Apps and Books da Apple**, se presente.
3. Realize uma das seguintes tarefas:
   a. Clique em **Revogar todas as licenças** para revogar todas as licenças de todos os usuários ou dispositivos.
   b. Clique na guia **Activity Log**. Use a coluna **Ações** para revogar licenças individuais por usuário ou por dispositivo.

- Para dispositivos iOS, a Apple permite um período gratuito de 30 dias para aplicativos Apps and Books depois que a licença do Apps and Books for revogada. Portanto, o aplicativo Apps and Books permanece instalável.
- Para dispositivos macOS, após a revogação da licença Apps and Books, o aplicativo permanece no dispositivo.

Para revogar uma licença de Apps and Books para um usuário:

1. Clique em um aplicativo.
2. Clique na guia **Uso da licença**.
3. Clique no link **Revogar licença** para o usuário que deve ter o acesso à licença removido.

As licenças do Apps and Books serão revogadas automaticamente se o usuário for excluído ou se ele remover o perfil MDM do dispositivo.

Notificações de erro de autenticação de Apps and Books

Alguns erros de autenticações podem ocorrer ao usar o serviço Apps and Books da Apple. Essas notificações de erros de autenticação do Apps and Books são:

Notificação de Erro	Ação
Token de Autenticação Inválido	Como carregar um sToken de Apps and Books válido
Token Expirado	Gere um novo token online usando a conta da sua empresa
O sToken foi revogado	Como carregar um Apps and Books válido
Login necessário	Faça login no serviço Apps and Books

Comportamento do Apps and Books para dispositivos macOS e iOS

Apps and Books para iOS

Ação	Licença baseada em dispositivo	Licença baseada em usuário
Remover o aplicativo Apps and Books da distribuição para o usuário	O aplicativo é desinstalado no dispositivo do usuário	O aplicativo é desinstalado no dispositivo do usuário
Desautorizar o aplicativo Apps and Books	O aplicativo é desinstalado de todos os dispositivos em espaços que não são padrão	O aplicativo é desinstalado de todos os dispositivos em espaços que não são padrão
Como excluir o aplicativo Apps and Books do espaço padrão ou personalizado	O aplicativo é desinstalado de todos os dispositivos	O aplicativo é desinstalado de todos os dispositivos

Apps and Books para macOS

Ação	Licença baseada em dispositivo	Licença baseada em usuário
Remover o aplicativo Apps and Books da distribuição para o usuário	O aplicativo não é desinstalado no dispositivo do usuário	N/D
Desautorizar o aplicativo Apps and Books	O aplicativo não é desinstalado de todos os dispositivos em espaços que não são padrão	N/D
Como excluir o aplicativo Apps and Books do espaço padrão ou personalizado	O aplicativo não é desinstalado de todos os dispositivos	N/D

Direito de licença do Apps and Books quando um dispositivo move espaços

Quando um dispositivo é transferido para um novo espaço, a licença de Apps and Books atribuída ao dispositivo ou a seu proprietário é revogada. Uma nova licença de Apps and Books é atribuída de acordo com a disponibilidade no novo espaço.

Veja a seguir os cenários de direitos de licença do Apps and Books:

Cenário	Titularidade
Uma licença do Apps and Books é atribuída a um dispositivo ou ao proprietário de um dispositivo no espaço de origem e uma licença do Apps and Books do mesmo aplicativo está disponível no espaço de destino.	Atribua uma licença do token do Apps and Books no espaço de destino.
Uma licença do Apps and Books é atribuída a um dispositivo ou ao proprietário de um dispositivo no espaço de origem e nenhuma licença do Apps and Books do mesmo aplicativo está disponível no espaço de destino.	Revogue a licença do token do Apps and Books no espaço de origem.
Nenhuma licença do Apps and Books é atribuída a um dispositivo ou proprietário de um dispositivo no espaço de origem e uma licença do Apps and Books para qualquer aplicativo Apps and Books instalado está disponível no espaço de destino.	Atribua uma licença do token do Apps and Books no espaço de destino.

Se você não conseguir executar tarefas na página das **Categorias de aplicativo,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de aplicativo e conteúdo

Configurações do catálogo

Esta seção contém os seguintes tópicos:

Na página **Aplicativos** > **Configurações do catálogo**, configure as preferências a serem aplicadas a todos os aplicativos do seu catálogo. Você pode fazer o seguinte:

- Incluir atualizações do aplicativo durante o registro do dispositivo
- Impedir backup no iCloud e iTunes (somente iOS)
- Configurar região da App Store padrão (Apple e Microsoft)
- Remover apps iOS quando o dispositivo não estiver registrado
- Habilitar as "Classificações e opiniões" do Ivanti Neurons for MDM
- Carregar tokens de Apps and Books em iOS e macOS (requer licença Gold)

Alterando as configurações de gerenciamento de aplicativos Apple

Essas configurações serão aplicadas a todos os apps, a menos que a configuração de gerenciamento de um aplicativo tenha sido criada para apps individuais.

1. Marque ou desmarque uma ou mais das seguintes caixas de seleção:
    - **Atualizar aplicativos durante o check-in do dispositivo** (selecionado por padrão)
    - **Impedir backup no iCloud e iTunes**
    - **Remover aplicativos mediante cancelamento do registro**
2. Clique em **Salvar**.

Notificações

1. Clique na lista suspensa em **Gerar notificação do sistema quando novas versões de aplicativo estiverem disponíveis na Apple App Store e na Google Play Store**e selecione uma das seguintes opções:
    - **Uma vez por semana**
    - **Uma vez por dia**
2. Clique na lista suspensa em **Gerar notificação ao usuário final para novas atualizações de aplicativos disponíveis no AppCatalog** e selecione uma das opções:
    - **Uma vez por semana**
    - **Uma vez por dia**

Definindo a região padrão da App Store

Nas configurações do App Catalog, defina a região padrão para as App Stores da Apple e Microsoft.

1. Na seção Região da App Store padrão:
    - Selecione **Região da loja de aplicativos da Apple**.
    - Selecione **Região da loja de aplicativos da Microsoft**.

2. Selecione ou desmarque a opção de usar a última região selecionada da App Store como a região padrão para cada administrador. Se essa opção estiver selecionada, então a região da App Store será definida como a última região selecionada por cada administrador e substituirá as configurações anteriores. Se essa for a primeira vez que um administrador estiver usando esse recurso, então as regiões de armazenamento de aplicativos padrão serão definidas para as configurações anteriores nesse procedimento.
3. Clique em **Salvar**.

Habilitar/Desabilitar atualizações de aplicativo iOS

1. Selecione ou desmarque **Atualizar aplicativos durante o check-in do dispositivo.**
   - Por padrão, esta opção está selecionada.
   - Quando desmarcada, nenhum check-in de dispositivo (inclusive check-in forçado pelo administrador) incluirá atualizações de aplicativo.
   - No entanto, o usuário pode atualizar manualmente o aplicativo clicando na ação Forçar check-in, no catálogo de aplicativos do dispositivo.
   - As novas instalações de aplicativos e todas as outras configurações e definições serão atualizadas durante o check-in do dispositivo.
2. Clique em **Salvar**.

Para um aplicativo gerenciado, o administrador pode clicar no botão **Atualizar** na página de detalhes do aplicativo para atualizar manualmente o aplicativo com a versão mais recente da App Store.

No dispositivo de um usuário, o usuário pode clicar no botão **Forçar check-in** no menu App Catalog para deixar o dispositivo fazer check-in e permitir as atualizações de aplicativo junto com outras configurações e atualizações.

Juntas, essas configurações permitem que os usuários finais escolham quando seus apps serão atualizados:

- Aguarde até estar conectado ao Wi-Fi para evitar cobranças de dados.
- Evite ser bloqueado no momento errado durante as atualizações do aplicativo.

Habilitar/Desabilitar classificações e análises do aplicativo

Isso permitirá que os usuários classifiquem e emitam opiniões sobre os aplicativos e que outros usuários leiam esses comentários.

1. Selecione ou desmarque **Habilitar classificações e opiniões no App Catalog do usuário final**.
2. Clique em **Salvar**.

O formato do sToken do Apps and Books foi alterado. Em vez de uma cadeia de caracteres como a das versões anteriores, agora a cadeia de caracteres é armazenada em um arquivo de texto no formato vpptoken. Envie este arquivo diretamente para o console do administrador para que ele seja processado. A página da conta do Apps and Books foi atualizada para exibir o nome da organização do Apps and Books e as datas de expiração.

Carregar ou atualizar um sToken do Apps and Books em iOS/macOS (Licença: Gold)

1. Selecione **Adicionar sToken do Apps and Books**.
2. Insira um nome para o arquivo sToken no campo **Nome do alias**.
3. Arraste e solte o arquivo sToken para a área especificada ou clique em **Escolher arquivo** para navegar até o arquivo sToken.
4. Clique em **Salvar**, ou, se você estiver atualizando um arquivo sToken, clique em **Atualizar**.
5. Acesse a página Apple Apps and Books para visualizar os aplicativos associados a este token.

Se os tokens do Apps and Books tiverem sido reservados para usuários individuais em uma versão anterior do Ivanti Neurons for MDM, você precisa confirmar se eles ainda estão reservados para esses usuários e, se necessário, reservá-los novamente.

Remover um sToken de Apps and Books em iOS/macOS do seu serviço Ivanti Neurons for MDM

Você pode revogar um aplicativo que não é mais necessário por um usuário e transferi-lo conforme necessário. Se o aplicativo foi implantado como um aplicativo gerenciado com MDM para iOS/macOS, então você terá a opção de remover o aplicativo e todos os dados imediatamente.

1. Selecione um aplicativo para remover.
2. Clique em **Excluir**.
   Uma caixa de diálogo de alerta aparecerá.
3. Como alternativa, você poderá fornecer ao usuário um período de 30 dias de cortesia para:
   - Salvar seus dados.
   - Comprar uma cópia pessoal do aplicativo.
   - Transferir aplicativos que eles instalaram por esta conta Apps and Books para suas contas pessoais para continuarem a usá-los.

Se você não conseguir executar tarefas na página **Configurações de catálogo,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de aplicativo e conteúdo

Implantando dependências de aplicativo

Ao fazer upload de um pacote de aplicativo interno, o Ivanti Neurons for MDM verifica o aplicativo para identificar dependência. Se alguma dependência for encontrada, ele a listará na terceira etapa do Assistente para adicionar aplicativo. Para qualquer dependência do aplicativo, os administradores podem optar por fazer upload de um arquivo de dependência. No entanto, alguns apps podem não ser instalados sem o upload do arquivo de dependência.

O administrador tem a opção de definir a dependência ao instalar um app específico. Nesse caso, pode haver um ou mais aplicativos marcados com o aplicativo principal. Quando o usuário tentar instalar o aplicativo principal, será notificado sobre os aplicativos dependentes que serão instalados com o aplicativo principal.

 Este recurso é compatível apenas com dispositivos iOS, Android, Windows e macOS.

Observe os seguintes pontos sobre dependências e pré-requisitos do aplicativo:

- O administrador pode definir os apps dependentes que são pré-requisitos antes que um aplicativo possa ser instalado em um dispositivo. O aplicativo de pré-requisito pode ser um aplicativo interno, público, privado (Android) ou VPP.
- A contagem de apps de pré-requisito será, então, exibida na coluna Apps de pré-requisito na página App Catalog. Você pode passar o mouse sobre o número para visualizar a lista de apps de pré-requisito.
- Um aplicativo de pré-requisito é baixado diretamente assim que o aplicativo principal for acionado para instalação.
- Se um aplicativo principal for delegado, os apps de pré-requisito associados serão autodelegados.
- Não é possível excluir um aplicativo de pré-requisito do App Catalog até que a relação de pré-requisito seja removida.
- Diversas versões de um aplicativo podem ter diferentes apps de pré-requisito.
- A página Trilhas de Auditoria registra a adição, remoção e delegação automática de aplicativos de pré-requisito para iOS, Android e macOS.

- Se o administrador ou o usuário final instalar um aplicativo que tenha apps de pré-requisito, os apps de pré-requisito são instalados antes do aplicativo principal ser instalado. Se o registro de um dispositivo ocorrer antes de todos os apps de pré-requisito serem instalados, todos os apps de pré-requisito serão desinstalados.

Embora um aplicativo precise de um arquivo de dependência, o Ivanti Neurons for MDM não requer que você faça o upload de nenhum arquivo para implantar um aplicativo.

Para dispositivos Samsung, o administrador deve adicionar os aplicativos de pré-requisito à lista de aplicativos permitidos no de modo quiosque. Os aplicativos de pré-requisito adicionados à lista de aplicativos permitidos não são adicionados à lista de aplicativos proibidos.

Para dispositivos não Samsung, se o aplicativo principal for adicionado à lista de aplicativos permitidos no modo de quiosque, o aplicativo de pré-requisito deve ser executado silenciosamente em segundo plano. Você pode visualizar o aplicativo de pré-requisito no modo de quiosque somente se o administrador definir o aplicativo nesse modo.

Dispositivos Windows - se o aplicativo Bridge for um aplicativo de pré-requisito não distribuído e o aplicativo principal for um .exe distribuído silenciosamente. Quando a dependência for removida, o aplicativo Bridge será desinstalado, mas o .exe falhará após essa etapa. O administrador deve certificar-se de que o aplicativo Bridge não seja distribuído por padrão.

Dispositivos Windows - quando o aplicativo principal é distribuído em modo não silencioso e tem um aplicativo de pré-requisito sem distribuição, o aplicativo de pré-requisito é instalado primeiro e é bem-sucedido. No entanto, caso o aplicativo principal não seja instalado, o aplicativo de pré-requisito é imediatamente desinstalado. A repetição do aplicativo principal com falha ocorre apenas quando o usuário aciona uma solicitação de instalação.

Adicionar um aplicativo interno

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **Adicionar**.
3. Arraste o arquivo do aplicativo até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo em seu sistema e clique em **Confirmar**.

4. Clique em **Avançar** (inferior direito). O Ivanti Neurons for MDM verifica o aplicativo em busca de arquivos de dependência e lista-os na tabela **Dependências do aplicativo**.
5. Revise as informações do aplicativo e verifique se você selecionou o aplicativo correto.
6. Clique no ícone Upload na coluna **Ações**. A janela **Dependência de upload** é exibida.
7. Clique em **Escolher arquivo** para procurar e localizar uma cópia local do arquivo e clique em **Upload**.
8. O Ivanti Neurons for MDM busca pacotes opcionais para o aplicativo, se houver, e os lista na tabela Pacotes opcionais. Se estiver listado, clique no ícone Upload na coluna Ações. A janela Fazer upload de pacote opcional é exibida.
9. Revise as informações do aplicativo e confirme se você selecionou o aplicativo correto.
10. Clique em **Escolher arquivo** para procurar e localizar uma cópia local do arquivo e clique em Upload.
11. Clique em **Avançar**.
12. (Opcional) Adicione capturas de tela do aplicativo e clique em **Avançar**
13. Se o aplicativo precisar de outros apps de pré-requisito.
    a. Selecione a opção **Ligado** na seção **Apps de pré-requisito**.
    b. Procure o aplicativo de pré-requisito na guia **Add Apps**.
    c. Selecione os apps.
    d. Clique em **Salvar**.
14. Defina a distribuição do aplicativo e clique em **Avançar**.
15. Defina a seção Configuração do aplicativo e clique em **Concluído**. Na próxima vez em que os dispositivos forem sincronizados com o Ivanti Neurons for MDM, o aplicativo será implantado no dispositivo junto com os arquivos dependentes.

> Você pode adicionar mais dependências clicando no botão Adicionar dependências. Quando carregadas, essas dependências também são listadas na tabela Dependências do aplicativo. O administrador também pode adicionar manualmente o pacote opcional apenas com o tipo de conteúdo. Este tipo de pacote não depende de versão.

Adicionar um aplicativo de pré-requisito

É possível adicionar um aplicativo de pré-requisito a um aplicativo principal. É possível adicionar diferentes pré-requisitos para diferentes versões de um aplicativo principal. A página App Catalog fornece a opção de manter a descrição, os scripts, as capturas de tela, a distribuição, os pré-requisitos do aplicativo e as configurações do aplicativo iguais à versão existente do aplicativo ou alterar os apps requeridos associados. Não é possível excluir um aplicativo de pré-requisito sem remover a associação com o aplicativo principal.

A página Trilha de auditoria agora exibe os apps de pré-requisito com suporte em campos específicos da seguinte forma:

A seção Aplicativos de Pré-requisito para os aplicativos iOS, Android, e macOS compatíveis na página Trilhas de Auditoria exibe os seguintes campos:

- appVersionId
- nome
- platformAppId

Os apps de pré-requisito que são delegados automaticamente ou não delegados que contêm os campos a seguir são exibidos:

- dmPartitionDistributionType
- dmPartitionDistributionReason

Procedimento

1. Selecione um aplicativo no **App Catalog**.
2. Clique em **Editar**.
3. Role para baixo até **Delegação do aplicativo** e selecione a opção **Delegar este aplicativo a todos os espaços**.
4. Clique em **Salvar**.

> Se você delegar diversos apps e optar por remover delegação do aplicativo principal, o aplicativo de pré-requisito não será removido da delegação automaticamente.

Implementação do Divide Productivity com Android Enterprise

O Divide Productivity é um aplicativo PIM que você pode implantar em dispositivos Android Enterprise.

1. Acesse **Apps > Catálogo de aplicativos**.
2. Em **Aplicativos comerciais**, clique em **Divide Productivity**.
3. Insira categorias adicionais ou uma descrição.
4. Clique em **Avançar**.
5. Aceite as permissões exibidas.
6. Clique em **Avançar**.
7. Selecione uma opção de distribuição.
8. Expanda **Opções avançadas e configuração do aplicativo**.
9. Use as diretrizes a seguir para habilitar as opções:

Configuração	O que fazer
Bloqueia a desinstalação do aplicativo pelo usuário	Selecione para impedir a desinstalação do aplicativo pelo usuário final, quando ele tiver sido instalado no modo silencioso.
Endereço de e-mail	Use variáveis para definir o endereço de e-mail que será associado ao aplicativo.
Senha	Use a variável para definir a senha para a conta de e-mail. Se este campo for deixado em branco, o usuário será notificado a inserir a senha.
Host	Insira o nome do host do servidor de e-mail que será usado. Insira o nome de domínio totalmente qualificado do servidor do ActiveSync. Se estiver usando um Sentry Autônomo, insira seu nome de domínio totalmente qualificado (FQDN). Por exemplo: mySentry.mycompany.com
Tipo de servidor	Selecione o tipo de servidor de e-mail.
Nome de Usuário	Use variáveis para definir o nome de usuário para a conta de e-mail.
O SSL é obrigatório?	Selecione se desejar ter uma comunicação segura usando https no servidor especificado no campo Host.
Confiar em todos os certificados	Selecione apenas se desejar que o aplicativo aceite automaticamente certificados não confiáveis. Geralmente, essa opção é selecionada ao trabalhar em um ambiente de teste.

Configuração	O que fazer
Assinatura de e-mail padrão	Insira a assinatura de e-mail padrão para todos os e-mails. O usuário final poderá alterar esse item a qualquer momento. Depois que o usuário final alterar esse campo, as alterações posteriores nesse campo não terão efeito.
Tamanho máximo do anexo de e-mail	Insira o tamanho máximo que será permitido para arquivos anexos.
Habilitar tarefa	Selecione para sincronizar tarefas.
Alias de certificado de login	Insira o alias do certificado de login.
Certificado de assinatura do Smime Alias	Não suportado atualmente.
Certificado de criptografia do Smime Alias	Não suportado atualmente.
Opções avançadas	
Instalar no dispositivo	Selecione para notificar o usuário a instalar o aplicativo.
Instalar silenciosamente em dispositivos Samsung Knox	Selecione para instalar o app automaticamente em dispositivos Samsung Knox.
Não exibir o aplicativo no App Catalog do usuário final	Selecione caso não deseje que o aplicativo seja exibido no catálogo de aplicativos do dispositivo.

10. Selecione uma opção de promoção.
11. Clique em **Concluído** .

Configuração do aplicativo Provisioner

Esta seção contém os seguintes tópicos:

O Provisioner é um aplicativo do Ivanti Neurons for MDM usado para provisionar dispositivos de propriedade da empresa para que eles possam ser registrados como dispositivos gerenciados de trabalho e colocados no modo de Proprietário do dispositivo.

Um dispositivo gerenciado pela empresa possui somente um perfil corporativo e nenhum perfil profissional. O administrador pode definir até vinte bloqueios no dispositivo, o que pode restringir as funções do dispositivo , tais como câmera, chamadas, SMS, rede e outras.

O aplicativo Provisioner é obrigatório no aparelho que iniciará a configuração do dispositivo Android Enterprise de destino com um toque NFC. Para fornecer dispositivos de propriedade da empresa, instale o aplicativo Provisioner em um dispositivo principal, e use a entrada NFC (Comunicação por campo de proximidade) para fornecer novos dispositivos. A entrada está utilizando os dois dispositivos em conjunto. Os dispositivos podem ser provisionados para usar um destes apps cliente:

- Go para usar com o Ivanti Neurons for MDM
- At Work UEM, um aplicativo cliente sem marca, para ser usado com o Ivanti Neurons for MDM.

Requisitos de fornecimento

Para provisionar um dispositivo Android Enterprise de propriedade da empresa como um dispositivo gerenciado de trabalho:

- Dispositivos de propriedade da empresa nativamente compatíveis com Android Enterprise devem ser restaurados às configurações de fábrica antes do provisionamento.

- A configuração do Android Enterprise deve ser definida e aplicada ao grupo de dispositivos com Android.
- Um dispositivo Android com capacidade de NFC projetado para ser utilizado como o principal ou como modelo, com o aplicativo Provisioner instalado.
- Dispositivos compatíveis com Android Enterprise a serem provisionados.
- Aplicativo Provisioner
  Baixe o aplicativo Provisioner para Android no Google Play.

Habilitar Android Beam para usar a entrada NFC

Procedimento

1. Acesse **Configurações** no dispositivo.
2. Acesse **Wireless e redes** e clique em **Mais**.
3. Marque a caixa de seleção **NFC**.
4. Clique em **Android Beam** e deslize o botão para **Ligado**.

As etapas exatas podem ser ligeiramente diferentes em seu dispositivo.

Fornecer um dispositivo de propriedade da empresa

Procedimento

1. Instale o aplicativo Provisioner no dispositivo a ser usado como o dispositivo Android principal.
2. Fornecedor de lançamento no dispositivo principal.
3. Selecione um aplicativo no menu suspenso.

4. Insira as informações solicitadas pelo aplicativo Provisioner. Alguns campos podem ser preenchidos automaticamente se algum tipo de Wi-Fi suportado estiver presente. Use estas orientações:

Campo	Valor
Selecionar aplicativo para o fornecimento	Go (selecione para usar com o Ivanti Neurons for MDM) At Work UEM (aplicativo cliente sem marca; selecione para uso com Ivanti Neurons for MDM com marca).
SSID de rede de Wi-Fi	Insira o SSID de Wi-Fi que o dispositivo principal deve usar.
Tipo de segurança Wi-Fi	Insira o tipo de segurança Wi-Fi
Senha Wi-Fi	Insira a senha do Wi-Fi
Fuso horário	Insira o fuso horário local atual
Local	Insira o local

5. Clique em **Continuar**.
   A tela **Tocar os dispositivos** será exibida no dispositivo principal.

6. Com o dispositivo alvo ligado e exibindo a tela de Boas Vindas do Android, pressione o dispositivo principal sucessivamente com o dispositivo alvo para iniciar uma transferência de NFC.
   Se a transferência de NFC for realizada com êxito, o dispositivo alvo poderá emitir um som e, em seguida, proceder para fazer o download do aplicativo cliente escolhido. Se o dispositivo não estiver criptografado, ele iniciará o processo de criptografia antes de continuar.

7. Continue fornecendo dispositivos adicionais tocando os dispositivos. O dispositivo alvo deve exibir a tela de Boas-Vindas, e o dispositivo principal deve exibir a tela **Tocar dispositivos**.

Registrar o dispositivo

Quando o dispositivo de propriedade da empresa tiver sido provisionado usando o incremento NFC, ele terá o aplicativo cliente selecionado instalado. Ative o aplicativo cliente e registre o dispositivo.

Verificar o status de registro do dispositivo

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Clique no link para um dispositivo para visualizar os detalhes.
3. O status do dispositivo será listado no painel à esquerda.

Gerenciar aplicativos Windows

Os usuários podem gerenciar o ciclo de vida completo (importação, configuração, agendamento, distribuição, atualização e remoção) de aplicativos Windows. Os processos de distribuição e atualização de aplicativos têm suporte por meio do console MDM. Para mais detalhes sobre como gerenciar aplicativos Windows e outros aplicativos, consulte "Configuração do aplicativo" na página 354, "Percepção de aplicativo" na página 52 e "App Catalog" na página 301.

Tipos de aplicativos suportados

- Interno (verifique as opções em **Adicionando um aplicativo interno** na seção "App Catalog" na página 301)
- MSB (integração do Microsoft Store for Business)
- Loja pública (via integração nativa da Microsoft Store). A região da Microsoft Store pode ser definida em Aplicativos > Configurações do catálogo. Para mais informações, consulte **Adicionando um aplicativo de uma loja pública** na seção "App Catalog" na página 301.

Extensões de aplicativo suportadas

- MSI
- MSIX
- APPX
- Pacotes APPX
- EXE (via "Ivanti Bridge" na página 429)

Controle de aplicativo

A configuração Controle de Aplicativo controla a instalação do aplicativo em cada dispositivo. Para mais informações, consulte "Configuração de controle do aplicativo: Controle os apps que serão instalados por dispositivo" na página 470.

Pacotes e dependências

Estão disponíveis os seguintes recursos diferentes:

1. Aplicativos do Windows podem ser definidos como pré-requisitos para todos os tipos de aplicativo. Para informações sobre como definir pré-requisitos de aplicativo, consulte "Implantando dependências de aplicativo" na página 414.
2. As dependências em Dependências do Aplicativo e Outros Pacotes de APPX e pacotes APPX. Na página "Visualizando detalhes do aplicativo" na página 351, revise a seção Dependências do Aplicativo e Outros Pacotes.
3. Os aplicativos Win32 suportam a seleção do código de produto correto (MSIs), linhas de comando e variáveis. Uma lista com opções comuns de linha de comando pode ser encontrada aqui.

Scripts

Os scripts são suportados via cliente Ivanti Bridge. Para informações sobre como configurar os Scripts, consulte o "Ivanti Bridge" na página 429

Assim que o Ivanti Bridge estiver instalado nos dispositivos, os scripts podem ser distribuídos da seguinte forma:

- No nível do dispositivo, com Scripts e Ações via ação do Ivanti Bridge
- Via configuração do Ivanti Bridge (acesse Configurações > Bridge)

Scripts e arquivos pré e pós-instalação

Para arquivos .exe e .MSI

Você pode configurar scripts de pré e pós-instalação do PowerShell, scripts de registro e arquivos executáveis do Windows (.exe), bem como baixar outros tipos de arquivo para apps Windows no nível de Detalhes do Aplicativo.

Ao adicionar um novo script ou arquivo de pré ou pós-instalação, a tela do Ivanti Bridge é exibida. Você pode anexar o script ou arquivo, adicionar um argumento de script e também fornecer um local de destino para os arquivos. O script de pré-instalação deve ser executado com sucesso no dispositivo antes de se enviar o comando de instalação do aplicativo para o dispositivo. Os scripts e arquivos pré e pós-instalação serão executados/instalados na mesma ordem em que foram carregados no console. Se o download ou a instalação do script de pré-instalação falhar, a instalação do aplicativo não poderá prosseguir.

Se o script de pós-instalação falhar, você poderá visualizar os erros na página de detalhes do dispositivo na seção Logs do dispositivo. Além disso, você não pode reverter os scripts de pré-instalação/arquivos baixados nem os arquivos .exe instalados caso as ações de pós-instalação falhem.

Você pode reordenar os scripts e arquivos de pré ou pós-instalação usando a opção Priorizar Scripts e Arquivos. Essa opção estará disponível apenas se houver pelo menos dois ou mais scripts ou arquivos disponíveis. Usando essa opção, você pode arrastar e soltar os arquivos ou scripts dentro de suas respectivas seções, pré ou pós, e não de uma seção para outra.

Comportamento e configurações de instalação

Aplicativos Windows suportam os seguintes recursos:

- Instalações silenciosas
- "Programação de aplicativo do Windows" na página 1071
- Opções de reinicialização

Para mais detalhes sobre as opções de comportamento de instalação, consulte "Configuração do aplicativo" na página 354

Aplicativos MSI e EXE (instalados usando o Bridge) oferecem suporte a instalações com sessões MDM sem usuário.

Por exemplo, nos seguintes cenários:

- O dispositivo foi reiniciado e ainda não há nenhum usuário conectado
- O usuário saiu da sessão do Windows
- O dispositivo foi inscrito no modo Autopilot sem usuário (autoimplantação ou pré-provisionamento)
- Os aplicativos são instalados no nível do dispositivo

Permite instalar os aplicativos MSI de maneira mais eficiente, por exemplo, durante a inscrição do Autopilot ou durante a noite, quando ninguém estiver usando o dispositivo Windows. Quando se usa o reempacotamento simples para EXEs no MSI, ele pode ser instalado, mas não atualizado ou excluído. O pacote MSI real tem conexão com o CSP. Outros tipos de aplicativos serão instalados depois que o usuário fizer login.

Tunnel for Windows (VPN por aplicativo)

O Tunnel é um aplicativo nativo autônomo do Windows. Está atualmente disponível na Microsoft Store para distribuição aos dispositivos. Cria uma configuração de VPN por Aplicativo. Necessário implantação do Sentry. Para configurar o aplicativo Tunnel, acesse **Configurações** > **+Adicionar** > procure Tunnel (escolha as configurações que suportem dispositivos Windows). Selecione o perfil do Sentry e defina as configurações para começar a fazer o tunneling dos dados do aplicativo pelo Sentry. Para configurar um Servidor Sentry, acesse **Administrador** > **Infraestrutura** > **Sentry**.

Inventário de aplicativos

O inventário de aplicativos e software instalado em sua frota de dispositivos Windows pode ser monitorado em dois níveis:

- Para verificar os aplicativos instalados em seus dispositivos, vá para **Dispositivos** > **Inventário de aplicativos**
- Para verificar o inventário no nível do dispositivo, vá para Dispositivos > escolha um dispositivo > clique em Aplicativos instalados

Os administradores podem definir intervalos para coleta de inventário de aplicativos Windows. Acesse Administrador > Windows > Intervalos de Inventário de Aplicativos. Os intervalos são usados quando a configuração de privacidade está definida para coletar todos os aplicativos do dispositivo. Para definir a Configuração de Privacidade, acesse Configurações > +Adicionar > procure Privacidade > escolha Coletar inventário de aplicativos para todos os aplicativos no dispositivo. Selecione os tipos de aplicativo a serem coletados.

Catálogo de Aplicativos Corporativos (Apps@Work)

Os clientes podem habilitar um Catálogo Corporativo em dispositivos Windows usando o Apps@Work. O Apps@Work é disponibilizado e implantado por meio do Catálogo de Aplicativos no Neurons for UEM. Para mais informações, consulte "Apps@Work (iOS, Android, Windows e macOS)" na página 334.

Ivanti Bridge

Esta seção contém os seguintes tópicos:

O Ivanti Bridge unifica operações móveis e de desktop para o Windows 10 usando um único console e canal de comunicações. Ele estende os recursos do UEM ao gerenciamento de PCs e permite que as organizações aproveitem custos significativamente reduzidos e maior eficiência, garantindo segurança consistente em PCs e dispositivos móveis. Usando o Ivanti Bridge, as empresas podem usar um único protocolo para dispositivos desktop com Windows 10, tal como fazem para os dispositivos móveis Windows suportados, a fim de enviar informações aos aplicativos legados no SO.

O Ivanti Bridge permite que a TI modernize as operações do Windows em UEM sem abrir mão de funcionalidades críticas. A TI pode aplicar políticas e scripts que já existem sem precisar de uma imagem do sistema, mesclagem de domínio ou vários canais de comunicação com o dispositivo.

Com o Ivanti Bridge, as organizações agora podem:

- Ter controle total sobre os PCs com UEM
- Gerenciar PCs remotamente, over-the-air
- Reduzir a necessidade de criar imagens de desktops
- Aproveitar comandos baseados em GPO com scripts PowerShell implantados por UEM
- Editar e gerenciar Registry com facilidade
- Implementar sem esforço apps Win32 empacotados não MSI
- Obter visibilidade do sistema de arquivos

O Ivanti Bridge é usado somente com dispositivos desktop do Windows 10 Pro ou do Windows 10 Enterprise e não é compatível com processadores ARM. O Ivanti Bridge não é compatível com dispositivos desktop do Windows 10 Home.

Tipos de arquivos suportados pelo Bridge

O Ivanti Bridge inclui suporte para os seguintes tipos de arquivo:

- PowerShell

  Os scripts do PowerShell enviados por push para dispositivos que utilizam o suporte do Bridge são chamados de argumentos.

  Os scripts PowerShell de 64 bits são suportados em dispositivos Windows 10 Desktop de 64 bits.

  No lado do servidor, o tempo limite do Bridge para esperar o resultado após o envio de um script PowerShell ao dispositivo é cerca de 20 minutos. O tempo limite é registrado como uma falha. No entanto, o script no dispositivo continua funcionando.

  No lado do dispositivo, o tempo limite do Bridge para esperar o processo de execução de um script PowerShell é cerca de 60 minutos. Após 60 minutos, o processo será encerrado, nenhuma saída do script será salva e uma nova falha será enviada ao servidor.

  Os tempos limite do lado do servidor e do lado do dispositivo são registrados como falhas. Se o segundo tempo limite decorrer e o script gerar alguma saída, nenhuma saída será registrada no lado do servidor.

- Registro
- Scripts VB

- .EXE para implementação de aplicativo Win32

> Se os administradores precisarem enviar Arquivos Win32 (.EXE) para um dispositivo (por exemplo, como um aplicativo interno Windows), a funcionalidade Bridge será usada automaticamente se estiver disponível. É obrigatório inserir um argumento para executar o arquivo silenciosamente (por exemplo, /SILENT ou /VERYSILENT).
> Os aplicativos .EXE são instalados por meio do Bridge usando o modo Admin PowerShell. Em dispositivos Windows, para realizar a instalação usando as credenciais do usuário, selecione a opção "Executar como usuário".

Usando o Ivanti Bridge, o dispositivo pode ser aumentado nas seguintes áreas principais.

- **Registry:** Ler, gravar e atualizar os valores de registro.
- **Arquivos:** Verificar, ler e atualizar o conteúdo de um arquivo.
- **Implementação de aplicativo:** Adicionar a habilidade de instalar aplicativos com base em .EXE para o dispositivo desktop. Esses aplicativos podem residir nos servidores do Ivanti Neurons for MDM ou em uma Rede de Distribuição de Conteúdo (CDN) na nuvem.

Configuração do Bridge

A configuração do Ivanti Bridge exige que os administradores executem as etapas a seguir nesta ordem:

1. "Ativando licenças do Bridge" abaixo
2. "Instalação do aplicativo móvel Bridge" abaixo
3. "Carregando scripts nos dispositivos" na página seguinte para uso permanente ou único nos dispositivos.

Ativando licenças do Bridge

O Ivanti Bridge faz parte do pacote legado Gold e do pacote atual UEM Seguro.

Instalação do aplicativo móvel Bridge

Após a ativação das licenças do Ivanti Bridge, o aplicativo móvel do Bridge pode ser instalado da seguinte forma:

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **+Adicionar**.
3. Clique em **Ivanti Bridge** na seção Aplicativos Comerciais.
4. Adicione detalhes, personalize e distribua o aplicativo móvel Bridge para os dispositivos necessários conforme as licenças adquiridas.
   Se você tiver ativado a opção **Instalar silenciosamente em dispositivos Windows**, o aplicativo móvel Bridge será instalado silenciosamente, e o serviço Bridge começará a ser executado nos dispositivos.

O aplicativo Bridge é adicionado ao App Catalog por padrão e também distribuído por padrão para todos os dispositivos.

Carregando scripts nos dispositivos

Os administradores podem fazer o upload dos scripts para os dispositivos para uso permanente criando uma nova configuração do Bridge:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Ivanti Bridge**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela da etapa 7.
   1. Insira as configurações da categoria **Arquivo de script** para especificar um script de instalação a ser enviado ou executado nos dispositivos.
   2. (Opcional) Insira as configurações da categoria **Desfazer arquivo de script** para especificar um script de desinstalação a ser enviado ou executado nos dispositivos. Isso é útil em cenários como saída de dispositivo ou exclusão de configuração.

3. (Opcional) Selecione a opção **Configurar Outlook** para configurar o Microsoft Outlook para um dispositivo que usa o Bridge.

   Tem suporte apenas no Outlook 2010 e 2013.

6. Clique em **Avançar**.

7. Selecione uma distribuição para essa configuração.
   Um registro forçado será feito automaticamente para essas ações do dispositivo.

Categoria	Configuração	O que fazer
	Nome	Insira um nome que identifique essa configuração.
	Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Arquivo de script	**Todas as versões (Windows 10+ Desktop)**	
	Arquivo de script	Selecione um arquivo de script ou executável válido (.ps1, .reg, .exe). • O arquivo de script especificado ou arquivo executável (.ps1, .reg, .exe) será executado automaticamente. • Outros tipos de arquivos só serão copiados para a pasta de destino.
	Argumentos de script	Especifique a lista de argumentos para o arquivo de script. •  Para arquivos Win32 (.exe), insira um argumento para executar silenciosamente o arquivo (por exemplo, /SILENT ou /VERYSILENT). Isso é obrigatório.
	Pasta de destino	Especifique a pasta de destino para o arquivo de script. • Se a pasta de destino não for especificada, o valor da variável %TEMP% do ambiente do sistema será usada como pasta de destino.

Desfazer arquivo de script	**Todas as versões (Windows 10+ Desktop)**	
	Arquivo de script	Selecione um arquivo de script ou executável válido (.ps1, .reg, .exe). • O arquivo de script especificado ou arquivo executável (.ps1, .reg, .exe) será executado automaticamente. • Outros tipos de arquivos só serão copiados para a pasta de destino.
	Argumentos de script	Especifique a lista de argumentos para o arquivo de script. • Para arquivos Win32 (.exe), insira um argumento para executar silenciosamente o arquivo (por exemplo, /SILENT ou /VERYSILENT). Isso é obrigatório.
	Pasta de destino	Especifique a pasta de destino para o arquivo de script. • Se a pasta de destino não for especificada, o valor da variável %TEMP% do ambiente do sistema será usada por padrão.

Fazendo o upload dos scripts para os dispositivos para uso único

Os administradores podem fazer o upload dos scripts para os dispositivos para uso único (ad hoc).

1. Acesse **Dispositivos > Dispositivos**.
2. Clique no link do nome do dispositivo para acessar a página Detalhes do dispositivo. Este é um dispositivo do Windows 10 Desktop para o qual o script de uma única vez será enviado/executado.

3. Clique no ícone e clique em **Script e Ações via Ivanti Bridge**.
4. Insira um nome.
5. Na seção Arquivo de script, especifique um script a ser enviado/executado no dispositivo conforme descrito na tabela precedente.
6. Clique em **Aplicar**.
   A execução do script será enfileirada e pode demorar um pouco para ser concluída. Vá até a guia Registros para verificar e exibir o status (mensagens de saída ou falha). Um registro forçado será feito automaticamente para essas ações do dispositivo.

Registros do Bridge

Este recurso permite recuperar logs do Ivanti Bridge em dispositivos individuais para solucionar problemas e diagnosticar aplicativos. Os registros são enviados no registro seguinte do dispositivo. Você pode aguardar a próxima sincronização programada, ou realizar um registro forçado do dispositivo para obter os registros rapidamente:

Para recuperar logs de um dispositivo:

1. Acesse **Dispositivos > Dispositivos**.
2. Clique no link do nome do dispositivo para acessar a página Detalhes do dispositivo. Este é um dispositivo do Windows 10 Desktop para o qual o script de uma única vez será enviado/executado.
3. Clique no ícone e clique em **Recuperar log do Ivanti Bridge**. A janela **Recuperar Log Ivanti Bridge** é exibida.
4. Selecione uma das opções a seguir:
   Log individual – solicita ao Ivanti Neurons for MDM que recupere o log mais recente do Bridge no dispositivo.
   Todos os logs – solicita que o Ivanti Neurons for MDM recupere todos os logs no dispositivo (até 30 dias).

5. Clique na guia **Recuperar log**. Após o dispositivo o enviar ao Ivanti Neurons for MDM, você pode visualizar o log do Bridge na guia Logs da página de detalhes do Dispositivo.

> Somente os registros enviados com a opção **Todos os registros** podem ser transferidos como arquivo zip.

Último check-in no Bridge

A coluna Último Check-in no Bridge apresenta a data e hora do último check-in do serviço Bridge na página Dispositivos. A coluna pode ser adicionada à página Dispositivos usando-se a opção Personalizar Colunas, e não está visível por padrão.

Para tornar essa coluna visível, selecione **Dispositivos** > **Personalizar colunas** > selecione **Check-in no Bridge**.

> Os dados exportados também terão os detalhes do último check-in do Bridge sempre que aplicável.

Recuperação de falha do serviço Bridge

A recuperação de falha do serviço Bridge foi introduzida no Bridge versão 2.1.14. Por padrão, essa versão é importada para o Catálogo de Aplicativos de todos os usuários. Em alguns casos raros, o serviço Bridge pode falhar sem qualquer motivo conhecido. Nesses casos, há suporte disponível no Bridge 2.1.14 e nas versões posteriores.

Conteúdo

Use a página Conteúdo para distribuir conteúdo hospedado em uma fonte externa. O conteúdo pode incluir arquivos que podem ser baixados pelos usuários, como apresentações de vendas, imagens, planilhas e documentos.

Esta seção contém os seguintes tópicos:

Gerenciando conteúdo

Esta seção contém os seguintes tópicos:

O conteúdo hospedado é compatível com a distribuição de conteúdo baixado em URLs externas. A URL externa deve direcioná-lo apenas a arquivos para download em PDF, EPUB ou IBOOK, e a URL externa deve ter essas extensões.

Não há suporte para a distribuição de licenças VPP Book e, portanto, não há suporte para a distribuição de Apple Books com base noID da iTunes Store.

Use o aplicativo Books ou Pages no dispositivo para acessar o conteúdo enviado do Ivanti Neurons for MDM. Você pode acessá-lo na seção Biblioteca.

O conteúdo de **iBook e EPUB** pode ser distribuído para dispositivos iPad iOS 8+ (licença Gold).Esses formatos são restritos ao iPad, pois a Apple oferece suporte à distribuição interna desses formatos apenas para o iPad. Essa restrição não se aplica aos dispositivos iOS 9.

As pré-visualizações de conteúdo não estão disponíveis para estes formatos.

Para o conteúdo **PDF**, você tem a opção de enviar o documento por push para o aplicativo iBook nos dispositivos iOS 8+.

Distribuindo conteúdo hospedado

Embora você não possa carregar novos documentos para Ivanti Neurons for MDM, você pode fornecer um caminho (URL) em que o conteúdo está hospedado e distribuí-lo aos grupos de dispositivos.

Procedimento

1. Acesse **Conteúdo** > **Conteúdo hospedado**.
2. Clique em **+ Adicionar**.
3. Forneça as seguintes informações:
   - Título
   - Autor
   - Categoria
   - (Opcional) Descrição
4. No campo **Caminho do conteúdo hospedado**, insira um URL para o arquivo que você gostaria de carregar.
5. Clique em **Avançar**.
6. Faça as alterações necessárias para a distribuição.
7. Clique em **Concluído**.

Para modificar o Conteúdo hospedado, o conteúdo anterior deve ser excluído, o novo Conteúdo hospedado deve ser adicionado e distribuído.

Para modificar as configurações além do URL:

1. Acesse **Conteúdo** > **Conteúdo hospedado**.
2. Clique no link do documento na coluna **Nome**.
3. Clique no ícone do Editar.
4. Faça as alterações necessárias.
5. Clique em **Avançar**.

6. Faça as alterações necessárias para a distribuição.
7. Clique em **Concluído** .

Excluindo conteúdo

1. Clique no link do documento na coluna **Nome**.
2. Selecione **Ações > Excluir este documento**.
3. Clique na caixa de seleção para confirmar.
4. Clique em **Excluir documento**.

Ao excluir um documento:

- Ele é removido do sistema.
- Ele não estará mais disponível no catálogo de conteúdo.
- Ele é removido dos dispositivos que o baixaram.

Se você não conseguir executar tarefas na página **Conteúdo,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de aplicativo e conteúdo

Categorias

Esta seção contém os seguintes tópicos:

Como parte do Término do suporte do conteúdo anunciado em 15 de abril de 2017, a capacidade de adicionar um novo conteúdo foi desabilitada. O conteúdo carregado atualmente ainda pode ser distribuído para o aplicativo Apple iBooks e usado.

As categorias descrevem os tipos de **conteúdo**[1] no **catálogo de conteúdos**[2]. As categorias ajudam a organizar o conteúdo para que os usuários possam encontrar facilmente o que precisam. Cada item adicionado ao catálogo de conteúdo deve ter pelo menos uma categoria atribuída.

Adição de categorias

Procedimento

1. Clique em **Adicionar** (canto inferior esquerdo)
2. Digite o nome da categoria.

As categorias não fazem distinção entre letras maiúsculas e minúsculas.

1. Clique em **Salvar**.

Remoção de categorias

Procedimento

1. Clique no X ao lado da categoria.

[1]files that are published by and distributed to users.
[2]a list of files that have been published by and distributed to users. A typical catalog might include sales presentations, images, spreadsheets, and documents.

Se você não conseguir executar tarefas na página **Conteúdo (Conteúdo),** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de aplicativo e conteúdo

Configurações

As configurações são conjuntos de definições enviados aos dispositivos. Por exemplo, você pode usar configurações para instalar automaticamente configurações de VPN e requisitos de senha nos dispositivos. As configurações existentes para seu sistema são listadas na página Configurações.

Esta seção contém os seguintes tópicos:

Trabalhando com configurações

Esta seção contém os seguintes tópicos:

Configurações são conjuntos de parâmetros que você, como administrador, envia aos dispositivos. Por exemplo, você pode usar configurações para instalar automaticamente configurações de VPN e requisitos de senha nos dispositivos. As configurações existentes para seu sistema são listadas na página Configurações. Você pode selecionar diversas configurações na página de Configurações e inseri-las em diversos dispositivos de uma vez. Essas configurações podem ser enviadas a dispositivos específicos dos espaços, e os dispositivos em outros espaços permanecem inalterados. As configurações podem ser enviadas para um único espaço, vários espaços ou todos os espaços de uma vez.

Existem vários tipos de configurações disponíveis.Eles fazem parte das seguintes categorias básicas:

- segurança
- recursos do usuário
- acesso à rede corporativa

- rede celular
- outro (mais configurações)

Você pode realizar as seguintes ações para a maioria das configurações:

- adicionar
- editar
- clonar
- excluir
- excluir uma ou mais configurações de um dispositivo específico
- inserir uma ou mais configurações em um dispositivo específico

Determinadas configurações têm ações restritas:

- Algumas configurações não podem ser adicionadas ou clonadas. O Bloqueio de Ativação do iOS é um exemplo desse tipo de configuração. Portanto, essas configurações não aparecem entre os blocos listados quando você adiciona uma configuração. Essas configurações são listadas somente na página Configurações.
- As configurações definidas pelo sistema não podem ser editadas ou excluídas. SCEP para Registro de iOS é um exemplo desse tipo de configuração.
- Algumas configurações podem ser marcadas para não serem excluídas ou reinstaladas a partir de um dispositivo. Essas configurações não podem ser excluídas ou inseridas no dispositivo.

Filtrando a exibição de configurações

Quando você visualiza a página de **Configurações**, todas as configurações são listadas. Para limitar essa lista a determinadas configurações, use os filtros (painel esquerdo) em SO e Tipo de configuração. Por exemplo, para limitar a lista para exibir apenas as configurações de macOS, selecione **macOS** na seção **SO**.

Para visualizar a configuração em todos os dispositivos ou em dispositivos de múltiplo espaço, selecione múltiplos espaços na lista suspensa. Quando você passa o mouse sobre as configurações exibidas, uma janela pop-up com uma lista de espaços é exibida. Clique em um espaço para exibir a página de detalhes da configuração.

Para procurar uma configuração existente pelo nome, digite o nome da configuração no campo **Pesquisar**.

A partir da versão 81 do Ivanti Neurons for MDM, os administradores globais poderão delegar administradores de espaço para editar o certificado de identidade gerado dinamicamente para todos os dispositivos e para a opção de distribuição personalizada.

Adicionando uma configuração

Essa opção é ativada apenas se um único espaço for selecionado na lista suspensa.

Você pode distribuir um máximo de 100 arquivos de configuração ao mesmo tempo.

Procedimento

1. Clique em **Adicionar**.
2. Selecione o tipo de configuração que você deseja criar.
3. Clique em **Avançar**.
4. Caso não queira essa configuração ativada imediatamente, desmarque a opção **Ativar essa configuração**.

5. Selecione um nível de distribuição para esta configuração:

   - **Todos os dispositivos** - distribuir a configuração para todos os dispositivos disponíveis. Para delegar configurações entre os espaços, selecione uma das opções a seguir:

     - **Não se aplica a outros espaços**.

     - Para delegar configurações em espaços, selecione **Resumo da distribuição** > **Aplicar a dispositivos em outros espaços**.

       - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.

   - **Nenhum dispositivo** – Selecione esta configuração para distribuição em um momento posterior.

   - **Personalizado** – Define um conjunto específico de dispositivos que receberão esta configuração. Para delegar configurações entre os espaços, selecione uma das opções a seguir:

     - **Não se aplica a outros espaços**.

     - **Resumo de distribuição** > **Aplicável a dispositivos em outros espaços**.

       - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.

     O administrador pode usar a opção Distribuição personalizada para distribuir Configuração personalizada para Dispositivo, Grupos de dispositivos, Usuário e Grupos de usuários. A atribuição ou distribuição de configuração para Usuário ou Grupos de usuários não está disponível para as seguintes configurações:

     - Android Enterprise: Perfil de Trabalho (Android for Work)
     - Android Enterprise: dispositivo gerenciado de trabalho (Android for Work)
     - Android Enterprise: Dispositivo Gerenciado com Perfil de Trabalho/Perfil de Trabalho em dispositivo de Propriedade da Empresa
     - Dispositivos Gerenciados de Trabalho Android (Proprietário do Dispositivos) para dispositivos em modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP)

6. Se o seu serviço tiver Espaços definidos, será necessário especificar se a configuração deve ser aplicada aos outros Espaços e a prioridade.
7. Clique em **Concluído**.

Para configurações que emitem um comando para o dispositivo ao invés de instalar um perfil no dispositivo, os detalhes de configuração não listarão a configuração como tendo sido aplicada a nenhum dispositivo.

Inserindo configurações em um dispositivo

Se desejar reinstalar qualquer configuração excluída em um dispositivo, você pode enviar as configurações por push.

Procedimento

1. Acesse **Dispositivos** > **Dispositivos**.
2. Clique no nome de um dispositivo para visualizar a página de detalhes.
3. Vá até **Configurações**.
4. Marque as caixas de seleção para selecionar as configurações específicas a serem inseridas no dispositivo.
5. Clique em **Inserir perfis**.
6. Para inserir uma única configuração, clique em **Inserir** na coluna **Ações**.

Inserindo configurações em diversos dispositivos

Você pode selecionar diversas configurações na página de Configurações e inseri-las em diversos dispositivos de uma vez.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá até **Configurações**.
3. Marque as caixas de seleção para selecionar as configurações específicas.

4. Clique em **Ações**, selecione **Inserir configurações selecionadas** para os dispositivos. O assistente de Inserir configurações é aberto, e todas as configurações e seus status de inserção são exibidos.
5. Clique em **Inserir configuração(ões) válida(s)**. As configurações são inseridas em massa em todos os dispositivos. Configurações que são excluídas de dispositivos específicos da guia **Dispositivos** > **Configurações** não são inseridas.

Excluindo configurações

Algumas das configurações distribuídas anteriormente podem ser manualmente removidas de um dispositivo excluindo-as.

Procedimento

1. Acesse **Dispositivos** >**Dispositivos**.
2. Clique no nome de um dispositivo para visualizar a página de detalhes.
3. Vá até **Configurações**.
4. Marque as caixas de seleção para selecionar as configurações específicas.
5. Clique em **Excluir perfis**.

   Para excluir uma única configuração, clique em **Excluir** na coluna **Ações**. As configurações selecionadas agora estão listadas na guia Configurações excluídas.

Inserindo uma configuração excluída

Procedimento

1. Acesse **Dispositivos** >**Dispositivos**.
2. Clique no nome de um dispositivo para visualizar a página de detalhes.
3. Acesse **Configurações** > **Configurações excluídas**.
4. Selecione uma ou mais configurações a serem inseridas no dispositivo.
5. Clique em **Inserir perfis**.
6. Para inserir uma única configuração, clique em **Inserir** na coluna **Ações**.

Exportando configurações

Você pode exportar os detalhes das configurações selecionadas ou todas as configurações de espaços selecionados para arquivos individuais.

Procedimento

1. Vá até **Configurações**.
2. Marque as caixas de seleção para selecionar as configurações específicas.
3. Clique em **Ações** > **Exportar as configurações selecionadas com detalhes**. Se você quiser exportar todas as configurações, selecione **Exportar todas as configurações com detalhes**.

   Um conjunto de arquivos YAML será incluído em um arquivo .ZIP. O relatório inclui os detalhes de todas as configurações existentes nos espaços selecionados.

Exportar todas as configurações

Exporte seus arquivos de configuração para enviar ao suporte para uso como uma assistência de diagnóstico. Você pode exportar um único arquivo de configuração para um arquivo no formato Yaml ou exportar todas as configurações em um arquivo .zip. Você pode exportar arquivos de diferentes áreas da página Configuração, dependendo de quais configurações você deseja exportar.

Procedimento

1. Vá até **Configurações**.
2. Marque as caixas de seleção para selecionar as configurações específicas.
3. Clique em **Ações** > **Exportar as configurações selecionadas com detalhes**. Se você quiser exportar todas as configurações, selecione **Exportar todas as configurações com detalhes**.

   Um conjunto de arquivos YAML será incluído em um arquivo .ZIP. O relatório inclui detalhes de todas as configurações existentes nos espaços selecionados.

Exportando uma configuração personalizada

Procedimento

1. Vá até **Configurações**.
2. Clique em **+Adicionar** para selecionar uma configuração.

3. Siga as etapas para personalizar a configuração.
4. Clique em **Avançar**.
5. Escolha um nível de distribuição.
6. Clique em **Concluído**.
7. Selecione a configuração criada na lista da página **Configuração**.
8. Clique no menu suspenso **Ações** e clique em **Exportar.**
   Um arquivo com o nome da configuração e uma indicação _yyyymmdd.yaml é baixado em seu dispositivo.

Exportando uma configuração existente

Procedimento

1. Vá até **Configurações**.
2. Selecione uma configuração existente.
3. Clique no menu suspenso **Ações** e clique em **Exportar**.
   Um arquivo com o nome da configuração e uma indicação _yyyymmdd.yaml é baixado.

Importando configurações

Você pode importar um arquivo YAML contendo os detalhes de configuração. Para editar uma configuração, você pode editar os detalhes no arquivo YAML, selecionar uma configuração e importar o arquivo, e os valores atualizados aparecem na configuração. Se mais de uma configuração ou espaço forem selecionados, o botão Importar será desabilitado. Se for selecionado um tipo de arquivo incorreto, uma mensagem de erro será exibida. Se você selecionar um arquivo YAML que contenha detalhes diferentes daqueles necessários para a configuração, uma mensagem de erro será exibida.

Procedimento

1. Vá até **Configurações**.
2. Selecione uma configuração, clique em **Importar**, clique em **Escolher arquivo**, selecione o arquivo YAML e clique em **Importar**. O arquivo YAML com os detalhes de configuração é importado.

Criar uma configuração usando o arquivo YAML

Você pode criar uma configuração a partir de um arquivo YAML. As especificações relacionadas à distribuição não fazem parte do arquivo YAML. O valor padrão da distribuição é Nenhum Dispositivo.

Procedimento

1. Vá até **Configurações**.
2. Clique em **Importar**, clique em **Escolher arquivo**, selecione o arquivo YAML e clique em **Importar**. O arquivo YAML com os detalhes de configuração é importado. A página Criar configuração aparece exibindo todos os detalhes que foram adicionados ao arquivo YAML.
3. Selecione *um* dos tipos de distribuição:
   - **Todos os dispositivos**
   - **Nenhum dispositivo**
   - **Personalizada**
4. Verifique os detalhes da configuração e selecione *uma* das seguintes opções de Resumo de Distribuição:

   O resumo de distribuição não está disponível para todas as configurações.

   - **Não se aplica a outros espaços**
   - **Aplicar a dispositivos em outros espaços**
5. Se o novo nome da configuração corresponder ao nome de uma configuração existente, uma mensagem de erro será exibida; clique em **OK**, clique em **Voltar** e edite o nome da configuração.
6. Clique em **Próximo**, depois clique em **Concluído**.

Editando uma configuração

Você pode abrir uma configuração e editar diretamente os detalhes dela ou importar um arquivo YAML com todos os detalhes necessários. Se mais de uma configuração ou espaço forem selecionados, o botão Importar será desabilitado.

Procedimento

1. Vá até **Configurações**.
2. Selecione e abra uma configuração, clique no ícone de edição (lápis) e edite a configuração.
3. Como alternativa, na página de edição da configuração, clique no ícone **Importar**, selecione o arquivo YAML e clique em **Importar**. A página Editar configuração aparece exibindo todos os detalhes que foram adicionados ao arquivo YAML.
4. Verifique os detalhes da configuração e selecione uma das seguintes opções de Resumo de Distribuição:

   O resumo de distribuição não está disponível para todas as configurações.

   - **Não se aplica a outros espaços**.
   - **Aplicar a dispositivos em outros espaços**

     O valor padrão da distribuição é Nenhum Dispositivo.
5. Clique em **Avançar**.
6. Clique em **Próximo**, depois clique em **Concluído**.

Apagando configurações

Você pode apagar configurações selecionadas.

Procedimento

1. Marque as caixas de seleção para selecionar as configurações específicas.
2. Selecione **Ações** > **Excluir**.

Agendar atualizações de aplicativos internos

O Ivanti Neurons for MDM atualiza automaticamente os aplicativos internos quando o dispositivo faz check-in. Os administradores agora podem agendar atualizações de aplicativos internos com base no fuso horário do servidor. O aplicativo é atualizado somente quando o dispositivo é registrado dentro do horário agendado. Por padrão, o agendamento de atualizações de aplicativos está desativado.

Essa configuração é aplicável somente a atualizações, não a novas instalações. Você pode usar o comando Enviar instalação/atualização para substituir o agendamento de atualização automática para apps iOS. Se a atualização automática estiver habilitada no nível do aplicativo ou no nível do catálogo, ela terá precedência sobre a configuração de aplicativo agendada, e o aplicativo será atualizado imediatamente no check-in.

A configuração é aplicável somente aos seguintes tipos de aplicativos:

- Aplicativos internos iOS.
- Aplicativos internos Android que estão somente no modo DO.
- Aplicativos macOS nos formatos .pkg e .MIP.
- Aplicativos Windows.

Pré-requisitos

Assegure que os pré-requisitos a seguir sejam atendidos para que a configuração funcione conforme esperado:

- O aplicativo deve ser gerenciado para iOS e Android. Para macOS, o aplicativo pode estar no estado gerenciado ou não gerenciado.
- Assegure que a opção Instalar no dispositivo em Configuração do aplicativo está ativada.
- O dispositivo deve ser registrado durante o horário agendado.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá até **Configurações**.
3. Clique em **Adicionar**. A página Adicionar configuração se abre.
4. Procurar **Atualização automática do aplicativo**. A página Criar configuração de atualização automática do aplicativo se abre.
5. Especifique um nome no campo **Nome**.
6. Na seção **Instalação da configuração**, selecione o **Fuso horário** na lista suspensa.
7. Selecione o **Horário de início** na lista suspensa e, em seguida, selecione a **Duração** na lista suspensa.

8. Clique em **Avançar**.
9. Selecione o grupo de usuários e dispositivos requeridos e, em seguida, clique na caixa de seleção **Ativar esta configuração**.
10. Clique em **Concluído** . A configuração é aplicada, o aplicativo agora será atualizado somente no agendamento especificado.

Se você não conseguir visualizar a página Configurações, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Tópicos relacionados:

- Espaços
- Priorizar configurações

Criação de uma configuração do Portal de autoatendimento do usuário

Como um usuário corporativo, você pode usar o Portal de autoatendimento para gerenciar seus dispositivos e certificados. A guia Meus dispositivos exibe os dispositivos que você registrou.

Você pode realizar as seguintes tarefas da guia Meus dispositivos:

- Bloquear
- Desbloquear
- Desativar
- Reiniciar senha de aplicativos seguros

Você pode executar as seguintes tarefas da guia Meus certificados:

- Fazer upload do certificado

Você pode distribuir um máximo de 100 arquivos de configuração ao mesmo tempo.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Clique em **Adicionar**.
3. Procure **Criar uma configuração do Portal de autoatendimento do usuário**.
4. Clique em **Avançar**.
5. Caso não queira essa configuração ativada imediatamente, desmarque a opção **Ativar essa configuração**.

6. Selecione um nível de distribuição para esta configuração:
    - **Todos os dispositivos** - distribuir a configuração para todos os dispositivos disponíveis. Para delegar configurações entre os espaços, selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - Para delegar configurações em espaços, selecione **Resumo da distribuição** > **Aplicar a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.
    - **Nenhum dispositivo** – Selecione esta configuração para distribuição em um momento posterior.
    - **Personalizado** – Define um conjunto específico de dispositivos que receberão esta configuração. Para delegar configurações entre os espaços, selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Resumo de distribuição** > **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.
7. Se o seu serviço tiver Espaços definidos, será necessário especificar se a configuração deve ser aplicada aos outros Espaços e a prioridade.
8. Clique em **Concluído**.

Para configurações que emitem um comando para o dispositivo ao invés de instalar um perfil no dispositivo, os detalhes de configuração não listarão a configuração como tendo sido aplicada a nenhum dispositivo.

Configuração personalizada

Esta seção contém os seguintes tópicos:

Licença: Silver

Aplicável a: iOS, macOS, Android, Windows

Descrição

Permite que você importe e distribua um arquivo de configuração predefinido.

Os formatos válidos de arquivos de configuração são os seguintes:

SO	Formatos válidos de arquivo de configuração
iOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android	.xml. Atualmente, esse recurso é compatível somente com arquivos .xml para dispositivos Zebra.
Windows	SyncML.

Definição de configurações personalizadas

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.

3. Digite "personalizar" no campo de busca e clique na configuração **Personalizar**.
   A página de detalhes Configuração personalizada é exibida.
4. Defina as configurações nessa página. Consulte a tabela na seção Definições da configuração personalizada para obter informações sobre os valores.
5. Clique em **Avançar** para configurar as definições de distribuição.
6. (Dispositivos macOS) Selecione uma opção adicional para a configuração **A quem essa configuração se aplica** dependendo do comportamento que você deseja para essa configuração:
   - Todo o dispositivo (usada comumente).
   - Específica do usuário (atualmente registrado).
7. Clique em **Concluído**.

Definições da configuração personalizada

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Selecionar SO	Clique em um ícone de SO para carregar um arquivo de configuração que corresponda ao ícone selecionado.
Escolher arquivo	Essa opção será exibida depois que você selecionar um SO. Arraste um arquivo de configuração na caixa de arrastar e soltar ou clique no botão **Escolher arquivo** para selecionar um arquivo de configuração.

Configuração de CSP personalizado (somente Windows)

Você pode criar uma configuração de CSP Personalizado somente em dispositivos Windows. Ao selecionar o sistema operacional Windows na seção Escolher sistema operacional, você terá duas opções:

Opção 1 - Arquivo XML CSP - selecione esta opção e siga o mesmo processo mencionado para a configuração **Escolher arquivo**.

Opção 2 - Nós de esquema OMA-URI de CSP personalizado

Procedimento

1. Selecione a opção Nós de esquema OMA-URI de CSP personalizado na lista. A seção Configuração de CSP personalizado aparece na tela.
2. Em **AÇÕES**, clique no botão + para começar a criar a configuração com diferentes campos OMA-URI.
3. A janela pop-up **Adicionar linha** aparece na tela com os seguintes campos:
   - Descrição - insira qualquer informação geral sobre a configuração
   - OMA-URI - insira o OMA-URI que deseja usar como configuração
   - Tipo de dado - selecione o tipo de dado a ser usado na configuração - DATA, FLUTUANTE, BASE64, NÓ, XML, BINÁRIO, CARACTERE, HORA, BOOLEANO, INTEIRO
   - Valor - Insira um valor associado ao tipo de dado selecionado
   - Tipo de acesso - adicionar, excluir, executar, substituir, obter
4. Clique em **Salvar e fechar** para fechar a janela com os detalhes fornecidos. Clique em **Salvar e adicionar** outro para criar uma nova linha.
5. Clique em **Avançar**.
6. Selecione o modo de distribuição e clique em **Concluído**.

Tópicos relacionados

- Envio do SyncML aos dispositivos usando configuração personalizada
- Como criar uma configuração

Envio de SyncML aos dispositivos usando configurações personalizadas

Você pode criar os seus próprios arquivos de configuração da Linguagem de Marcação para Sincronização (SyncML) ou obtê-los a partir de um terceiro para implementar recursos personalizados ao adicioná-los a uma configuração personalizada.

Plataformas compatíveis:

- Telefone Windows 10
- Desktop Windows 10
- Dispositivos Windows 8.1

Dispositivos compatíveis:

- Windows 10+
- Microsoft HoloLens 2

Procedimento

1. Vá até **Configurações**.
2. Clique em **+Adicionar**.
3. Clique em **Configuração Personalizada** para exibir a página **Criar Configuração Personalizada**.
4. Insira um nome para a configuração.
5. Clique no ícone SO do Windows.
6. Arraste e solte o arquivo SyncML na interface ou clique em **Escolher Arquivo** para navegar ao arquivo a fim de selecionar o dispositivo a ser atualizado.

   O Ivanti Neurons for MDM não realiza verificações de validação no código do arquivo.

7. Clique em **Avançar**.

Log de SyncML Personalizado

Os comandos SyncML enviados ao dispositivo Windows e as respostas SyncML a esses comandos a partir do dispositivo podem ser visualizados na guia Logs do Dispositivo. Essas informações de log estarão disponíveis após o envio da configuração **SyncML Personalizado do Windows**. Quando o sistema envia uma configuração de SyncML Personalizado, ela sempre tem o status "Instalado" na guia "Configuração" do dispositivo para a configuração, independentemente das respostas SyncML.

Configuração do layout da tela inicial

Esta seção contém os seguintes tópicos:

- "Definição da configuração do layout da tela de início" abaixo
- "Definições da configuração do layout da tela inicial" na página 466

Licença: Silver

Dispositivos elegíveis: somente iOS 9.3+ supervisionado

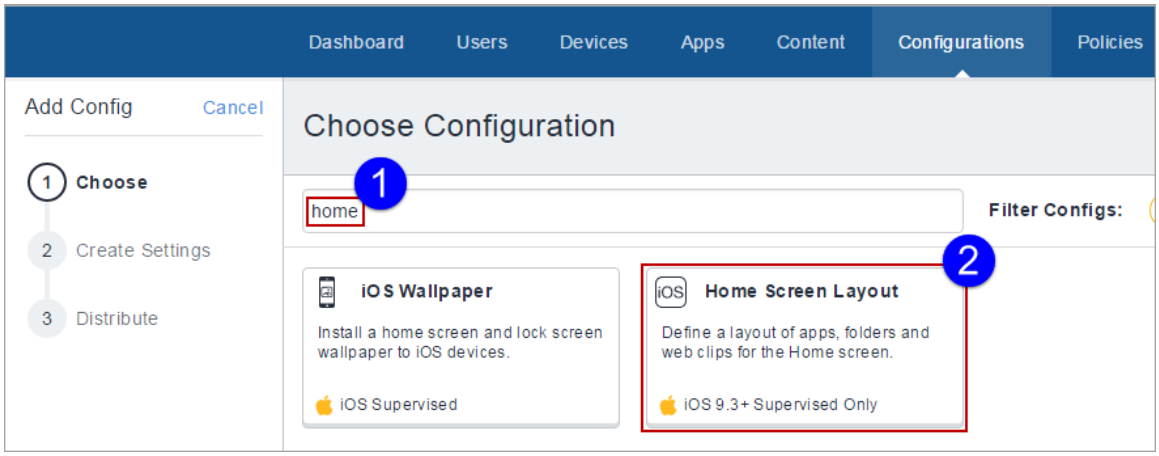
Descrição

Define um layout de apps, pastas e web clips para a tela inicial.

Definição da configuração do layout da tela de início

Procedimento

1. Acesse **Configurações** > clique em **+ Adicionar**.
2. Digite "inicial" no campo de busca e clique na configuração **Layout da tela inicial**. A página de detalhes Configuração do Layout da Tela Inicial é exibida.



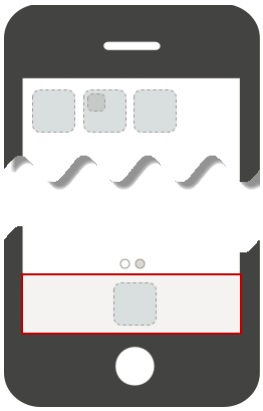
3. Defina as configurações nessa página. Consulte a tabela na seção Home_Screen_Layout_Configuration_Settings para obter informações sobre os valores.

4. Clique em **Avançar** para configurar as definições de distribuição. Para dispositivos iPad compartilhados, selecione o canal **Dispositivo** ou o canal **Usuário**. Para mais informações, consulte "Trabalhando com configurações" na página 445.

5. Clique em **Concluído**.

Definições da configuração do layout da tela inicial

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.

Doca	Clique no ⊕ para adicionar um aplicativo ou clipe da web à doca da tela inicial, mostrada em destaque aqui, e siga as instruções nas telas subsequentes:  Você pode adicionar manualmente aplicativos do sistema digitando o ID do pacote Apple (começando com "com.apple"). Por exemplo, digite "com.apple.DocumentsApp" para adicionar o aplicativo "Files".

Página 1	Clique no ⊕ para adicionar um aplicativo ou clipe da web à área da página da tela inicial, mostrada em destaque aqui, e siga as instruções nas telas subsequentes:  Você pode clicar em Add Page para adicionar outra página à tela do telefone.

Configuração de controle do aplicativo: Controle os apps que serão instalados por dispositivo

A configuração Controle do aplicativo permite que você classifique apps como Lista de permitidos ou Lista de bloqueados no nível do dispositivo. Os apps já instalados não estarão visíveis e não poderão ser executados. Os apps ainda estarão visíveis na App Store, mas não poderão ser baixados ou iniciados. Qualquer dispositivo com essa configuração distribuída a usará e ignorará as configurações da Política de apps permitidos. Essa configuração substitui qualquer política relacionada aos mesmos aplicativos nos dispositivos de destino.

Essa configuração substitui qualquer política relacionada aos mesmos aplicativos nos dispositivos de destino. Para dispositivos com Windows 10, as restrições acontecem no nível do dispositivo, portanto, a configuração é a única maneira de aplicar as regras do aplicativo.

A configuração Controle do aplicativo permite que você crie uma:

- **Lista de permitidos:** permitir apenas os apps explicitamente adicionados a esta lista. Nenhum outro aplicativo poderá ser instalado nos dispositivos.
- **Lista de bloqueados:** impedir a instalação de apps específicos nos dispositivos.

Dispositivos compatíveis

Você pode usar a configuração Controle do aplicativo para colocar diferentes apps na Lista de bloqueados ou na Lista de permitidos nos seguintes dispositivos:

- Perfil de trabalho do Android ativado em dispositivos de propriedade da empresa
- Somente iOS 9.3+ supervisionado
- tvOS 11+
- Windows

Criar configuração Controle do aplicativo

Procedimento

1. Selecione **Configurações**.
2. Clique em **+Adicionar**
3. Insira **Controle do aplicativo** no campo **Escolher configuração** resultante e selecione a configuração **Controle do aplicativo**.
4. Insira um nome e uma descrição para a configuração.
5. Selecione um SO e continue com a seção abaixo que se aplica ao seu SO.

Perfil de trabalho do Android ativado em dispositivos de propriedade da empresa

Os usuários podem adicionar até 50 IDs de apps ao grupo Lista de permitidos ou Lista de bloqueados.

Procedimento

1. Selecione **Criar uma lista de permitidos para apps pessoais** ou **Criar uma lista de bloqueados para apps pessoais** para adicionar a lista de apps apropriados a serem permitidos ou bloqueados.
2. Insira o ID do aplicativo (com.exemplo.com) e clique em **Adicionar**.
3. Clique em **Avançar** e escolha uma opção de distribuição.
4. Clique em **Concluído**.

Dispositivos com iOS 9.3 supervisionado

Procedimento

1. Escolha se deseja criar uma lista de permitidos ou uma lista de bloqueados.
2. Clique em **Adicionar apps**.
3. Escolha os apps para a lista de permitidos ou a lista de bloqueados clicando em uma ou ambas as guias a seguir:
   - Clique em **Adicionar por pesquisa** para procurar e selecionar aplicativos da App Store ou do Catálogo de Aplicativos.
   - Clique em **Adicionar manualmente** para escolher os apps inserindo o ID do pacote da Apple (começa com "com.apple") somente para os apps do sistema Apple.

4. Clique na guia **Allowedlist** ou na **Blockedlist** para revisar a lista de apps escolhidos como permitidos ou bloqueados.
5. (Opcional) Selecione a opção **Incluir todos os clipes da web**.
6. Clique em **Avançar** e escolha uma opção de distribuição.
7. Clique em **Concluído**.

Dispositivos com Windows

Procedimento

1. Selecione **Permitido** ou **Proibido** para adicionar a lista de apps apropriados a serem permitidos ou bloqueados.
2. Na seção **Definição da regra**, selecione o **Tipo de aplicativo** na lista.
3. Insira um nome identificador na caixa **Identificador do aplicativo** para procurar um aplicativo específico. Você também pode usar o link **Pesquisar apps** para abrir um novo diálogo e procurar identificadores de aplicativos específicos do Windows.
4. (Opcional) Insira uma descrição sobre o aplicativo na caixa **Descrição do aplicativo**.
5. Use o link **+Adicionar** para adicionar mais definições de regra para colocar os apps na Lista de permitidos ou na Lista de bloqueados.
6. Clique em **Avançar** e escolha uma opção de distribuição.
7. Clique em **Concluído**.

Configuração das notificações do aplicativo

Escolha como os usuários receberão as notificações dos apps selecionados.

Aplicável a: dispositivos iOS 9.3+ supervisionados.

Criação de configuração de notificações do aplicativo

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite notificações no campo de busca e, então, clique na configuração **Notificações do aplicativo**. A página Definir configuração das notificações do aplicativo é exibida.
4. Nomeie e descreva a configuração.
5. Adicione aplicativos consultando a App Store ou inserindo manualmente o ID do pacote.
6. Escolha um aplicativo para aplicar as configurações de notificação do aplicativo.

7. Configure as definições de notificação. Aqui estão as notificações que você pode selecionar:
    - Permitir notificações
        - Exibir na Central de notificações
        - Sons
        - Ícone de aviso de aplicativo
        - Mostrar na tela de bloqueio
        - (iOS 12.0+ supervisionado) Exibir o alerta crítico ao usar o CarPlay
        - (iOS 12.0+ supervisionado) Permitir a habilitação de alertas críticos (ignorar "Não perturbe")
    - Estilo de alerta de desbloqueio
        - Banners
        - Alerta modal
        - Nenhum
    - (iOS 12.0+ supervisionado) Tipo de agrupamento
        - Automático
        - Por aplicativo
        - Desligar
    - (iOS 14.0+) Tipo de visualização de notificação – Selecione um tipo de visualização para exibir nas visualizações de mensagem de notificação do dispositivo.
        - Controlado pelo usuário – Exibe visualizações de mensagens de acordo com as configurações do usuário para os apps no dispositivo.
        - Sempre – Exibe visualizações de mensagens.
        - Quando desbloqueado – Exibe visualizações de mensagens apenas quando um dispositivo está desbloqueado.
        - Nunca – Impede que os apps exibam visualizações de mensagens nas Notificações.
8. Clique em **Avançar** para configurar as definições de distribuição.

9. Clique em **Concluído**.

Para obter mais informações, consulte Como criar uma configuração.

Exportação de configurações

Exporte seus arquivos de configuração para enviar ao suporte para uso como uma assistência de diagnóstico. Você pode exportar um único arquivo de configuração para um arquivo no formato Yaml ou exportar todas as configurações em um arquivo .zip.

Procedimento

Exportar configuração

Você pode exportar arquivos de diferentes áreas da página Configuração, dependendo de quais configurações você deseja exportar.

Exporte todas as configurações:

1. Vá até **Configurações**.
2. Marque as caixas de seleção para selecionar as configurações específicas.
3. Clique em **Ações** > **Exportar as configurações selecionadas com detalhes**. Se você quiser exportar todas as configurações, selecione **Exportar todas as configurações com detalhes**.

   Um conjunto de arquivos YAML será incluído em um arquivo .ZIP. O relatório inclui detalhes de todas as configurações existentes nos espaços selecionados.

Exporte uma configuração personalizada:

1. Vá até **Configurações**.
2. Clique em **+Adicionar** para selecionar uma configuração.
3. Siga as etapas para personalizar a configuração.
4. Clique em **Avançar**.
5. Escolha um nível de distribuição.
6. Clique em **Concluído**.
7. Selecione a configuração criada na lista da página **Configuração**.

8. Clique no menu suspenso **Ações** e clique em **Exportar.**
   Um arquivo com o nome da configuração e uma indicação _yyyymmdd.yaml é baixado em seu dispositivo.

Exporte uma configuração existente:

1. Vá até **Configurações**.
2. Selecione uma configuração existente.
3. Clique no menu suspenso **Ações** e clique em **Exportar**.
   Um arquivo com o nome da configuração e uma indicação _yyyymmdd.yaml é baixado.

Priorização de configurações

Se você selecionar diversos grupos de dispositivos para uma configuração, então diversas configurações do mesmo tipo devem ser atribuídas a um determinado dispositivo. Quando configurações do mesmo tipo são aplicadas ao mesmo dispositivo, a prioridade definida determina qual configuração é aplicada. A configuração com a prioridade mais alta possui o número mais baixo. Por exemplo, a configuração com prioridade 1001 possui uma prioridade mais alta do que a configuração com a prioridade 1002. O serviço atribui números automaticamente.

A prioridade de Wi-Fi não pode ser aplicada ao dispositivo e está dispensado da prioridade.

Essa opção está disponível apenas se a página contiver duas ou mais configurações do mesmo tipo e se um único espaço for selecionado na lista suspensa. Você pode alterar a prioridade das configurações.

Procedimento

1. Vá até **Configurações**.
2. Sem nenhuma configuração selecionada, selecione **Ações > Priorizar configurações**.

   Se a opção **Ações** não for exibida, você não tem várias políticas que exigem prioridades.
3. Use as setas para mover as configurações para que a que deve ter a prioridade mais alta apareça no topo.

   Um ícone de cadeado indica que a prioridade da configuração não pode ser alterada sem editar a definição de distribuição Todos os dispositivos na configuração.
4. Clique em **Salvar**.

   A priorização pode ser feita em até 400 configurações.

Se você não conseguir visualizar a página Configurações, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Como gerenciar configurações

Esta seção contém os seguintes tópicos:

Tipos de configuração

Esta seção contém os seguintes tópicos:

Pesquisar uma configuração

Use o recurso de pesquisa e filtro na página **Escolher Configurações** para encontrar a configuração que deseja aplicar.

Procedimento

1. Escolha **Configurações**.
2. Escolha uma das configurações relacionadas e clique no botão **+Adicionar**.

   A página **Escolher configuração** será exibida
3. Clique em uma das configurações relacionadas ou:
   - Insira o nome da configuração na caixa de busca
   - Clique em um ícone de filtro à direita da caixa de busca para exibir os tipos de configuração compatíveis com a plataforma.
4. Clique em um botão de configuração para acessar as opções de definição das configurações.

Para mais informações, consulte "Trabalhando com configurações" na página 445.

Segurança

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Android Enterprise	Especifica as opções do Android Enterprise	Android Enterprise	Licença
Dispositivo AppConnect	Especifica as configurações de segurança de aplicativos habilitados para AppConnect em dispositivos	• Android • iOS	Licença
Azure Active Directory (Locatário do Azure)	Ao conectar o Ivanti Neurons for MDM ao Azure Active Directory, será possível usar o status de conformidade dos dispositivos gerenciados para acesso condicional aos aplicativos do Microsoft 365.	• iOS • Android	• Para novos clientes: UEM Seguro Premium • Para clientes existentes: Platinum
Certificado	Estabelece confiança com os servidores	• Android • iOS • macOS	
"Transparência de certificado" na página 542	Controla a aplicação da Transparência de Certificado, que só pode aparecer em um perfil de dispositivo.	• iOS • macOS • tvOS	
Log do dispositivo	Recupera logs adicionais, como logs de rede e segurança, dos dispositivos.	• Android Enterprise	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Criptografia para Android	Solicita que os usuários iniciem a criptografia.	Android	
DNS criptografado	Permite que você aprimore a segurança sem precisar configurar a VPN.	• iOS • macOS	Licença
Defesa contra ameaças móveis	Protege dispositivos gerenciados contra ameaças e vulnerabilidades móveis que afetam o dispositivo, a rede e os aplicativos.	• Android • iOS	
Ações locais de defesas contra ameaças	Crie e distribua uma configuração do dispositivo que defina as ações locais a serem realizadas em dispositivos Android compatíveis quando o cliente com defesa contra ameaças detectar uma ameaça.	Android	
FileVault 2	Oferece a capacidade de realizar a criptografia XTS-AES 128 completa no conteúdo de um volume.	macOS	Licença

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Chave de recuperação do FileVault	Determina as configurações de redirecionamento das chaves de recuperação do FileVault para um servidor corporativo.	macOS	Licença
Certificado de identidade	• Autentica o dispositivo para os servidores. • Autentica o dispositivo para os recursos de rede.	• Android • iOS • macOS	
Bloqueio de Ativação do iOS	Habilita o recurso de Bloqueio de Ativação da Apple em dispositivos supervisionados.	iOS	Licença
iOS Configuração personalizada	Distribui um perfil de configuração do iOS criado por um aplicativo diferente.	iOS	
Restrições do iOS	• Bloqueia os recursos do dispositivo. • Habilita os recursos do dispositivo.	iOS	
Exibição em sala de conferência	Ativa o modo Exibição em sala de conferência no Apple TV.	tvOS 10.2+	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Bloqueio e quiosque: Android	• Bloqueia os recursos do dispositivo. • Habilita novamente os recursos do dispositivo. • Aplica o recurso do quiosque.	Android	
Bloqueio e Quiosque: Android Enterprise	• Define quais recursos e aplicativos estão restritos nos dispositivos com Android corporativo. • Aplica o recurso do quiosque.	Android 5.0 +	
Bloqueio E Quiosque: Samsung Knox padrão	• Define quais recursos e aplicativos estão restritos nos dispositivos Samsung Knox Standard. • Aplica o recurso do quiosque.	Samsung Knox	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Firewall do macOS	Gerencia as configurações do Firewall do aplicativo acessíveis no painel Preferências de segurança nos dispositivos macOS. O Administrador pode ativar o modo furtivo especificando um dispositivo que não pode ser descoberto pelo comando ping.	macOS 10.12+	Licença
Restrições do macOS	Determinam quais restrições estão habilitadas em dispositivos macOS.	macOS	Licença
Restrições de macOS AppStore	Definem quais restrições estão habilitadas na AppStore do macOS.	macOS	Licença
Restrições de gravação de disco do macOS	Gerenciar restrições de gravação de disco no Mac OS.	macOS	Licença
Mobile@Work para macOS	Crie e distribua regras de execução para o Mobile@Work para macOS.	macOS	Licença

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Script do Mobile@Work para macOS	Crie scripts para distribuir ao Mobile@Work para macOS.	macOS	Licença
"Preferência de identidade" na página 700	Identifique um item de Preferência de identidade no conjunto de chaves do usuário que faça referência a um conteúdo de identidade incluído no mesmo perfil.	macOS	Licença
"Preferência de certificado" na página 694	Identifique um item da Preferência de certificado no conjunto de chaves do usuário que faça referência a um Conteúdo de certificado incluído no mesmo perfil.	macOS	Licença
Controle de mídia permitido	Configure as opções de montagem, desmontagem e ejeção de mídias físicas.	macOS	Licença
Configurações do Finder do macOS	Gerenciar configurações do aplicativo Finder no Mac OS.	macOS	Licença
Política de extensão Kernel de macOS	Controla restrições e configurações para carregar Extensões Kernel aprovadas pelo usuário.	macOS	Licença

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
"Active Directory (macOS)" na página 695	Configure opções avançadas para vincular dispositivos macOS a um domínio do Active Directory (AD) para acessar serviços de software que dependem do AD para autenticação e segurança.	macOS	Licença
"Criação de conta automática do Office 365 (macOS)" na página 702	Configurar as informações e opções do usuário para definir a configuração inicial de todos os aplicativos do Microsoft Office 365.	macOS	Licença
Catálogo de aplicativos da Apple	Gerencia o acesso ao Catálogo de Aplicativos Apple por meio de um clipe da web.	• iOS • macOS	Licença
Domínios Gerenciados	Especifica domínios confiáveis da web e de e-mail.	• iOS 8 ou superior	
Senha	• Torna a senha obrigatória. • Especifica o tamanho e o conteúdo da senha. • Altera os requisitos da senha.	• Android • iOS • macOS	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
"Preferência de privacidade (macOS)" na página 716	Configure quais aplicativos têm permissão para obter acesso aos serviços do sistema, arquivos do sistema e recursos do sistema.	macOS	Licença
Autenticar	Forneça autenticação sem senha para serviços em nuvem e/ou logins em desktop.	• macOS • Windows	
"Configuração de privacidade" na página 721	Especifica se os dados de localização são coletados.	• iOS • Android • Windows	
"Informações de declaração de privacidade do cliente" na página 727	Exibir política de privacidade para o usuário no cliente Go.	• Android • Android corporativo • iOS	
"Privacidade do cliente" na página 720	Configure para coletar dados via MixPanel, incluindo informações do dispositivo e de uso necessários para solucionar problemas e manter a mais alta qualidade de serviços.	• iOS • macOS	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Atualizações de software	Cria e distribui regras para atualizações de SO.	• iOS • macOS • Windows	
"Servidor de tempo" na página 739	Permitir que os dispositivos se conectem aos servidores de tempo personalizados.	macOS	Licença
Filtro de conteúdo da Web	Controla o conteúdo Safari.	iOS 7 supervisionado	Silver
Proteção de informações do Windows	Define as configurações da Proteção de informações do Windows (WIP) para proteger os dados corporativos.	Windows 10+	Licença
Restrições do Windows	Determina quais recursos estão disponíveis nos dispositivos de Windows Phone.	Windows Phone	

Recursos do usuário

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
CalDAV	• configura o acesso para um servidor CalDAV (como o Google Calendar)	• iOS	
CardDAV	• configura o acesso a um servidor CardDAV (como o Google Contacts)	• iOS	
E-mail	• configura o acesso para o e-mail POP/IMAP (como o Gmail)	• iOS	
configuração do	• configura o acesso para o e-mail com base no ActiveSync (como o Outlook) para dispositivos móveis Android e iOS • configura o e-mail com base no Exchange Web Services (EWS) para dispositivos macOS • define o quanto sincronizar ao dispositivo • define a segurança para o e-mail	• Android • iOS • macOS	• O Exchange via Sentry não tem suporte no macOS • O sinalizador Sincronizar e-mails dos últimos dias não é aplicável para macOS

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Google	• Cria configurações da conta Google que conectam os dispositivos iOS 9.3.2+ a contas Google. • Especifica qual aplicativo usar a fim de fazer chamadas para contatos no sistema Google.	• iOS	
Fonte	• instala fontes não padrão, necessárias para a exibição correta de documentos	• iOS	
Calendário assinado	• configura uma assinatura para um calendário da internet	• iOS	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Web clip	• exibe um atalho (ícone) para uma página da web	• iOS • macOS	
Cache de conteúdo	• fornece o serviço de cache de conteúdo para habilitar cópias locais do software da App Store e • habilita clientes conectados para downloads mais rápidos de software e aplicativos.	• macOS	

Acesso à rede corporativa

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
AirPlay	• configura o acesso para alternar dispositivos para uma exibição de mídia	• iOS • macOS	Silver
AirPrint	• configura uma impressão sem fio	• iOS • macOS	Silver
VPN Sempre Ativa	• configura o acesso para um servidor VPN sem a interação do usuário	• Android 7.0+ • iOS 8 ou superior	• Gold para Android corporativo • Silver para iOS
Permissões padrão de tempo de execução do aplicativo	• configura a permissão de tempo de execução para aplicativos implementados em dispositivos com Android corporativo.	• Aplicativos desenvolvidos para API Android 23 ou superior e que executam Android 6.0 ou superior em dispositivos com Android corporativo.	
Educação	• Configura a carga útil de Educação da Apple e o aplicativo Classroom para líderes e membros	• supervised iOS 9.3+	Licença
Proxy global	• configura os dispositivos para direcionar o tráfego HTTP para um servidor proxy	• iOS 7 supervisionado	Silver
LDAP	• configura o acesso a um diretório corporativo	• iOS	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Tunnel	• define uma conexão VPN por aplicativo entre um cliente e o Sentry usando o Tunnel	• iOS 7+ • Windows 10+	
Bridge	• permite que a TI modernize as operações do Windows em UEM sem abrir mão de funcionalidade crítica	• Windows 10+ Desktop	Licença Bridge
O servidor macOS	• Define uma conta de servidor do macOS com tipos configurados de conta e configurações relevantes. Permite que o usuário ative o Compartilhamento de arquivos no servidor.	• iOS 10+	
VPN por aplicativo	• configura conexões entre apps específicos e um servidor VPN	• iOS	Silver
Logon único	• configura um logon único para apps específicos gerenciados	• iOS	
Entrada segura multiusuário	• configura login seguro de vários usuários por meio de web clip	• iOS	

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
VPN	• configura o acesso para um servidor VPN	• Android • Windows • iOS • macOS	
VPN sob demanda	• configura o acesso a um servidor VPN com base em domínios, nomes do host, etc.	• iOS	
Wi-Fi	• configura o acesso para uma rede sem fio	• Android • Windows • iOS • macOS	

Rede celular

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
APN	• define o nome do ponto de acesso celular para o dispositivo	• iOS	
Celular	• configura o acesso à rede celular	• iOS	
"Definição das configurações de telecomunicação para iOS" na página 990	• configura os valores padrão para restrições de roaming • configura os valores padrão para restrições de pontos de acesso pessoais	• iOS	

Mais configurações

Tipo	O que ele faz	Para esses dispositivos	É necessário ter esta licença
Apple TV	• define o idioma e o local para a Apple TV	• iOS 7 supervisionado	Silver
Nome do dispositivo padrão	• define um nome do dispositivo padrão usando variáveis	• iOS 8 supervisionado	Silver
Imagem de fundo do iOS	• instala uma imagem de fundo para a tela inicial e tela de bloqueio	• iOS 7 supervisionado	Silver
Imagem de fundo do macOS	• Instala um papel de parede para a tela inicial e tela de bloqueio nos dispositivos. Os papéis de parede podem ser alterados pelo usuário, mas não removidos de um dispositivo após a distribuição		Não obrigatório
Modo de aplicativo único	• restringe o dispositivo para o uso do aplicativo especificado	• iOS 7 supervisionado	Silver
"Configuração Domínios Associados" na página 992	• A configuração Domínios Associados é um dicionário que mapeia os aplicativos a seus domínios associados. • Domínios associados podem ser usados com recursos como AppSSO extensível, links universais e preenchimento automático de senha.	macOS 10.15+	Gold

Configuração de sincronização do dispositivo

As definições de Sincronização do Dispositivo fornecem uma lista de pontos de dados que podem ser monitorados nos dispositivos. As configurações de Sincronização do Dispositivo não podem ser editadas. Para visualizar uma lista das configurações verificadas:

Procedimento

1. Vá até **Configurações**.
2. Clique em **Configuração de sincronização do dispositivo**. A guia Detalhes da página **Configuração de Sincronização do Dispositivo** é exibida com uma lista de itens marcados.

Configuração	**Tempo entre as leituras em minutos**
Lista de certificados	
Informações do dispositivo	60
Lista de aplicativos instalados	60
Lista de aplicativos gerenciados	60
Lista de perfis	60
Lista de perfis de aprovisionamento	60
Restrições	60
Informações de segurança	60
iOS 9+	
Verificar atualizações	1440

Tópicos relacionados

- Variáveis
- "Trabalhando com configurações" na página 445

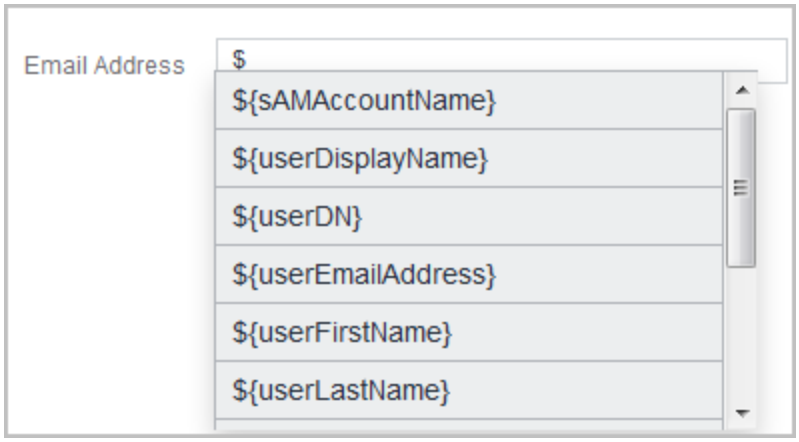
Variáveis

Você pode usar variáveis em alguns campos de configuração para representar valores específicos a um determinado usuário. Qualquer campo que suporte variáveis exibe uma lista das variáveis suportadas se você digitar $. Esta seção contém os seguintes tópicos:

- "Variáveis de conta de usuário suportadas" abaixo
- "Variáveis de dispositivo suportadas" na página 505

Variáveis de conta de usuário suportadas

Variáveis de usuário



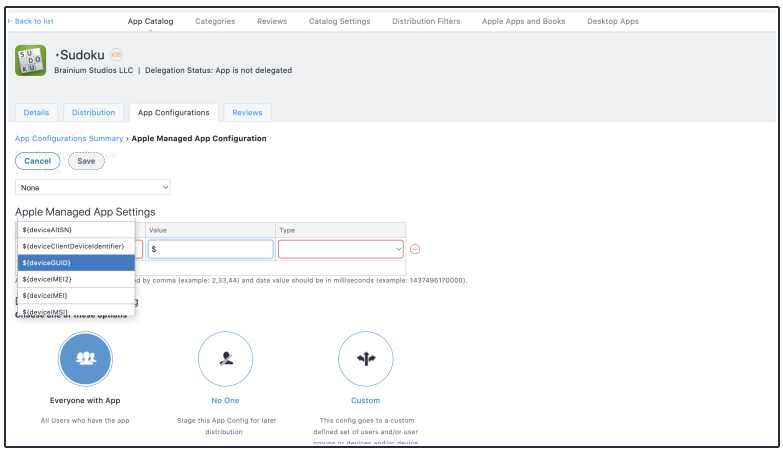
Chave variável	Descrição do valor
${department}	atributo departamento (requer Azure Active Directory)
${edipi}	Sem descrição
${managedAppleId}	ID Apple gerenciado do usuário
${sAMAccountName}	atributo sAMAccountName (requer Active Directory)
${userCN}	Atributo Nome Comum (CN) extraído do nome distinto (requer LDAP)
${userDisplayName}	Nome de exibição
${userDN}	Nome Distinto (requer LDAP)
${userEmailAddressDomain}	A parte do domínio do endereço de e-mail (parte após '@')
${userEmailAddressLocalPart}>	A parte local do endereço de e-mail (parte antes de '@')
${userEmailAddress}	Endereço de e-mail
${userFirstName}	Nome
${userLastName}	Sobrenome
${userLocale}	Local
${userOU}	Atributo Unidade Organizacional (OU) extraído do nome distinto (requer LDAP)
${userREALM}	Informações do Realm Kerberos (requer Active Directory)
${userUIDDomain}	A parte do domínio do ID de login (parte após '@')

${userUIDLocalPart}	A parte local do ID de login (parte antes de '@')
${userUID}	ID de login (formato de endereço de e-mail)
${userUPN}	Atributo userPrincipalName (requer Active Directory)

Variáveis de dispositivo suportadas

Use variáveis de dispositivo para especificar informações sobre um dispositivo móvel.

Variáveis de dispositivo



Chave variável	Descrição do valor
${clientLastCheckin}	Data em que o cliente fez check-in pela última vez (check-in mais recente - MDM ou Cliente)
${deviceAltSN}	Número de série alternativo
${deviceClientDeviceIdentifier}	Identificador usado pelo aplicativo cliente
${deviceGUID}	Identificador de dispositivo globalmente exclusivo
${deviceIccIdentifier}	Sem descrição
${deviceIMEI2}	IMEI2
${deviceIMEI}	IMEI
${deviceIMSI}	IMSI
${deviceLastCheckin}	Data em que o dispositivo fez check-in pela última vez (check-in mais recente - MDM ou Cliente)
${deviceMdmChannelId}	Identificador de dispositivo interno
${deviceMdmDeviceIdentifier}	Identificador usado para MDM
${deviceMEIdentifier}	Sem descrição
${deviceModel}	Modelo
${deviceName}	Nome do dispositivo
${devicePhoneNumber}	Número de telefone do dispositivo
${devicePK}	Identificador de dispositivo exclusivo do cluster
${deviceSN}	Número de série
${deviceUDID}	UDID do iOS
${deviceWifiMacAddress}	Endereço MAC do Wi-Fi

Variáveis de modelo de e-mail

Chave variável	Descrição do valor
${policyMessageContent}	Sem descrição
${policyMessageTitle}	Sem descrição

Variáveis de carimbo de data/hora

Chave variável	Descrição do valor
${timestampMS}	Carimbo de data/hora atual (milissegundos desde a época)

Variáveis de modelo de política

Chave variável	Descrição do valor
${nameOfPolicy}	Nome de política violado
${nextAction}	Próxima Ação de Conformidade Estratificada (diferente de esperar e desativar) a ser executada após o envio da mensagem
${nonComplianceTime}	Contagem de dias que o dispositivo esteve em estado não conforme
${policyViolationFirstTime}	Carimbo de data/hora de quando a violação da política foi acionada pela primeira vez (formato UTC DD-MM-AAAA)
${ruleConditions}	Definição de regra (string de consulta do jeito que aparece agora)

Tópicos relacionados:

- "Atributos" na página 1164

Configurações do AppConnect

Esta seção contém os seguintes tópicos:

Visão geral do AppConnect

Licença: Gold

O AppConnect é um recurso que contém aplicativos para proteger dados em dispositivos iOS e Android. Cada aplicativo com o AppConnect habilitado torna-se um contêiner seguro cujos dados são criptografados, protegidos contra acesso não autorizado e removíveis. Como cada usuário tem vários aplicativos da empresa, cada contêiner de aplicativos também é conectado a outros contêineres de aplicativos seguros. Essa conexão permite que os aplicativos habilitados para AppConnect compartilhem dados, como documentos. O Ivanti Neurons for MDM usa políticas para gerenciar os aplicativos com o AppConnect ativado.

Para obter informações sobre o AppConnect e sobre como configurar e implantar aplicativos AppConnect, consulte o *Guia do AppConnect para Ivanti Neurons for MDM*.

Status de apps seguros

Na página **Dispositivos > Dispositivos**, clique em um dispositivo para visualizar a página **Visão geral**. Nessa página, os usuários podem verificar o status dos apps seguros com as seguintes informações:

- **Status de apps seguros** – Indica se o AppConnect está ativado ou desativado.
- **Status de criptografia de apps seguros** – Indica se a senha do AppConnect está ativada ou desativada.
- **Modo de criptografia de apps seguros** – Indica o modo de criptografia (como AES 256).

Além disso, esses campos podem ser usados:

- Como filtros (painel à esquerda) para restringir as entradas de dispositivo exibidas quando os usuários estão tentando localizar/filtrar dispositivos.
- Como regras ao criar um grupo de dispositivos gerenciados dinamicamente.
- Como filtros de distribuição, que refinam os dispositivos para os quais os apps serão distribuídos com base em regras definidas.

Para cada aplicativo seguro, os administradores podem revisar a Política do recipiente e os status de configuração (instalado, aplicado, enviado ou instalação pendente) na guia **Configurações** da página de detalhes do dispositivo.

Senha do AppConnect

Esta seção contém o seguinte tópico:

Você pode solicitar uma senha do AppConnect, também conhecida como senha de apps seguros. Usando um único login com a senha do AppConnect, o usuário do dispositivo pode acessar todos os apps seguros. No Portal do Administrador, você configura as regras para a senha do AppConnect. A senha do AppConnect não é a mesma senha utilizada para desbloquear o dispositivo.

Alteração/Redefinição da senha

Os usuários podem alterar ou redefinir a senha dos Apps Seguros no aplicativo Secure Apps Manager para dispositivos Android e no aplicativo Go para iOS, desde que o código tenha sido permitido na configuração do AppConnect. Para dispositivos iOS:

Procedimento

1. Abra o aplicativo Go para iOS.
2. Clique em **Apps seguros**.
3. Clique em **Autenticação**.
4. Clique em **Alterar senha de apps seguros** e siga as instruções para alterar/redefinir a senha.

Para dispositivos Android:

1. Abra o aplicativo Secure Apps Manager.
2. Clique em **Alterar senha** no menu de opções.
3. Clique em **Esqueci a senha** para reiniciar a senha.

Geração de PIN avulso para redefinir a senha de apps seguros para dispositivos com iOS

Os administradores podem configurar o Ivanti Neurons for MDM para permitir que usuários de dispositivos iOS redefinam a senha de seus Apps Seguros (AppConnect) quando a esquecerem. Quando esta opção está configurada, os usuários de dispositivos que se registraram no Ivanti Neurons for MDM usando um nome de usuário e uma senha podem inserir as credenciais no Go 3.1.0 para iOS ou em versões mais recentes suportadas para se autenticar e redefinir a senha de Apps Seguros. No entanto, os usuários de dispositivos que esqueceram a senha e o PIN precisam de um mecanismo diferente para se autenticar.

Procedimento

1. No Ivanti Neurons for MDM, o administrador ativa a opção **Senha de Apps Seguros** na configuração padrão do AppConnect para iOS (ou em qualquer outra configuração do AppConnect para iOS).
2. O usuário gera um PIN avulso para um dispositivo específico com iOS no portal de autosserviço clicando na opção **Redefinir senha de apps seguros** e seguindo as instruções. O PIN avulso é válido por 30 minutos.
3. No Go para iOS de um dispositivo, o usuário segue as instruções para redefinir a senha esquecida de Apps Seguros.
4. Quando solicitado, o usuário informa seu nome de usuário e o PIN avulso no lugar da senha regular.
5. O usuário redefine a senha de apps seguros.

Configuração de segurança

Esta seção contém os seguintes tópicos:

Android Enterprise

Licença: Silver

A configuração Android Enterprise define quais opções do Android Enterprise são habilitadas para dispositivos compatíveis. Você pode criar configurações alternativas para diferentes grupos de dispositivos ou apenas editar a configuração padrão. Para obter uma lista de dispositivos compatíveis com Android Enterprise, acesse aqui.

Configurações do Android Enterprise

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Desativar captura de tela (Android 5.0 +)	Selecionar para impedir que os dispositivos usem o recurso de captura de tela nativa.
Impedir controle de apps (Android 5.0 +)	Selecionar para impedir que os usuários modifiquem apps nas Configurações ou iniciadores.
Impedir credenciais de configurações (Android 5.0 +)	Selecionar para impedir que os usuários configurem credenciais de usuário.
Impedir copiar e colar entre perfis (Android 5.0 +)	Selecione para impedir que os dispositivos copiem e colem para outros perfis do Android corporativo.
Impedir Modificar contas (Android 5.0 +)	Selecionar para impedir que os usuários adicionem e removam contas.
Impedir feixe de saída (Android 5.0 +)	Selecione para impedir que um usuário use o NFC para transferir dados do aplicativo.
Impedir Compartilhar local (Android 5.0 +)	Selecionar para impedir que sites e apps avisem o usuário do dispositivo para compartilhar sua localização.

Restringir métodos de entrada (Android 5.0 +)	Selecione para restringir os métodos de entrada designando uma lista de nomes de pacotes permitidos. Se não houver pacotes na lista de permissão, apenas os métodos de entrada do sistema serão permitidos. Os métodos de entrada não são restritos apenas aos apps de trabalho, mas a todo o dispositivo.
Restringir serviços de acessibilidade (Android 5.0 ou superior)	Selecione para restringir os serviços de acessibilidade designando uma lista de nomes de pacotes permitidos. Se não houver pacotes na lista de permissão, apenas serviços de acessibilidade do sistema serão permitidos. Os serviços de acessibilidade não são restritos apenas aos apps de trabalho, mas a todo o dispositivo.
Desativar ID do chamador (Android 6.0 +)	Define se as informações do ID do chamador do perfil de trabalho serão exibidas no dispositivo no recebimento de chamadas.

- Configuração do Android Enterprise

Editando a configuração padrão do Android Enterprise

Administradores globais podem permitir que administradores de espaço editem a distribuição para qualquer uma das seguintes configurações padrão do Android Enterprise no espaço personalizado.

- Android Enterprise: perfil de trabalho em dispositivo de propriedade da empresa (Android for Work)
- Android Enterprise: dispositivo gerenciado de trabalho (Android for Work)
- Android Enterprise: dispositivo gerenciado com perfil de trabalho

Editar a distribuição para qualquer uma das configurações acima

Procedimento

1. Na guia Configurações, selecione a configuração a ser editada.
2. Clique no ícone Editar.
3. Clique em **Avançar**
4. Selecione qualquer um dos seguintes níveis de distribuição para a configuração:
   - Todos os dispositivos – para distribuir a configuração a todos os dispositivos compatíveis.
     a. Na seção Resumo da distribuição, selecione Aplicar a dispositivos em outros espaços.
     b. Selecione "Permitir que o administrador de espaço edite a distribuição".
   - Personalizado – Define um conjunto específico de grupos de dispositivos que receberão esta configuração.
     a. Em Definir distribuição do grupo de dispositivos, marque a caixa de seleção ao lado do tipo de dispositivo para o qual você deseja distribuir as configurações. Como alternativa, você pode procurar grupos de dispositivos digitando o nome do grupo no campo de pesquisa Pesquisar grupos de dispositivos.
     b. Selecione "Permitir que o administrador de espaço edite a distribuição".
5. Clique em **Concluído**.

Quando essa configuração é aplicada aos espaços, os administradores de Espaço poderão editar a distribuição clicando no ícone de distribuição no espaço personalizado.

Configuração do Android Enterprise

Esta seção contém o seguinte tópico:

Licença: Silver

O Android Enterprise é um programa oferecido pelo Google que permite aos administradores de mobilidade:

- Separar dados pessoais e referentes ao trabalho
- Proteger e gerenciar aplicativos corporativos
- Controlar aplicativos do sistema (como Câmera e Galeria)
- Provisionar e configurar aplicativos centralmente no contêiner do Android Enterprise
- Impedir a perda de dados (captura de tela)

Você pode configurar o Ivanti Neurons for MDM como o servidor UEM que gerencia o Android Enterprise. O Android Enterprise requer pelo menos Android 3.0. Há duas configurações suportadas do Android Enterprise: Proprietário do Dispositivo e Perfil Gerenciado – Pertencente ao Funcionário.

Dispositivos compatíveis

Ivanti Neurons for MDM atualmente oferece suporte a Android Enterprise apenas em dispositivos que executam Android 5.0 e têm o Android Enterprise habilitado pelo fabricante. O Android Enterprise é obrigatório para o modo Quiosque em dispositivos que executam Android 5.0.

Pré-requisito

Se você ainda não tiver registrado seu domínio no Google, é necessário primeiro se cadastrar no programa no site do Google:

https://admin.google.com.

Durante o processo, o usuário irá:

- Reivindicar um domínio (deve corresponder ao domínio dos endereços de email do usuário)
- Receber um token
- Fazer o download de uma ID do cliente JSON

Ambos os itens são necessários ao configurar o Android Enterprise no Ivanti Neurons for MDM.

Após o processo, o usuário receberá um e-mail com instruções para a confirmação de que ele possui o domínio reivindicado.

Se a empresa já tiver usado seu nome de domínio para se cadastrar no Google Apps for Work, consulte https://support.google.com/work/android/answer/6174062 para obter informações sobre como habilitar o Android Enterprise.

Conectar o Ivanti Neurons for MDM com ao Android Enterprise

Depois de se inscrever no Android Enterprise, configure o Ivanti Neurons for MDM como o servidor UEM.

Obter credenciais do Android Enterprise

Procedimento

1. Acesse **Admin** > **Android Enterprise**.
2. Clique em **Console de desenvolvedores do Google**.
3. Clique no primeiro link exibido para acessar o Console de desenvolvedores do Google.
4. Selecione **Criar um projeto** a partir do menu suspenso.
5. Inserir um nome para o projeto.
6. Aceite os termos de serviço.
7. Clique em **Criar**.
8. Clique em **API**.
9. Selecione **APIs**.
10. Digite **emm** no campo Pesquisar para encontrar a EMM do Google Play.
11. Clique no link **Google Play EMM API**.
12. Clique em **Habilitar API**.
13. Clique em **Credenciais**.
14. Selecione **conta de Serviço**.
15. Clique em **Criar** para salvar o arquivo JSON.

Adicionar o token MDM do Android Enterprise ao Ivanti Neurons for MDM

Procedimento

1. Faça login em https://admin.google.com.
2. Clique em **Segurança**.
3. Caso não veja Configurações do Android Enterprise, clique em **Mostrar mais**.
4. Selecione **Configurações do Android Enterprise**.
5. Em **Administrar provedor de gerenciamento de mobilidade empresarial**, copie o token MDM.
6. Retorne ao portal do Ivanti Neurons for MDM.
7. Clique em **Concluído**.

8. Na caixa 2, cole o token MDM que você acabou de copiar.
9. No campo **Domínio**, insira o domínio que você reivindicou no Google.
10. Clique em **Escolher arquivo** e carregue o arquivo JSON que você baixou.
11. Clique em **Conectar**.
    A mensagem **Conectado ao Google** é exibida quando a conexão ocorre com êxito.
12. Na caixa 3, clique em **Autorizar** para indicar que deseja conceder ao Ivanti Neurons for MDM acesso aos seus dados de usuário do Google.
13. Clique em **Aceitar**.
    A mensagem **Conectado aos usuários** será exibida no portal do Ivanti Neurons for MDM.

Sincronizar usuário entre Ivanti Neurons for MDM e Google

Antes de você implantar o Android Enterprise para usuários Android gerenciados pelo Ivanti Neurons for MDMIvanti Neurons for MDM, cada usuário deve ter um registro correspondente no Google Admin Portal. As etapas necessárias para sincronizar as informações do usuário entre o Ivanti Neurons for MDM e o Google Admin Portal mudam em função de você ter ou não configurado uma integração com os serviços de diretório da sua organização (AD/LDAP).

Usuários do Active Directory/LDAP

Se você tiver configurado uma integração AD/LDAP com o Ivanti Neurons for MDM, deverá usar o Google Apps Directory Sync para configurar uma integração AD/LDAP com o Google Admin Portal. Consulte https://support.google.com/a/answer/106368?hl=en para obter mais informações.

Usuários locais

Se você criou somente usuários locais no Ivanti Neurons for MDM e não pretende integrá-lo a um serviço de diretório, conclua as seguintes etapas para sincronizar esses usuários com o Google Admin Portal:

Procedimento

1. Faça login no Google Admin Portal em https://admin.google.com.
2. Clique em Usuários.
3. Clique no ícone Adicionar usuário ou Adicionar vários usuários no canto inferior direito.

4. Para cada usuário do Ivanti Neurons for MDM que usará o Android Enterprise, adicione um usuário do Google com o mesmo nome de usuário e endereço de e-mail do usuário do Ivanti Neurons for MDM.

5. No portal do Ivanti Neurons for MDM, para cada usuário do Ivanti Neurons for MDM que acabou de ser adicionado ao Google Admin Portal:
   a. Clique no link do nome de usuário na guia Usuários para exibir os detalhes do usuário.
   b. Selecione **Sincronizar o usuário com o diretório de usuários do Google**.
   c. Clique em **Sincronizar com diretório de usuários do Google**.
   d. Confirme se o Status do Google está listado como Habilitado.

Implantar o Android Enterprise em dispositivos compatíveis

Duas configurações são necessárias para implantar o Android Enterprise:

- A configuração Android Enterprise: Perfil de Trabalho em Dispositivo de Propriedade da Empresa habilita o Android Enterprise.
- A configuração Bloqueio e Quiosque define as restrições do Android Enterprise a serem aplicadas.

Desativar dispositivos registrados

Em cenários de BYOD, mudar de Administrador do Dispositivo para o Perfil de Trabalho do Android Enterprise em Dispositivo de Propriedade da Empresa não exige a desativação e reinscrição de dispositivos. O apagamento ou a desativação de um dispositivo é necessário apenas para passar do modo Administrador do dispositivo para o modo Proprietário do dispositivo.

Quando você seleciona um dispositivo inscrito nos modos Proprietário do Dispositivo / Proprietário de Perfil Avançado / Habilitação Pessoal de Propriedade da Empresa para a ação Desativar, um pop-up aparece na tela indicando que "O comando Desativar não é compatível com dispositivos de propriedade organizacional".

Implementar o dispositivo

Procedimento

1. No portal do Ivanti Neurons for MDM, acesse **Configurações**.
2. Clique em **Android Enterprise: Perfil de Trabalho**.
3. Clique em **Editar**.
4. Clique em **Avançar**.

5. Selecione **Todos os dispositivos** ou **Personalizar**.
6. Se você selecionou **Personalizar**, pesquise e selecione os grupos de dispositivos que devem receber as configurações do Android for Work.
7. Clique em **Concluído**.
8. Clique em **Voltar à lista** (canto superior esquerdo).
9. Clique em **+Adicionar**.
10. Clique em **Bloqueio e Quiosque: Android Enterprise**.
11. No campo **Nome**, insira o texto que identifica a configuração.
12. Em **Escolha o tipo de bloqueio**, selecione **Perfil de trabalho**.
13. Selecione as configurações de bloqueio que você deseja aplicar aos dispositivos de destino.
14. Clique em **Avançar**.
15. Selecione **Todos os dispositivos** ou **Personalizar**.
16. Se você selecionou Personalizar, pesquise e selecione os grupos de dispositivos que devem receber as configurações do Android Enterprise.
17. Clique em **Concluído**.

não é possível fazer alterações no perfil resultante depois de sua implantação. Em vez disso, você precisa criar uma nova configuração do Android Enterprise e implementá-la.

Confirmar a implementação

É possível confirmar se o Android Enterprise foi implementado das seguintes formas:

- Em **Usuários > Usuários**, encontre a entrada para um usuário e, em seguida, verifique se o **Status do Google** está **Habilitado**.
- Em **Dispositivos > Dispositivos,** clique no link de um dispositivo e verifique se o status de **Android Enterprise** é **Habilitado**.

O **Status do Google** para um usuário deve estar listado como **Habilitado**. Se ele não estiver Habilitado, o usuário não será capaz de registrar dispositivos.

Para empresas que não são assinantes do GSuite, o método de contas gerenciadas do Google Play permite que os usuários se registrem no Android Enterprise. Se o Android Enterprise tiver sido configurado como Contas Google Play gerenciadas, o usuário não será mostrado como **Status do Google: ativado** até um dispositivo Android Enterprise ser registrado. Consulte Contas gerenciadas do Google Play para obter mais informações sobre Contas gerenciadas do Google Play.

Implantar os apps do Android Enterprise

Todo aplicativo desenvolvido para Android Enterprise pode incluir opções que você pode configurar por meio do Ivanti Neurons for MDM.

Procedimento

1. No portal do Ivanti Neurons for MDM, acesse **Aplicativos > Catálogo de Aplicativos**.
2. Encontre o aplicativo na Google Play Store.
3. Clique na entrada do aplicativo.
4. Aceite as permissões em nome dos usuários do Android Enterprise.
5. Clique em **Avançar**.
6. Selecione uma opção de distribuição.
7. Expanda **Opções avançadas e configuração do aplicativo**.
8. Use as diretrizes a seguir para concluir as opções:

Configuração	Descrição
Instalar no dispositivo	Selecione essa opção para iniciar a instalação imediatamente após a inscrição. O usuário deverá confirmar a instalação do aplicativo, exceto se o dispositivo for um Samsung Knox, e a opção de instalação silenciosa abaixo for selecionada.
Não exibir o aplicativo no App Catalog do usuário final	Selecione essa opção caso não queira que o usuário veja o aplicativo no catálogo de aplicativos no dispositivo.
Instalar silenciosamente em dispositivos Samsung Knox	Selecione essa opção caso não queira que seja solicitado ao usuário confirmar a instalação nos dispositivos Samsung Knox.

Configuração	Descrição
Definir prioridade de instalação de apps	No caso de apps Android Enterprise, você pode priorizar o download de apps específicos antes de outros apps. Por exemplo, você pode priorizar o download de apps Tunnel e E-mail antes de outros apps não críticos. As opções de níveis de prioridade disponíveis são as seguintes: • **Alto** • **Médio** (selecionada por padrão) • **Baixo**

Configuração	Descrição
	Essa configuração é aplicável a apps Internos, Públicos, Privados e da Web. Os apps internos são instalados via cliente, e os apps públicos e privados são instalados via Google. A prioridade do aplicativo é adotada somente para os apps que foram instalados pelo mesmo canal.
Instalar somente quando conectado ao Wi-Fi	Selecione essa opção para instalar o aplicativo apenas quando o dispositivo estiver conectado ao Wi-Fi.
Instalar somente ao receber carga	Selecione essa opção para instalar o aplicativo apenas quando o dispositivo estiver sendo carregando.

Configuração	Descrição
Instalar somente quando ocioso	Selecione essa opção para instalar o aplicativo apenas quando o dispositivo estiver ocioso (isto é, quando não estiver sendo ativamente utilizado pelo usuário).
Início automático na instalação	Selecione esta opção para iniciar um aplicativo logo após a instalação. Este recurso está disponível apenas se o aplicativo for recém-instalado no dispositivo e não for uma atualização de versão.

9. Clique em **Avançar**.
10. Selecione uma opção de promoção.
11. Clique em **Concluído**.

Configurar apps comerciais

Os aplicativos do Android Enterprise estão disponíveis na seção Aplicativos Empresariais do catálogo de aplicativos, incluindo os seguintes apps:

- Divide Productivity
- E-mail+

- Túnel
- Gmail

Android Enterprise: modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP)

O Ivanti Neurons for MDM oferece suporte ao registro de dispositivos no modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP), pelo proprietário do dispositivo, sem a necessidade dos Serviços do Google Mobile (GMS). Trata-se de uma configuração do sistema, e os administradores não podem adicionar a configuração. Os administradores podem distribuí-las ou não.

Procedimento

1. Faça login no Ivanti Neurons for MDM com as credenciais de usuário.
2. **Configurações de pesquisa** para Android Enterprise: modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP).
3. Edite a configuração e distribua-a para os grupos de dispositivos apropriados. Por exemplo: dispositivos com Android.
4. Clique em **Concluído**.

Para que os recursos do modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP) fiquem totalmente funcionais, você deve habilitar o Android Enterprise no seu locatário do Ivanti Neurons for MDM.

Desafio de trabalho (Work Challenge) do Android

Esta seção contém o seguinte tópico:

- "Como criar a configuração do Desafio de trabalho (Work Challenge) do Android:" abaixo
- "Definições de configuração" na página 535

Licença: Silver

Uma configuração de Desafio de trabalho (Work Challenge) do Android define senhas seguras para que os usuários acessem os dados do perfil de trabalho e dos apps. Exige o Work Profile do Android corporativo.

Observações de implementação:

- Os Administradores podem aplicar uma política de senha de dispositivo e uma política de senha de perfil de forma independente.

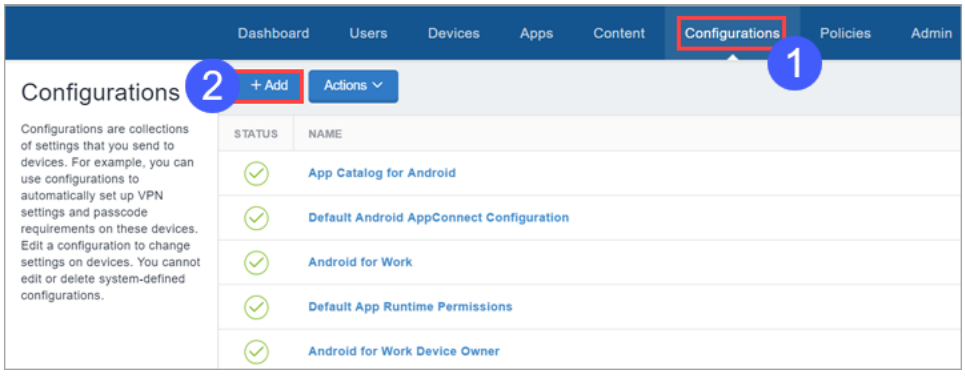
  O Ivanti Neurons for MDM não envia essa configuração a clientes Android com versão anterior à 7.0 porque tais dispositivos não são compatíveis com esse recurso.

- O Ivanti Neurons for MDM envia essa configuração apenas aos dispositivos com perfil de trabalho do Android Enterprise.

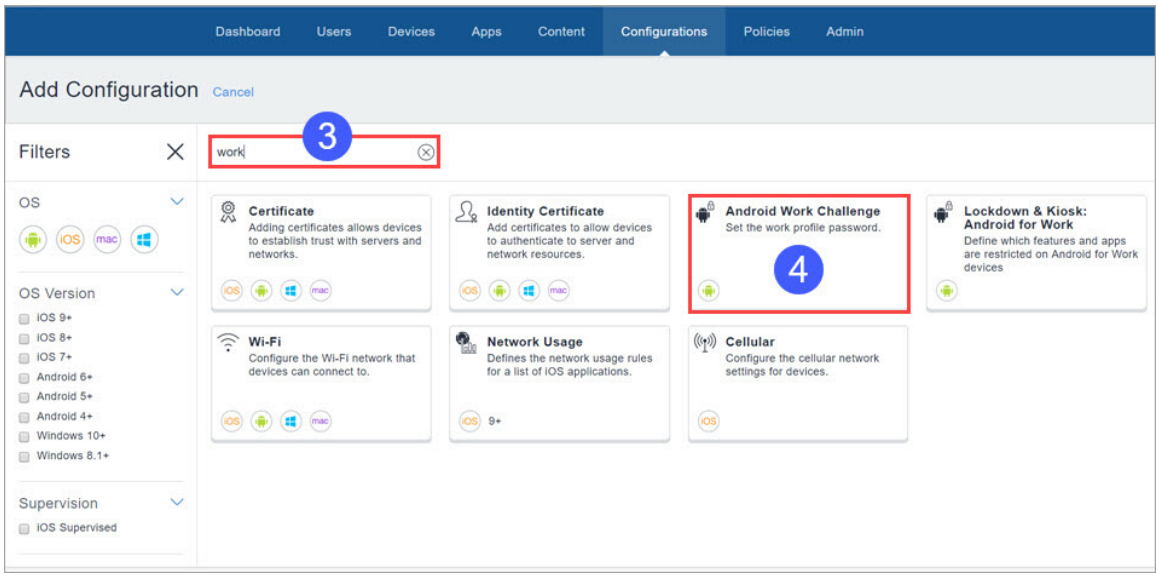
Como criar a configuração do Desafio de trabalho (Work Challenge) do Android:

Procedimento

1. Clique em **Configurações**.

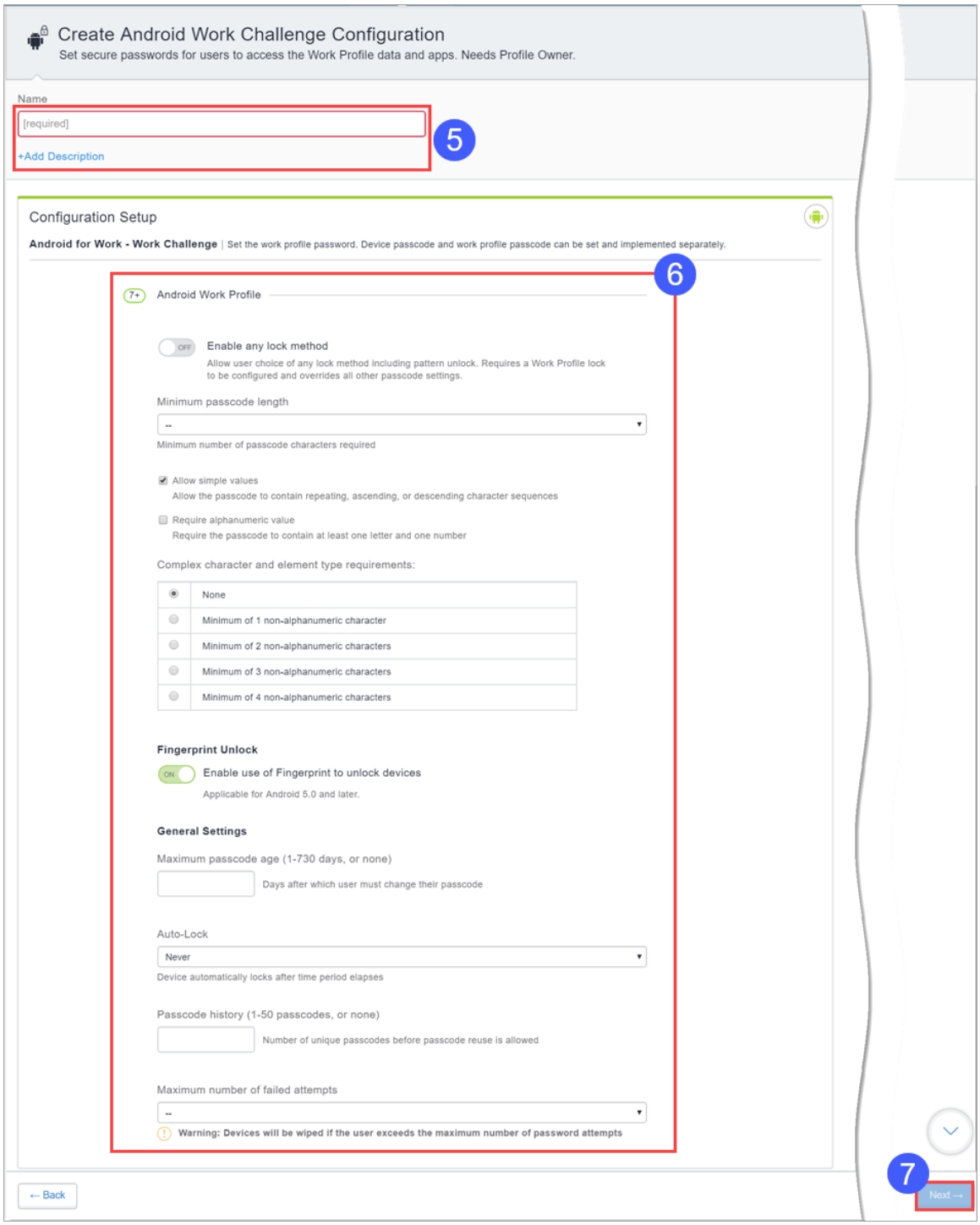


2. Clique em **+Adicionar**.



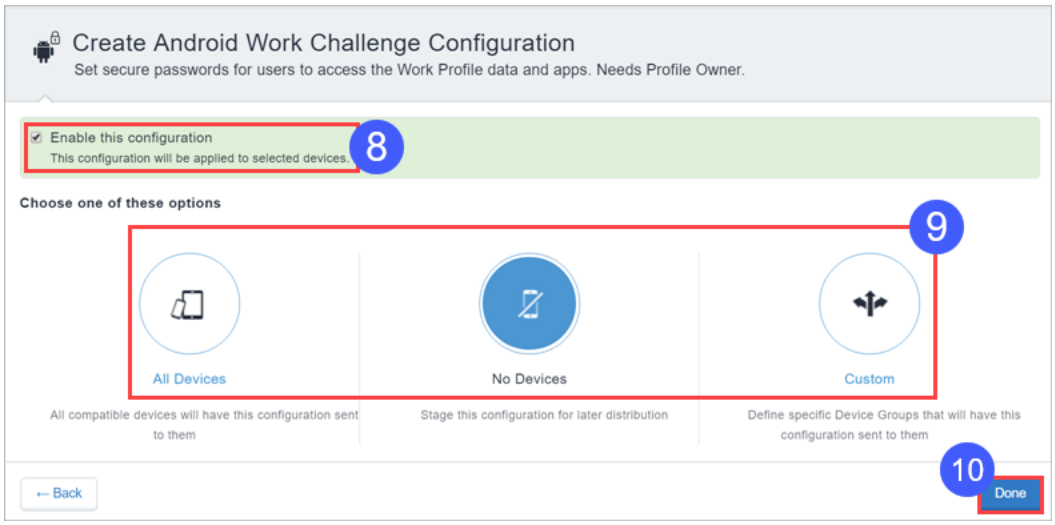
3. Digite "work" (trabalho) no campo de busca
 .

4. Selecione a configuração **Desafio de trabalho (Work Challenge) do Android**.



5. Insira um nome para a configuração e, se desejar, uma descrição.

6. Use os campos em Definição da Configuração para criar a configuração. Consulte Definições de configuração para obter detalhes sobre as configurações.
7. Clique em **Avançar ->**.



8. Habilite a configuração se desejar.
9. Configure as definições de distribuição para todos os dispositivos, nenhum dispositivo ou um conjunto personalizado de dispositivos.
10. Clique em **Concluído**.

Definições de configuração

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Ativar qualquer método de bloqueio	Permita que o usuário escolha qualquer método de bloqueio, incluindo o desbloqueio padrão. Substitui todas as outras configurações de senha.
Tamanho mínimo da senha	Selecione um tamanho mínimo da senha, de 4 a 16 caracteres.
Permitir valores simples	Habilite para permitir que a senha tenha sequências de caracteres repetidos, crescentes ou decrescentes.
Exigir valor alfanumérico	Habilite para exigir que a senha tenha pelo menos uma letra e um número.
Requisitos de caractere complexo e do tipo de elemento	Configure os requisitos de caractere complexo e tipo de elemento, como segue: • Nenhum • Pelo menos 1 caractere não alfanumérico • Pelo menos 2 caracteres não alfanuméricos • Pelo menos 3 caracteres não alfanuméricos • Pelo menos 4 caracteres não alfanuméricos
Desbloqueio por impressão digital	Habilite para permitir que os usuários desbloqueiem seus dispositivos com suas impressões digitais.

Duração máxima da senha	Configure uma duração máxima da senha, de nenhuma até 730 dias.
Bloqueio automático	Selecione um período após o qual o dispositivo entra em bloqueio automático. O intervalo de tempo é de nunca até 15 minutos.
Histórico da senha	Especifique o número de senhas exclusivas exigido antes que a reutilização da senha seja permitida, de nenhuma a 50 senhas.
Número máximo de tentativas com falha	Selecione o número máximo de tentativas com falha. **AVISO: o Ivanti Neurons for MDM apaga os dispositivos em que o usuário ultrapassa o número máximo de tentativas de senha.**

Configuração do certificado

Uma configuração de certificado identifica o certificado que será distribuído aos dispositivos.Os certificados permitem que os dispositivos estabeleçam uma confiança com o servidor e os recursos de rede. A partir da versão 76, só oferecemos suporte a certificados v3.

Como administrador, você agora pode gerar certificados do Ivanti Neurons for MDM para login de cartão inteligente e IDs de objetos personalizados (OIDs). É possível gerar certificados para as seguintes opções de autenticação:

- Autenticação do cliente – ativada por padrão
- IPSEC – opcional, pode ser ativada pelo administrador
- Login de cartão inteligente – opcional, pode ser ativada pelo administrador
- OIDs personalizados – opcionais, podem ser ativados pelo administrador

Este recurso só é aplicável para as seguintes autoridades de certificação (CA):

- Autoridade de certificação local
- Autoridade de certificação intermediária
- Autoridade de certificação externa – configure as políticas do aplicativo do modelo de autoridade de certificação no servidor NDES para oferecer suporte a IPSEC, login de cartão inteligente e OIDs personalizados
- Autoridade de certificação SCEP presencial

Distribuir configuração

A partir da versão 91 do Ivanti Neurons for MDM, os administradores globais poderão delegar administradores de espaço para editar a configuração do certificado para todos os dispositivos e para a opção de distribuição personalizada. Para a configuração do certificado, você pode selecionar a opção Permitir que esta configuração esteja disponível em todos os espaços. Esta opção disponibiliza a configuração Certificado para todos os Espaços e pode ser usada no Exchange, no Wi-Fi, em VPN e em qualquer outra configuração aplicável. Essa opção pode ser usada em cenários nos quais a configuração do certificado só precisa ser distribuída aos dispositivos (em Espaços não padrão) como parte de configurações associadas, e não como uma configuração individual.

Procedimento

1. Digite um nome no campo Nome.
2. Carregue o arquivo do certificado.
3. Clique em **Avançar**.
4. Selecione a opção **Habilitar essa configuração**.
5. Selecione uma das opções de distribuição a seguir:
    - **Todos os dispositivos**. Selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.
    - **Nenhum dispositivo** (padrão)
    - **Personalizado** Selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.

    Independentemente dos espaços, a configuração do certificado pode ser configurada em todos os espaços, distribuída a todos os dispositivos e aplicada a todos os dispositivos em outros espaços do dispositivo.
6. Clique em **Concluído** .

Configurações do certificado

Como um administrador, você pode configurar uma autoridade de certificação não SCEP local.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Administrador** > **Infraestrutura** > **Gerenciamento de certificados** > **Autoridade de certificação**.
3. Clique em **+Adicionar**. As opções a seguir são listadas:
   - **Criar a autoridade de certificação local fornecida pelo Ivanti Neurons for MDM**.
   - **Assinar CA local do Ivanti Neurons for MDM com sua CA existente**.
   - **Conectar a uma Autoridade de certificação do Cloud publicamente confiável**.
   - **Conectar uma Autoridade de certificação SCEP presencial**.
   - **Conectar uma Autoridade de Certificação não SCEP local**.
4. Preencha os campos a seguir conforme necessário:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
URL	URL da CA OpenTrust que o administrador deve adquirir da OpenTrust.
Senha	Insira a senha para o Certificado de autenticação.
Certificado de autenticação	Aceita o formato de arquivo .p12 que é fornecido pela OpenTrust/IDnomic.
Cadeia de certificados da CA TLS	Aceita formato de arquivo PEM que é fornecido pela OpenTrust/IDonomic.

5. Clique em **Concluído**.

Após configurar a autoridade de certificação não SCEP local, você deve criar o certificado de identidade. Com base no ID do perfil, preencha todos os campos obrigatórios para concluir a configuração.

Uma notificação é criada quando a geração do certificado CA SCEP falha devido aos dois motivos a seguir e o tempo limite da Etapa 2 é atingido:

1. O conector não está acessível
2. O servidor CA não está acessível

Transparência de certificado

Aplicável a: iOS 12.1.1, macOS 10.14.2, e tvOS 12.1.1 e a versões mais recentes com suporte.

Imposição de transparência de certificado de controles que somente pode aparecer em um perfil de dispositivo. Você pode incluir múltiplos certificados e desabilitar domínios conforme necessário.

Criar uma configuração de Transparência de certificado

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **certificado** no campo de pesquisa e, então, clique na configuração **Transparência de certificado**.
4. Digite um nome e descreva a configuração.
5. Especificar os **Domínios que serão desabilitados**. Clique em **+ Adicionar domínio** para adicionar mais de um domínio. Pode ser usado um ponto no início para corresponder subdomínios, no entanto, uma regra de correspondência de domínio não deve corresponder a todos os domínios em um domínio de nível superior. Por exemplo, ".exemplo.com" e ".exemplo.co.uk" são permitidos, mas ".com" e ".co.uk" não. Domínios curinga não são suportados.
6. Especificar um **Certificado Hash** após selecionar um algoritmo (SHA 256). Clique em **+ Adicionar** para adicionar mais de um certificado hash.
7. Clique em **Avançar** para configurar as definições de distribuição.
8. Clique em **Concluído**.

Para gerar os dados especificados pela chave hash no dicionário subjectPublicKeyInfo, use o seguinte comando para obter um certificado com código PEM:

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Se seu certificado possui código DER, use o seguinte comando:

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Para obter mais informações, consulte Como criar uma configuração.

Configuração de verificação de revogação de certificado

Esta configuração permite que os administradores verifiquem uma matriz de certificados revogados de um dispositivo. Os administradores podem certificar uma autoridade de certificação (CA) que permite que a configuração habilite a verificação de revogação para todos os certificados vinculados a essa CA.

Aplicável a: iOS 14.2+

Procedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **certificado** no campo de pesquisa e, então, clique na configuração **Verificação de revogação de certificado**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Selecione o algoritmo como **SHA 256** e insira o **hash** do certificado raiz.

   No hash, você deve inserir um hash SHA-256 codificado Base64 (binário) na chave pública do certificado. Consulte a documentação da Apple quanto aos certificados raiz confiáveis disponíveis para os sistemas operacionais Apple. Você pode adicionar múltiplos certificados raiz nesta configuração.

5. Clique em **Avançar**.
6. Selecione a opção **Ativar esta configuração**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizado.
8. Clique em **Concluído**.

Criar configuração Modo de Aplicativo Único Autônomo

A configuração Modo de Aplicativo Único Autônomo permite assegurar que apenas aplicativos específicos sejam executados em um dispositivo. Mesmo que o usuário tente iniciar um aplicativo diferente, a configuração inicia apenas o aplicativo específico.

Procedimento

1. Acesse **Configurações** > **Adicionar** > **Modo de Aplicativo Único Autônomo**.
2. Use as diretrizes a seguir para definir o aplicativo e as configurações relacionadas.

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Definição da configuração	**Identificador do pacote** - (obrigatório) o identificador exclusivo do pacote. Se dois dicionários contiverem o mesmo valor BundleIdentifier, mas um valor TeamIdentifier diferente, isso será considerado um erro e o perfil não será instalado.
	Identificador de equipe - (obrigatório) o identificador da equipe do desenvolvedor, usado quando o aplicativo foi assinado.

3. Clique em **Avançar**.
4. Na tela **Distribuição**, selecione os grupos que receberão essa configuração.
5. Clique em **Concluído**.

Criar configuração de proxy DNS

Como administrador do Ivanti Neurons for MDM, você pode definir os parâmetros de proxy DNS usando a Configuração de Proxy DNS para usuários de dispositivos iPhone e iPad. Você pode usar a carga Proxy DNS para especificar o aplicativo que fornece a extensão de rede do proxy DNS e outros valores específicos do fornecedor.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá até **Configurações**

3. Digite **DNS** no campo de pesquisa e clique em **Configuração de Proxy DNS**.
4. Digite um nome e descreva a configuração.
5. Insira os seguintes parâmetros na Configuração de Proxy DNS:
   - Identificador do pacote de aplicativo (obrigatório).
   - Identificador de pacote do provedor.
   - Configuração do provedor (chave-valor)
6. Clique em **Avançar**.
7. Selecione a opção **Habilitar essa configuração**.
8. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
9. Clique em **Concluído**.

Configuração Log do Dispositivo

A configuração Log do Dispositivo permite habilitar logs de rede e segurança para dispositivos Android.

Criando uma configuração Log do Dispositivo

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. No campo de pesquisa, digite **Log do Dispositivo** e selecione a configuração.
4. Digite um nome e descreva a configuração.
5. Na seção **Definição da configuração**, selecione uma ou ambas as opções:

- Habilitar log de rede
- Habilitar log de segurança

> Para informações sobre as versões do Android com suporte para log de segurança e rede, consulte as tabelas em **Matriz de logs de segurança** abaixo.

6. Alguns fabricantes de dispositivos podem permitir a pré-concessão dessa permissão em dispositivos totalmente gerenciados usando OEMConfig (configurações gerenciadas).
7. Clique em **Avançar** para configurar as definições de distribuição.
8. Clique em **Concluído**.

Matriz de logs de segurança

Tipo de dispositivo	Versões Android suportadas
Dispositivos Gerenciados de Trabalho e modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP)	7, 8, 9, 10, 11, 12, 13
Dispositivos gerenciados com perfil de trabalho	8, 9, 10
Perfil de trabalho	N/D
Perfil de trabalho em dispositivo de propriedade da empresa	11, 12, 13

Matriz de log de rede

Tipo de dispositivo	Versões Android suportadas
Dispositivos Gerenciados de Trabalho e modo Dispositivo Gerenciado de Trabalho Não GMS (AOSP)	8, 9, 10, 11, 12, 13
Dispositivos gerenciados com perfil de trabalho	8, 9, 10
Perfil de trabalho	12, 13
Perfil de trabalho em dispositivo de propriedade da empresa	12, 13

Após instalar a configuração Log do Dispositivo no dispositivo, o usuário recebe uma notificação contendo informações sobre o gerenciamento do dispositivo e o log de rede. Clique em OK para reconhecer a notificação.

Solicitação de logs de depuração

Procedimento

1. Faça login no Ivanti Neurons for MDM.
2. Acesse **Dispositivos** > **Detalhes do dispositivo**.
3. Na seção **Visão Geral**, clique no botão de três pontos verticais ao lado do botão **Forçar check-in**.
4. Selecione **Solicitar logs de depuração**.
5. Selecione uma das opções a seguir:
    - Excluir relatório de bug - ao selecionar esta opção e clicar em Avançar, uma janela de confirmação aparece na tela. Clique em **Solicitar logs de depuração**. Os usuários não precisam dar nenhum consentimento para esta opção, e os logs excluiriam o relatório de bugs referentes aos dispositivos Android selecionados.
    - Incluir relatório de bug - ao selecionar esta opção e clicar em Avançar, uma janela de confirmação aparece na tela. Clique em **Solicitar logs de depuração**. Os usuários devem dar consentimento para compartilhar o relatório de bug. No caso de dispositivos Android, os usuários serão solicitados a enviar os logs do dispositivo, incluindo o relatório de bug.

Criptografia para Android

A configuração de criptografia define as exigências de criptografia de dispositivos Android no modo Administrador do Dispositivo.A criptografia do dispositivo assegura que os dados corporativos confidenciais não poderão ser acessados por técnicas conhecidas de modificação ou desbloqueio de dispositivos. A criptografia armazena dados do dispositivo em um formato ilegível para que qualquer pessoa que tente roubar o dispositivo não consiga acessar os dados.

A ativação da criptografia solicita que o usuário criptografe dispositivo e exige uma senha para ele. A senha descriptografa os dados para sua leitura seja possível. A criptografia do dispositivo é ativada automaticamente no Android corporativo (perfil de trabalho ou dispositivos gerenciados) ou nos dispositivos iOS quando uma senha é configurada. O dispositivo não pode ser usado enquanto estiver sendo criptografado. Após ser instalada, a criptografia só poderá ser desativada com a redefinição do dispositivo para configurações de fábrica.

Configurações de criptografia

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Habilitar criptografia do dispositivo	Selecione a configuração para ativar a criptografia em todos os dispositivos Android que podem criptografar e que receberem essa configuração.

A configuração de criptografia para Android foi preterida em dispositivos Samsung no modo Administrador do Dispositivo, no Android 11. Essa criptografia é suportada por padrão em dispositivos Android Enterprise quando uma senha de dispositivo está definida.

Para obter mais informações, consulte Como criar uma configuração.

DNS criptografado

Licença: Gold

Aplicável a:

- iOS 14.0 ou versões mais recentes com suporte.
- macOS 11.0 ou versões mais recentes com suporte.

Configure um DNS criptografado que permitirá aumentar a segurança sem a necessidade de configurar uma VPN.

Esta seção contém os seguintes tópicos:

- Configuração de DNS criptografado
- Definições da configuração de DNS criptografado

Configuração de DNS criptografado

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **DNS** no campo de pesquisa e clique na configuração **DNS criptografado**.
4. Digite um nome e descreva a configuração.
5. Insira as definições da configuração de DNS criptografado.
6. Clique em **Avançar**.
7. Selecione a opção **Habilitar essa configuração**.

8. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
9. Clique em **Concluído** .

Definições da configuração de DNS criptografado

Use as definições na tabela a seguir para configurar o DNS criptografado. Para obter mais informações sobre essas definições, consulte a Documentação da Apple.

Configuração	Descrição
Configurações de DNS	Um dicionário que define uma configuração para um servidor de DNS criptografado.
Protocolo de DNS	Especifica o protocolo de transporte criptografado usado para se comunicar com o servidor DNS. Selecione um dos protocolos a seguir: • HTTPS • TLS
URL do servidor	O modelo de URI de um servidor DNS sobre HTTPS, como definido em RFC 8484. Esse URL deve usar o esquema https://, e o nome de host ou endereço no URL será usado para validar o certificado do servidor. Se nenhum Endereço do servidor for fornecido, o nome de host ou endereço no URL será usado para determinar os endereços do servidor. Essa chave deve estar presente somente se o Protocolo de DNS for HTTPS.
Endereços do servidor	Uma lista não ordenada de strings de endereço IP do servidor DNS. Esses endereços IP podem ser uma mistura de endereços IPv4 e IPv6. Clique em **Adicionar** para adicionar um ou mais endereços de servidor.
Domínios de correspondência complementares	Uma lista de strings de domínio usada para determinar quais consultas de DNS usarão o servidor DNS. Se essa matriz não for fornecida, todos os domínios usarão o servidor DNS. Clique em **Adicionar** para adicionar um ou mais domínios.
Proibir que os usuários desabilitem as Configurações de DNS	Proíbe que os usuários desabilitem as configurações de DNS. Essa chave está disponível apenas em dispositivos supervisionados.
Regras de demanda	Uma matriz de regras que define as configurações de DNS. Se as regras não estiverem presentes, o sistema sempre aplicará as configurações de DNS. Clique em **+ Adicionar regras de demanda** para adicionar um ou mais conjuntos de regras de demanda.

Configuração	Descrição
Rede	A ação a ser tomada se esse dicionário corresponder à rede atual. Selecione uma das ações a seguir: • **Conectar:** aplique Configurações de DNS quando o dicionário corresponder. • **Desconectar:** não aplique Configurações de DNS quando o dicionário corresponder. • **Avaliar a conexão:** aplique Configurações de DNS com exceções por domínio quando o dicionário corresponder.
Avaliar a conexão	Essa opção de rede possui as seguintes configurações: • **Ação do domínio** - O comportamento das configurações de DNS para os domínios especificados. Selecione uma das ações a seguir: ◦ **Nunca se conectar** - Não usar as Configurações de DNS para os domínios especificados. ◦ **Conectar se necessário** - Permitir o uso das Configurações de DNS para os domínios especificados. • **Domínios** - Os domínios aos quais essa avaliação se aplica. Clique em **+ Adicionar** para adicionar um ou mais domínios.
Regras	Clique em **+ Adicionar** para adicionar uma ou mais regras para corresponder os seguintes parâmetros aos valores especificados correspondentes.
Associação de domínio de DNS	Uma matriz de nomes de domínio. Essa regra estabelece correspondência se qualquer um dos nomes de domínio na lista especificada corresponder a qualquer domínio na lista de domínios da pesquisa do dispositivo.
Associação de endereço do servidor de DNS	Uma matriz de endereços IP. Essa regra estabelece correspondência se qualquer um dos servidores DNS especificados da rede corresponder a qualquer entrada na matriz.

Configuração	Descrição
Associação de SSID	Uma matriz de SSID para estabelecer correspondência em relação à rede atual. Se a rede não for uma rede Wi-Fi ou se o SSID não aparecer nessa matriz, a correspondência falhará. Omita essa chave e a matriz correspondente para estabelecer correspondência em relação a qualquer SSID.
Associação do tipo de interface	Um tipo de interface. Se especificada, essa regra corresponde apenas se o hardware da interface de rede principal corresponder ao tipo especificado. Selecione um dos tipos a seguir: • Ethernet • WiFi • Celular
Investigação da sequência da URL	Um URL para investigar. Se esse URL for coletado com êxito (retornar um código de status de HTTP 200) sem redirecionamento, essa regra é correspondida.

Para obter mais informações, consulte Como criar uma configuração.

Defensa contra ameaças

Aplicável a:

- Go para cliente iOS 3.2.0 ou versões mais recentes com suporte.
- Go para cliente Android 52 ou versões mais recentes com suporte.

O Ivanti Neurons for MDM inclui a capacidade de distribuir tokens de ativação para ativar a tecnologia de Defesa contra ameaças MobileIron integrada ao Go para clientes Android e iOS. A Defesa contra ameaças protege dispositivos gerenciados contra ameaças e vulnerabilidades móveis que afetam o dispositivo, a rede e os aplicativos.

Quando essa configuração é ativada no Ivanti Neurons for MDM e aplicada aos dispositivos, as bibliotecas da Defesa contra ameaças são ativadas nos clientes Go. O serviço de Defesa contra ameaças pode ser desativado removendo o token de licença e reenviando a configuração da licença ao cliente.

A Defesa contra ameaças monitora:

- No nível do dispositivo: parâmetros do sistema, configuração, firmware e bibliotecas para identificar atividade suspeita ou maliciosa.
- No nível da rede: tráfego de rede e conexões suspeitas para e a partir de dispositivos móveis.
- No nível do aplicativo: apps de vazamento (possivelmente colocando dados corporativos em risco) e apps maliciosos, por meio de avaliação de risco e análise de código.

Documentação mais recente

Para ver as instruções mais recentes da Defesa contra ameaças, consulte o *Guia da solução Defesa contra ameaças do Ivanti Neurons for MDM* da Comunidade de Suporte na documentação de produto do Ivanti Neurons for MDM.

É necessário ter as credenciais de suporte para acessar a documentação na Comunidade de suporte.

FileVault 2

Licença: Gold

O FileVault 2 oferece a capacidade de realizar a criptografia completa do disco XTS-AES 128 no conteúdo de um volume.

Ao ativar o FileVault 2, as seguintes configurações poderão ser realizadas:

Categoria	Ajustes

Configurações de usuário do FileVault	• Adiar a ativação do FileVault até que o usuário designado efetue logout
	  • Sempre solicitar ao usuário para ativar o FileVault
	  • Número máximo de vezes que um usuário pode ignorar a ativação do FileVault
	• Não solicitar a ativação do FileVault no momento do logout do usuário

Caminho de saída	Inserir o caminho do local onde a chave de recuperação e os plist de informações do computador serão armazenados.

Chave de recuperação pessoal	• Criar uma chave de recuperação pessoal
	• Exibir a chave de recuperação pessoal para o usuário após o FileVault ser ativado
	
	Esta opção fica visível apenas quando **Criar uma chave de recuperação pessoal** estiver ativada. A opção está desativada por padrão.
	
	• Ativar a chave de recuperação institucional: Uso de chaves: se não for fornecida nenhuma informação de certificado neste carregamento, a chave existente em /Library/Keychains/FileVaultMaster.keychain será usada.
	Selecione uma das opções a seguir:
	  • Fazer upload do certificado
	  • Certificado
	  • Usar chaves no Sistema dos usuários

Chave de recuperação do FileVault

Licença: Gold

A configuração da chave de recuperação FileVault determina o redirecionamento e o armazenamento em garantia das chaves de recuperação do FileVault em um servidor corporativo.

Excluir e enviar novamente por push da configuração Chave de recuperação do File Vault está desabilitado, pois um dispositivo macOS para de enviar chaves de recuperação ao reenviar por push a configuração.

É possível configurar as seguintes opções:

Configuração	Descrição
Nome	Insira um nome que identifique essa configuração.
Descrição	(Opcional) Insira uma descrição que esclareça o propósito dessa configuração.
Configurações para macOS < 10.13	
Armazenar chave de recuperação no locatário do Ivanti Neurons for MDM	Selecione para permitir que o Ivanti Neurons for MDM armazene as chaves no seu locatário. Quando necessário, a chave poderá ser descriptografada na página de detalhes do dispositivo.
Redirecionar URL ao servidor	Insira as configurações a seguir: • Insira o **URL de redirecionamento** para onde as chaves de recuperação FDE devem ser enviadas no lugar da Apple. A URL deve começar com https://. • Selecione um certificado na lista suspensa. Apenas certificados do formato PKCS1 podem ser usados.
Configurações para macOS 10.13+	
Localização	(Obrigatório) Insira uma breve descrição do local onde a chave de recuperação será guardada. Este texto será inserido na mensagem exibida ao usuário quando o FileVault é ativado.
Chave do dispositivo	(Opcional) Insira um texto a ser incluído no texto de ajuda se o usuário esquecer a senha.

Configuração Opções do FileVault

Essa configuração permite que o administrador habilite ou desabilite o FileVault e destrua a chave FileVault quando o sistema entrar em espera.

Aplicável para: macOS 10.7+

Procedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **FileVault** no campo de pesquisa e, em seguida, clique na configuração **Opções do FileVault**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Em Configuração, selecione as opções necessárias:
    - Destruir a chave FileVault quando o sistema entrar em modo de espera
    - Não permitir a desativação da criptografia total de disco
    - Não permitir a ativação da criptografia total de disco
5. Clique em **Avançar**.
6. Selecione a opção **Ativar esta configuração**.
7. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizado.
8. Clique em **Concluído**.

Certificado de identidade

Esta seção contém os seguintes tópicos:

- Configurações do certificado de identidade
- Distribuir configuração

Uma configuração do certificado de identidade define um mecanismo de autenticação de certificado para dispositivos móveis. Os certificados de identidade são certificados X.509 (.p12 ou .pfx). Além disso, os certificados de identidade podem ser gerados dinamicamente usando a Autoridade de certificação como fonte. Antes de começar, você já deve saber como planeja distribuir os certificados para seus dispositivos móveis. Você também já deve ter configurado qualquer autoridade de certificação necessária.

- Os certificados SHA-1 são preteridos durante a criação dos certificados de identidade. Você pode escolher outros algoritmos. Ao atualizar os certificados, se os certificados mais antigos usarem SHA-1, o mesmo algoritmo SHA-1 poderá ser utilizado. Se os certificados mais antigos usarem um algoritmo acima de SHA-1, a alteração para SHA-1 não é permitida.
- Depois de configurar um certificado de identidade, você pode clicar em **Testar configuração e continuar** para emitir e verificar a validade do certificado de teste. Pode ser exibido um erro ao executar esse teste para uma configuração de certificado de identidade gerada dinamicamente nova ou existente se o nome do assunto é igual à autoridade de certificação local. Quando essa mensagem de erro for exibida, você deve modificar o nome do assunto do certificado de identidade que deve ser diferente do nome do assunto da autoridade de certificação local. Para configurações de certificado de identidade existentes que são modificadas com o nome do assunto, os certificados são emitidos novamente e as configurações são enviadas novamente.
  Se estiver configurada a opção de criar uma configuração sem emitir um certificado de teste para a distribuição de certificado **Gerada dinamicamente**, clique em **Continuar**.
- Ao editar a configuração de um certificado de identidade existente (que é usado em um perfil do Sentry para Tunnel ou aplicativo Tunnel), no menu **Ações** será possível selecionar a opção **Limpar certificados em cache e emitir novos com atualizações recentes** se necessário. Os certificados que não estão armazenados em cache serão emitidos de novo automaticamente.

- Quando os certificados de identidade são atribuídos a apps Android, o aplicativo do usuário obtém Certificados de identidade sem confirmar com os usuários para conceder a permissão (ao invés do aplicativo) para usar o certificado. Isso inclui todos os apps como Email+, Gmail, etc.

- O Email+ pode ser configurado com um certificado de identidade fornecido pelo usuário, enviado por push e atribuído como uma configuração de aplicativo a dispositivos Android corporativo. Isso é aplicável apenas aos modos Perfil de trabalho em dispositivo de propriedade da empresa e Proprietário do dispositivo.

Configurações do certificado de identidade

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.

Configuração	O que fazer
Distribuição de certificados	Selecione o tipo de distribuição de certificado para configurar: • **Arquivo único**: Faça o upload de um certificado existente para distribuir aos dispositivos. • **Gerado dinamicamente**: Crie certificados mediante solicitação usando uma autoridade de certificação local ou externa. • **Fornecido pelo usuário:** Crie rótulos para o tipo de certificados a serem transferidos pelo usuário. Quando criados, o usuário poderá ver os rótulos criados (opções) no portal de autoatendimento e fazer upload de certificados que correspondem a esses rótulos. • **Credenciais derivadas:** especifique um dos seguintes usos da credencial derivada. ◦ Autenticação ◦ Criptografia ◦ Assinatura ◦ Descriptografia •

Configuração	O que fazer
	• **Configuração SCEP**: especifique como solicitar um certificado de um servidor SCEP. Selecione uma das configurações a seguir: ◦ Configuração de Aplicativo ◦ Configuração do Windows Sua seleção determina as opções que serão exibidas no resto do formulário.
Permitir que todos os apps acessem a chave privativa (macOS 10.10+)	**Aplicável a:** certificados de identidade de Arquivo único, Gerados dinamicamente, Fornecidos pelo usuário e de Configuração SCEP para Apple. (Opcional) Para certificados PKCS#12, ative a opção **Permitir que todos os apps acessem a chave privada** para permitir que todos os apps acessem a chave privada. Por exemplo, essa chave pode ser usada nos casos em que a senha é solicitada do usuário a fim de permitir acesso a um certificado utilizado para VPN.
Arquivo único	
Dados do Certificado de identidade	Arraste o arquivo de certificado até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo do seu sistema de arquivos.
Senha	Digite a senha que protege o arquivo de certificado PKCS#12. Esta senha é usada para instalação sem aviso.
Gerado dinamicamente	

Configuração	O que fazer
Origem	Selecione a autoridade de certificação local na lista suspensa. Você já deve ter criado essa CA em **Admin** > **Gerenciamento de certificados**.
Criar configuração sem emitir certificado de teste	Selecione a caixa de verificação para criar uma configuração sem emitir um certificado de teste.
Somente Windows – Armazenamento do certificado de destino	Os administradores agora podem selecionar o armazenamento do certificado de destino em dispositivos Windows.
Fornecido pelo usuário	
Nome de exibição do certificado	Insira o nome do certificado. Este nome de certificado é exclusivo para cada locatário, e o usuário poderá ver o nome no portal de autoatendimento ao fazer upload do certificado.
Excluir a chave privativa	Selecione esta opção para excluir a chave privativa do certificado após *n* (1 a 30) dias. Você também pode usar as APIs fornecidas pelo Ivanti Neurons for MDM para essas operações. Consulte o *Ivanti Neurons for MDM Guia de API* para mais informações sobre as APIs. Se você tentar usar este certificado em alguma configuração (por exemplo, para autenticar um aplicativo ou enviar uma configuração de Wi-Fi ou de VPN) após a exclusão da chave privativa, a tarefa falhará. Realize a tarefa antes da exclusão da chave privativa.
Excluir a chave privativa após dias	Selecione o número de dias (1 a 30) após o qual as chaves privativas do certificado são apagadas. O valor padrão é 2 dias.

Configuração	O que fazer
Credencial derivada	
Uso de credencial derivada	Selecione qualquer uma das opções a seguir: • **Autenticação** – Para especificar que a credencial derivada é utilizada para autenticação. • **Criptografia** – Para especificar que a credencial derivada é utilizada para criptografia. • **Assinatura** – Para especificar que a credencial derivada é utilizada para assinatura. • **Descriptografia** – para especificar que a credencial derivada é utilizada para descriptografia.
Marca	Dentre as opções a seguir, selecione o Fornecedor de credenciais derivadas que você utiliza: • **Entrust** • **Intercede** • **Purebred** Para adicionar os fornecedores de credenciais derivadas personalizados que você utiliza, consulte a seção **Fornecedores de credenciais derivadas**.
Configuração ACME - aplicável apenas a iOS/iPadOS16+	
Identificador do cliente	Uma string única que identifica um dispositivo específico

Configuração	O que fazer
URL do diretório	(Obrigatório) O URL do diretório do servidor ACME. O URL deve usar o esquema https.
Uso de chave estendida	O valor é uma matriz de strings. Cada string é um OID em notação pontilhada. Por exemplo, ["1.3.6.1.5.5.7.3.2", "1.3.6.1.5.5.7.3.4"] indica autenticação do cliente e proteção de e-mail. O dispositivo solicita esse campo para o certificado emitido pelo servidor ACME. O servidor ACME pode substituir ou ignorar este campo no certificado que emite.
Tamanho da chave	(Obrigatório) Os valores válidos para Tamanho da Chave dependem dos valores de Tipo da Chave e de Vinculado ao Hardware. Consulte essas chaves para verificar requisitos específicos.
Tipo da chave	(Obrigatório) O tipo de par de chaves a ser gerado.
Assunto	(Obrigatório) O dispositivo solicita esse assunto para o certificado emitido pelo servidor ACME. O servidor ACME pode substituir ou ignorar esse campo no certificado que emite. Nome X.500 representado como matriz de OID e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar corresponde a: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]] Os números pontilhados podem representar OIDs, com atalhos para país (C), localidade (L), estado (ST), organização (O), unidade organizacional (OU) e nome comum (CN). Tipo: [string]

Configuração	O que fazer
Nome alternativo do assunto	O nome alternativo de assunto que o dispositivo solicita para o certificado emitido pelo servidor ACME. O servidor ACME pode substituir ou ignorar este campo no certificado que emite.
Uso da chave	Este valor é um campo de bits. O bit 0x01 indica assinatura digital. O bit 0x10 indica acordo de chaves. O dispositivo solicita essa chave para o certificado emitido pelo servidor ACME. O servidor ACME pode substituir ou ignorar este campo no certificado que emite.
Vinculado ao hardware	Se Vinculado ao Hardware for definido como verdadeiro, a chave privada será vinculada ao dispositivo, e somente então o tipo de chave deverá ser ECSECPrimeRandom e o tamanho da chave deverá ser 256 ou 384.
Atestar	Se verdadeiro, o dispositivo fornece atestados descrevendo o dispositivo e a chave gerada ao servidor ACME. Quando Atestar é verdadeiro, Vinculado ao Hardware também deve ser verdadeiro.
Configuração SCEP - Configuração Apple	
Certificado de identidade (SCEP)	Selecione para especificar um servidor SCEP.
Autoridade de certificação local	Selecione para especificar uma autoridade de certificação local que você já criou em **Admin > Gerenciamento de certificados**. Selecione a autoridade de certificação local da lista suspensa, exibida ao selecionar essa opção.

Configuração	O que fazer
URL	Informe o URL do servidor SCEP.
Identificador da CA	Insira o identificador fornecido pela autoridade de certificação.
Assunto	Insira um nome X.500 representado na forma de uma matriz de OIDs e valores separados por vírgulas. Normalmente, o assunto é configurado como o nome de domínio qualificado completo do usuário. Por exemplo, C=US,DC=com,DC=MobileIron,OU=InfoTech ou CN=www.mobileiron.com. Você também pode personalizar o Assunto inserindo uma variável no OID. Por exemplo, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. Para facilitar a configuração, você também pode usar a variável $USER_DN$ para preencher o Assunto com o FQDN do usuário. Não use o caractere de barra invertida (\) no nome do assunto.
Tipo de nome alternativo do assunto	Selecione Nome RFC 822, Nome DNS, Identificador de Recursos Uniforme ou Nenhum, com base nos atributos do modelo de certificado.

Configuração	O que fazer
Valor do nome alternativo do assunto	Insira o valor do tipo correspondente. Se você digitar '$' como o primeiro caractere, uma lista suspensa será exibida com possíveis atributos LDAP e AAD personalizados. Selecione o atributo personalizado adequado na lista. Se o valor AAD for usado, haverá suporte apenas para 'onPremisesImmutableId'. Insira fn:base64tohex (${onPremisesImmutableId})
Nome da entidade NT	Insira um nome de assunto alternativo para o ambiente da Microsoft. Ele normalmente seria configurado para incluir o UPN do usuário (nome principal do usuário).
Desafio	(Opcional) Usado como um segredo pré-compartilhado para a inscrição automática.
Tentativas	Selecione da lista para configurar o número de tentativas de autenticação após a primeira vez que for retornado o status de "pendente".
Intervalo entre novas tentativas	Selecione da lista para definir o tempo de espera em segundos antes de uma nova tentativa.
Tamanho da chave	Selecione 1024, 2048 ou 4096 bits.
Usar como assinatura digital	Selecione se o certificado pode ser usado para assinatura.
Usar como codificação da chave	Selecione se o certificado pode ser usado para criptografia.

Configuração	O que fazer
Impressão digital da CA	Se a sua autoridade de certificação usar HTTP, insira a sequência hexadecimal que será utilizada como impressão digital do certificado da CA. As impressões digitais MD5 são suportadas. Se você preferir, crie uma impressão digital a partir do certificado. Arraste e solte o certificado na área designada ou clique em **Criar do Certificado** para selecionar o certificado do seu sistema de arquivos.
Configuração de SCEP – Configuração do Windows	
CA (Autoridade de certificação)	Selecione para especificar uma autoridade de certificação que você já criou em **Admin > Gerenciamento de certificados**. Selecione a autoridade de certificação na lista suspensa, exibida ao selecionar essa opção.
Assunto	Insira um nome X.500 representado na forma de uma matriz de OIDs e valores separados por vírgulas. Normalmente, o assunto é configurado como o nome de domínio qualificado completo do usuário. Por exemplo, C=US,DC=com,DC=MobileIron,OU=InfoTech ou CN=www.mobileiron.com. Você também pode personalizar o Assunto inserindo uma variável no OID. Por exemplo, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. Para facilitar a configuração, você também pode usar a variável $USER_DN$ para preencher o Assunto com o FQDN do usuário. Não use o caractere de barra invertida (\) no nome do assunto.

Configuração	O que fazer
Tipo de nome alternativo do assunto	Clique em **+ Adicionar** para selecionar Nome RFC 822, Nome DNS, Identificador de Recursos Uniforme ou Nenhum, com base nos atributos do modelo de certificado.
Tentativas	Selecione da lista para configurar o número de tentativas de autenticação após a primeira vez que for retornado o status de "pendente".
Intervalo entre novas tentativas	Selecione da lista para definir o tempo de espera em segundos antes de uma nova tentativa.
Tamanho da chave	Selecione o tamanho da chave como 1024, 2048 ou 4096 bits.
Selecione o uso	Selecione pelo menos uma opção: • Usar como assinatura digital – Selecione se o certificado pode ser usado para assinatura. • Usar como codificação da chave – Selecione se o certificado pode ser usado para criptografia.

Configuração	O que fazer
Validade	Selecione a validade em dias, meses ou anos.
Impressão digital da CA	Se a sua autoridade de certificação usar HTTP, insira a sequência hexadecimal que será utilizada como impressão digital do certificado da CA. As impressões digitais MD5 são suportadas. Se você preferir, crie uma impressão digital a partir do certificado. Arraste e solte o certificado na área designada ou clique em **Criar do Certificado** para selecionar o certificado do seu sistema de arquivos.
Família do algoritmo de hash	Selecione algoritmos SHA-2 ou SHA-3.

Ao aplicar um Certificado de identidade a um perfil de trabalho em um dispositivo sem definir uma senha de Desafio de trabalho (Work Challenge), o dispositivo solicita uma senha do dispositivo, em vez de uma senha de Desafio de trabalho (Work Challenge).

Distribuir configuração

A partir da versão 81 do Ivanti Neurons for MDM, os administradores globais poderão delegar administradores de espaço para editar o certificado de identidade gerado dinamicamente para todos os dispositivos e para a opção de distribuição personalizada. Para os certificados gerados dinamicamente, você pode selecionar a opção **Permitir que esta configuração esteja disponível em todos os espaços**. Esta opção disponibiliza o Certificado de identidade gerado dinamicamente para todos os Espaços e pode ser usada no Exchange, no Wi-Fi, em VPN e em qualquer outra configuração aplicável, incluindo as configurações gerenciadas de aplicativo. Essa opção pode ser usada em cenários nos quais o certificado de Identidade gerado dinamicamente precisa ser distribuído aos dispositivos (em Espaços que não sejam padrão) somente como parte de configurações associadas e não como uma configuração individual.

Procedimento

1. Especifique os campos das configurações do Certificado de Identidade usando as informações da tabela anterior.
2. Clique em **Avançar**.

3. Selecione a opção **Habilitar essa configuração**.
4. (Opcional) Selecione **Permitir que esta configuração esteja disponível em todos os espaços**.
5. Selecione uma das opções de distribuição a seguir:
    - **Todos os dispositivos**. Selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.
    - **Nenhum dispositivo** (padrão)
    - **Personalizado** Selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.

    Independentemente dos espaços, o Certificado de identidade gerado dinamicamente pode ser configurado em todos os espaços, distribuído a todos os dispositivos e aplicado a todos os dispositivos em outros espaços do dispositivo.
6. Clique em **Concluído** .

Configuração do Bloqueio de ativação da Apple

Licença: Silver

Esta seção contém os seguintes tópicos:

- Habilitação da Trava de ativação do iOS
- Habilite o recurso de Trava de ativação do iOS em dispositivos supervisionados
- Habilitação da Trava de ativação do macOS
- Habilite o recurso de Trava de ativação do macOS em dispositivos supervisionados
- Uso do código de bypass da Trava de ativação do iOS
- Como apagar do código de bypass da Trava de ativação do iOS

O Bloqueio de Ativação é um recurso da Apple projetado para impedir que alguém utilize um dispositivo perdido ou roubado. Assim que o Find My é ativado, um mapeamento entre a conta da iCloud e um identificador de hardware para esses dispositivos é salvo nos servidores de ativação da Apple. A partir desse momento, ninguém pode desativar o Find My, apagar o dispositivo ou reativá-lo sem inserir o ID da Apple e a senha existentes. Se alguém diferente do usuário limpar o dispositivo e depois tentar reativá-lo e usá-lo, será solicitado a ID Apple e a senha no Assistente de Configuração.

A desativação do bloqueio de ativação não desativará o recurso em dispositivos supervisionados se o usuário final tiver habilitado o Buscar meu dispositivo. O Assistente de configuração solicitará que o usuário execute uma ação quando o dispositivo for reiniciado ou apagado remotamente.

O Bloqueio de Ativação oferece aos administradores mais opções para impedir o roubo de dispositivos supervisionados. No entanto, é provável que a maioria dos administradores corporativos deixem o Bloqueio de Ativação desabilitado pois ele é, primordialmente, um recurso para clientes. A tabela a seguir resume as opções para implementações corporativas confiáveis:

Tipo de dispositivo	Resultado
Confiança corporativa e dispositivos supervisionados	• O Bloqueio de Ativação é desabilitado para dispositivos supervisionados por padrão. • Os usuários dos dispositivos não podem ativar o Bloqueio de Ativação.
Confiança corporativa e dispositivos não supervisionados	• O Bloqueio de Ativação é habilitado assim que o usuário final faz login na iCloud com sua ID Apple e ativa o Find My Device. • Os servidores MDM, incluindo o Ivanti Neurons for MDM, não conseguem controlar o Bloqueio de ativação em dispositivos não supervisionados. Usuários de dispositivos podem bloquear a ativação com suas credenciais pessoais, deixando você sem recursos caso eles saiam da empresa.

Habilitação da Trava de ativação do iOS

Aplicável para: iOS 7+ supervisionado

Essa configuração será aplicada a dispositivos supervisionados (iOS 7 e posteriores) que tenham o recurso Find My ativado. Caso um administrador ou outro usuário tente apagar, ativar ou desabilitar o recurso Buscar meu dispositivo no dispositivo, uma tela do Bloqueio de Ativação da Apple será exibida. Para prosseguir, digite as credenciais do iTunes ou um código de bypass.

O código de bypass para dispositivos supervisionados será armazenado na ocorrência da ativação e pode ser visualizado nas informações do dispositivo. O código de bypass pode ser enviado remotamente utilizando o comando "Remover o Bloqueio de ativação" para dispositivos supervisionados. No entanto, o código deve ser digitado manualmente quando um dispositivo for reativado ou quando o recurso Buscar meu dispositivo for desligado.

Você só pode criar uma configuração do Bloqueio de ativação para todos os espaços.

Habilite o recurso de Trava de ativação do iOS em dispositivos supervisionados

Procedimento

1. Ative o recurso **Find My** no seu dispositivo.
2. Vá até **Configurações**.
3. Selecione a configuração **Bloqueio de ativação da Apple** na lista de configurações existentes.
4. Clique em **Editar**.
5. Na seção iOS 7+ supervisionado, clique em **Ativar bloqueio de ativação**.
6. Clique em **Concluído**.
7. Registre o dispositivo.

Habilitação da Trava de ativação do macOS

Aplicável para: macOS 10.15+ supervisionado

Essa configuração será aplicada aos dispositivos supervisionados com macOS 10.15 e posteriores. O bloqueio de ativação no macOS apenas é aplicável para Macs com o chip de segurança T2 da Apple. Em dispositivos supervisionados, sejam eles atualizados ou instalados recentemente, e em dispositivos registrados atualmente atualizados, o bloqueio de ativação está desabilitado por padrão. Habilitar o Encontrar meu não ativa automaticamente o Bloqueio de ativação nesses dispositivos

Caso um administrador ou outro usuário tente apagar, ativar ou desabilitar o recurso Find My no dispositivo, uma tela do Bloqueio de ativação da Apple será exibida. Para prosseguir, digite as credenciais do iTunes ou um código de bypass. O código de bypass para dispositivos supervisionados será armazenado na ocorrência da ativação e pode ser visualizado nas informações do dispositivo. O código de bypass pode ser enviado remotamente utilizando o comando "Remover o Bloqueio de ativação" para dispositivos supervisionados. No entanto, o código deve ser digitado manualmente quando um dispositivo for reativado ou quando o recurso Find My for desligado.

Você só pode criar uma configuração do Bloqueio de ativação para todos os espaços.

Habilite o recurso de Trava de ativação do macOS em dispositivos supervisionados

Procedimento

1. Ative o recurso Find My no seu dispositivo.
2. Vá até **Configurações**.
3. Selecione a configuração **Bloqueio de ativação da Apple** na lista de configurações existentes.

4. Clique em **Editar**.
5. Na seção macOS 10.15+ supervisionado, clique em **Ativar Bloqueio de ativação**.
6. Clique em **Concluído**.
7. Registre o dispositivo.

Uso do código de bypass da Trava de ativação do iOS

Quando o dispositivo é apagado com o bloqueio de ativação do iOS ativado, o código de bypass é retido no servidor de ativação da Apple e na interface administrativa do Ivanti Neurons for MDM.

Procedimento

1. Acesse **Dispositivos**.
2. Selecione o dispositivo.
3. Clique em **Ações > Apagar**. Pode levar alguns minutos até que o dispositivo reinicie.
4. Quando o dispositivo solicitar o Apple ID e a senha, deixe o **Apple ID** vazio.
5. Insira o código bypass no campo da **senha**.
6. Clique em **Avançar**.
7. Continue a configuração.

Como apagar do código de bypass da Trava de ativação do iOS

Quando o bloqueio de ativação do iOS é desmarcado na interface administrativa do Ivanti Neurons for MDM, o código de bypass é removido do servidor de ativação da Apple, mas permanece nas informações do dispositivo na interface administrativa do Ivanti Neurons for MDM.

Procedimento

1. Acesse **Dispositivos**.
2. Selecione o dispositivo.
3. Selecione **Configurações**.
4. Selecione **Bloqueio de ativação da Apple**.
5. Clique em **Editar**.

6. Na seção iOS 7+ supervisionado, desative a opção **Ativar Bloqueio de ativação**.
7. Clique em **Concluído**.
8. Acesse **Dispositivos**.
9. Selecione o dispositivo.
10. Clique em **Ações > Apagar**. Pode levar alguns minutos até que o dispositivo reinicie. O dispositivo pode ser configurado com o novo ID da Apple e senha do usuário.
11. Continue a configuração.

O status de liberar trava de ativação do iOS é exibido na interface da seguinte maneira:

Estado	**Resultado**
Pendente	• O servidor está enviando o código de liberar trava de ativação para a Apple.
Enviado	• A Apple acusou o recebimento do código de liberar trava de ativação.
Falha	• O servidor não conseguiu enviar o código à Apple. • A Apple relatou um erro.

Configuração personalizada do iOS

Uma configuração personalizada do iOS permite que você faça o upload e distribua um perfil de configuração do iOS criado por outro aplicativo, como um utilitário de configuração do iPhone da Apple.

Configurações personalizadas do iOS

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Dados do arquivo	Arraste e solte o arquivo de configuração ou clique em **Escolher arquivo** para selecioná-lo do seu sistema de arquivos.

Para obter mais informações, consulte Como criar uma configuração.

Restrições do iOS

As restrições do iOS são configurações que ajudam o usuário primário do dispositivo a controlar o que os outros usuários têm permissão de fazer com um dispositivo iOS. Essas configurações são definidas pela Apple e gerenciadas pelo Ivanti Neurons for MDM.

Durante a distribuição dessa configuração para iPads compartilhados, é possível selecionar o Canal do dispositivo ou o Canal do usuário. Isso é útil para distribuir configurações separadas e aplicar restrições que sejam aplicáveis apenas ao canal do dispositivo ou do usuário.

Configurações de restrições do iOS

Categoria	Configuração	O que fazer
	Nome	Insira um nome que identifique essa configuração.
	Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Funcionalidade do dispositivo	**Todas as versões do iOS**	**Ativar uso dos recursos do dispositivo.**
	Permitir capturas de tela e gravação da tela	Selecione para permitir que o usuário do dispositivo faça capturas de tela usando o recurso de captura de tela do iOS integrado.
	Permitir observação remota da tela (iOS 9.3 e posterior)	Selecione para permitir que o usuário observe a tela remota.
	Permitir observação de tela gerenciada não solicitada na sala de aula gerenciada (somente supervisionado - iOS 10.3 ou superior)	(Aplicável apenas a iPads) Selecione para permitir que uma mensagem não solicitada apareça na tela quando um iPad supervisionado for configurado com classes gerenciadas.
	Permitir sincronização automática durante roaming	Selecione para permitir a sincronização de contas de e-mail enquanto o dispositivo estiver fora do país de origem.

Categoria	Configuração	O que fazer
	Permitir Siri	Selecione para permitir o aplicativo do assistente pessoal nos dispositivos suportados.
	Permitir Siri enquanto dispositivo está travado	Selecione para permitir que o aplicativo do assistente pessoal execute tarefas quando o dispositivo estiver bloqueado.
	Ativar filtro de linguagem da Siri (apenas supervisionado)	Selecione para ativar o filtro de linguagem da Siri.
	Permitir discagem por voz	Selecione para permitir que os usuários disquem um contato ou número falando para o dispositivo.
	Permitir compra dentro do aplicativo	Selecione para permitir que os usuários façam compras através de apps executados no dispositivo.
	Permitir passbook enquanto dispositivo está travado	Selecione para permitir que as notificações do Passbook sejam exibidas enquanto o dispositivo estiver bloqueado.
	Permitir Central de Controle na tela de bloqueio	Selecione para permitir o acesso à Central de Controle da tela de bloqueio.
	Permitir visualização das Notificações na tela de bloqueio	Selecione para permitir que as notificações sejam exibidas na tela de bloqueio.
	Permitir Visualização para Hoje na tela de bloqueio	Selecione para permitir o acesso à visualização de Hoje na tela de bloqueio.
	Permitir opção Abrir em de apps gerenciados e não gerenciados	**Exige licença Gold**.

Categoria	Configuração	O que fazer
		Selecione para permitir que documentos em apps não gerenciados e contas sejam abertos em contas e apps gerenciados. Desabilitar essa opção impede a troca de documentos de apps e contas gerenciados com apps e contas não gerenciados. Por exemplo, você pode querer que os documentos corporativos não sejam abertos em apps pessoais. Você também pode utilizar esta opção (desativar) junto com uma configuração de domínio gerenciado para assegurar que os dados transferidos de domínios gerenciados possam ser abertos apenas em aplicativos gerenciados.
	Permitir opção Abrir em de apps não gerenciados em apps gerenciados	**Exige licença Gold**. Selecione para permitir que documentos em apps não gerenciados e contas sejam abertos em contas e apps gerenciados. Desabilitar essa opção impede a troca de documentos de não gerenciados com apps e contas gerenciados. Por exemplo, você pode querer impedir os usuários de enviar documentos pessoais usando o e-mail da empresa. Você também pode utilizar esta opção (desativar) junto com uma configuração de domínio gerenciado para assegurar que os dados transferidos de domínios não gerenciados possam ser abertos apenas em aplicativos gerenciados.
	Solicitar senha no primeiro emparelhamento do AirPlay	Selecione para solicitar que a Apple TV exiba uma senha que o usuário deve inserir no dispositivo iOS para autorizar o pareamento inicial dos dispositivos.

Categoria	Configuração	O que fazer
	Forçar senha em solicitações de AirPlay recebidas (tvOS até 10.1)	Selecione para exigir que o usuário insira a senha para todas as solicitações recebidas do AirPlay. Padrão: desmarcado
	Todas as versões do iOS supervisionadas	
	Permitir Apple Books	Selecione para permitir o acesso ao aplicativo Apple Books.
	Permitir conteúdo sexual explícito na iBooks Store (iOS e tvOS 11.3 e posterior)	Selecione para permitir que os usuários façam o download de materiais da iBookstore classificados como eróticos.
	Permitir modificação da conta	Selecione para permitir que os usuários com dispositivos iOS 7 supervisionados adicionem contas de e-mail e façam alterações nas contas de e-mail que já foram configuradas.
	Permitir modificação dos dados de celular do aplicativo	Selecione para permitir que os usuários façam alterações nas configurações dos dados do celular para apps.
	Permitir modificação do Find My Friends	Selecione para permitir que os usuários façam alterações nas configurações do aplicativo Find My Friends.

Categoria	Configuração	O que fazer
	Permitir pareamento com hosts que não são Configurator	Selecione para permitir o emparelhamento com host para a sincronização do iTunes. Na verdade, habilitar essa opção permite que os dispositivos supervisionados sejam sincronizados com o iTunes em um Mac, diferente do host de supervisão. Desabilitar essa opção faz com que todos os emparelhamentos com host sejam desabilitados, com exceção do host de supervisão. Se não foi configurado nenhum certificado de host de supervisão, todos os emparelhamentos serão desabilitados.
	Permitir AirDrop	Selecione para permitir o uso do AirDrop no dispositivo. O AirDrop é o sistema Wi-Fi ad hoc da Apple que habilita o compartilhamento de arquivos com os usuários próximos. Ao restringir esse recurso, você garante que documentos confidenciais não vazem para dispositivos não autorizados ou não protegidos.
	Permitir que o Touch ID / Face ID desbloqueie o dispositivo	Selecione para permitir o uso do Touch ID ou do Face ID para desbloquear os dispositivos.
	Permitir que a pesquisa do Spotlight retorne resultados de pesquisa da Internet	Selecione para permitir que a pesquisa do Spotlight retorne resultados de pesquisa da Internet.

Categoria	Configuração	O que fazer
	Permitir aplicativo no modo de aplicativo único	Insira uma lista separada por vírgulas de IDs de pacote para aplicativos que podem entrar de forma autônoma no modo de aplicativo único em dispositivos iOS supervisionados. Por exemplo, você pode especificar apps de exames personalizados para alunos. Quando o aluno iniciar o aplicativo, ele entrará no modo de Single-App para garantir que o aluno não use outros recursos ao prestar a prova. Esse recurso é aplicado em apps desenvolvidos para o modo de Single-App autônomo. A supervisão é estabelecida com o Apple Configurator.
	iOS 8 ou superior	
	Permitir o backup dos livros corporativos	Selecione para permitir backup pessoal de iBooks, ePub e documentos em PDF que foram baixados ao dispositivo por meio do MDM.
	Permitir a sincronização das anotações e destaques dos livros corporativos	Selecione para permitir que anotações e destaques sejam adicionados a livros corporativos para serem sincronizados ao iTunes.
	Forçar detecção de pulso do Apple Watch	Selecione para ocultar notificações na tela a menos que alguém esteja usando o Apple Watch.
	iOS 8+ supervisionado	
	Permitir teclado preditivo	Selecione para permitir que os usuários ativem a previsão do iOS da palavra que está sendo digitada, permitindo que os usuários toquem em uma das três previsões para completar a palavra.

Categoria	Configuração	O que fazer
	Permitir correção automática do teclado	Selecione para permitir o uso da correção automática com teclados Bluetooth.
	Permitir corretor ortográfico do teclado	Selecione para permitir o uso do corretor ortográfico com teclados Bluetooth.
	Permitir pesquisa de definição do teclado	Selecione para permitir a pesquisa de definição com teclados Bluetooth.
	Permitir a modificação das digitais do Touch ID / rostos do Face ID	Selecione para permitir que as configurações do Touch ID e do Face ID sejam alteradas.
	iOS 9+ Supervisionado	
	Permitir atalhos do teclado em iPads	Selecione para permitir o uso de atalhos no teclado do iPad.
	Permitir modificação do papel de parede	Selecione para permitir que o usuário troque as imagens do papel de parede.
	Permitir pareamento com o Apple Watch	Selecione para permitir pareamento do iPhone com o Apple Watch.
	Permitir modificação de nome do dispositivo	Selecione para permitir que o usuário modifique o nome do dispositivo.
	Permitir modificação da configuração de confiança do aplicativo corporativo	Selecione para permitir que o usuário altere as configurações de confiança do aplicativo corporativo.
	iOS 9.3+ supervisionado	
	Permitir modificações das configurações de notificações	Selecione para permitir que o usuário altere as configurações de notificação.
	iOS 9.3.2+ supervisionado	

Categoria	Configuração	O que fazer
	Permitir modificação de envio de diagnóstico	Selecione para permitir que o usuário altere as configurações relacionadas ao envio de dados de diagnóstico para a Apple.
	iOS 10+ Supervisionado	
	Permitir a modificação de Bluetooth	Selecione para permitir que o usuário modifique a configuração do Bluetooth em dispositivos supervisionados. Isso é útil para iPads compartilhados com o aplicativo Classroom para Educação que necessitam do Bluetooth para executar o aplicativo.
	iOS 10.3 ou superior supervisionado	
	Permitir ditado	Selecione para permitir que o usuário fale com o iPhone ou iPad em vez de digitar.
	iOS 11 ou superior supervisionado	
	Permitir AirPrint	Selecione para permitir o recurso AirPrint para impressão sem fio.
	Permitir armazenamento de credenciais no AirPrint	Selecione para permitir armazenar no Keychain o nome de usuário e a senha do AirPrint.
	Permitir descoberta de iBeacon no AirPrint	Selecione para permitir que o usuário configure a descoberta por iBeacon de impressoras AirPrint.
	Permitir a inclusão de configurações de VPN	Selecione para permitir que o usuário crie configuração de VPN
	Forçar requisito de TLS confiável de AirPrint	Selecione para permitir certificados confiáveis para comunicação de impressão TLS. Padrão: desmarcado

Categoria	Configuração	O que fazer
	Permitir remoção do aplicativo do sistema	Selecione para permitir a remoção do aplicativo do sistema.
	Permitir a modificação de configurações de plano celular	Selecione para permitir que os usuários modifiquem configurações de plano celular.
	Permitir a configuração de dispositivos próximos	Selecione para permitir que os usuários configurem novos dispositivos próximos.
	Entrar automaticamente em salas do Classroom sem aviso	Selecione para permitir que os usuários entrem automaticamente em salas do Classroom sem aviso. Padrão: desmarcado
	Permitir que o Classroom bloqueie um aplicativo e o dispositivo sem aviso	Selecione para permitir que o Classroom bloqueie um aplicativo e o dispositivo sem avisar o usuário. Padrão: desmarcado
	Forçar o usuário a se autenticar antes que senhas ou informações de cartão de crédito possam ser preenchidas automaticamente no Safari e nos aplicativos	O proprietário do dispositivo deve se autenticar antes que as senhas ou as informações de cartão de crédito possam ser preenchidas automaticamente no navegador Safari e nos aplicativos. Padrão: falso
	iOS 11.3+	
	Permitir emparelhamento com aplicativo remoto (tvOS 11.3 e posterior)	Selecione para permitir emparelhamento do dispositivo com o aplicativo Remoto.
	Permitir solicitações de AirPlay recebidas	Selecione para permitir o recebimento de solicitações do AirPlay.

Categoria	Configuração	O que fazer
	(tvOS 11.3 e posterior)	
	iOS 11.3+ supervisionado	
	Permitir modo restrito USB	Selecione para permitir que o usuário acesse o modo USB restrito.
	Adie atualizações de software por 30 dias (para iOS 11.3, tvOS 12.2 e posteriores apenas para dispositivos supervisionados)	Selecione para inserir o número de dias que você deseja adiar as atualizações de software. O padrão é 30 dias e o máximo 90 dias. Padrão: desmarcado
	Solicitar permissão do professor para sair de salas não gerenciadas do Classroom	Selecione para permitir que o usuário obtenha a permissão de professor necessária para sair das salas não gerenciadas do Classroom.
	iOS 12+ Supervisionado	
	Forçar data e hora automáticas (iOS 12.0, tvOS 12.2 e posterior)	Selecione para ativar o recurso de "Definir automaticamente" para Data e hora. Ele não pode ser desativado pelo usuário. Padrão: falso
	Permitir a modificação de configurações de eSIM (iPhone XS, iPhone XS Max e iPhone XR – iOS 12.1 e versões posteriores)	Selecione para permitir que o usuário modifique a configuração de eSim em dispositivos compatíveis. Esta opção também impede que usuários adicionem ou removam um plano de celular em Configurações nos dispositivos. Padrão: Verdadeiro
	iOS 12.2+ supervisionado	

Categoria	Configuração	O que fazer
	Permitir a modificação de configurações de Hotspot pessoal	Selecione para permitir que o usuário modifique as configurações de Hotspot pessoal. Padrão: Verdadeiro
	iOS 13.0+	
	Permitir que Files acesse a unidade da rede	Selecione para permitir que o usuário se conecte aos drives de rede no aplicativo Files. Padrão: Verdadeiro
	Permitir que Files acesse a unidade USB	Selecione para permitir que o usuário se conecte a quaisquer dispositivos USB conectados no aplicativo Files. Padrão: Verdadeiro
	iOS 13.0+ supervisionado	
	Permitir o caminho contínuo do teclado	Selecione para ativar o teclado de caminho contínuo (digitação de toque ou traço). Padrão: Verdadeiro
	Permitir suspensão do dispositivo	Selecione para ativar a suspensão do dispositivo. Padrão: Verdadeiro
	Permitir localizar dispositivo	Selecione para ativar Localizar meu dispositivo no aplicativo de localização. Padrão: Verdadeiro
	Permitir Find My Friend	Selecione para ativar Localizar meus amigos no aplicativo de localização. Padrão: Verdadeiro

Categoria	Configuração	O que fazer
	Forçar ativação do Wi-Fi	Selecione para ativar a energia do Wi-Fi no estado ligado. Padrão: falso
	iOS 13.4+	
	Permitir Sessão de convidado para iPad compartilhado	Se o valor for falso, as sessões temporárias não estarão disponíveis no iPad compartilhado. Padrão: Verdadeiro
	iOS 14.0+	
	Permitir publicidade personalizada da Apple	Se a condição for falsa, a publicidade personalizada da Apple é limitada. Esta restrição impede que a Apple utilize informações do usuário para segmentar anúncios. Isso pode reduzir o número de anúncios recebidos, mas os anúncios serão menos relevantes para o usuário. Padrão: Verdadeiro
	iOS 14.0+ Supervisionado	
	Permitir App Clips	Se o valor for falso, o usuário não poderá adicionar nenhum App Clip, e todos os App Clips existentes no dispositivo serão removidos. Padrão: Verdadeiro
	iOS 14.2+ supervisionado	
	Permitir NFC	Se falso, desative o NFC. Requer um dispositivo supervisionado. Disponível no iOS 14.2 e posterior.

Categoria	Configuração	O que fazer
		Padrão: Verdadeiro
	iOS 14.5+	
	Permitir desbloqueio automático	Os administradores podem usar a restrição allowAutoUnlock existente para gerenciar este recurso. Se falso, desativa o bloqueio automático. Disponível no macOS 10.12 e posterior, e no iOS 14.5 e posterior. Padrão: verdadeiro
	Forçar apenas ditado no dispositivo	Se verdadeiro, desativa as conexões aos servidores Siri para fins de ditado. Padrão: falso
	iOS 14.5+ supervisionado	
	Permitir a recuperação de boot externo desemparelhado	Se verdadeiro, permite que os dispositivos sejam inicializados para recuperação por um dispositivo desemparelhado. Padrão: falso
	Forçar Wi-Fi somente para redes autorizadas	Se verdadeiro, limita o dispositivo a entrar somente em configurações de redes Wi-Fi por meio do perfil de configuração. Padrão: falso Se a restrição **Forçar Wi-Fi somente para redes autorizadas** estiver ativada e a configuração Wi-Fi não for distribuída para o dispositivo, a conexão Wi-Fi será perdida.
	iOS 15+	

Categoria	Configuração	O que fazer
	Forçar apenas tradução no dispositivo	Se verdadeiro, o dispositivo não se conectará aos servidores Siri para fins de tradução. Padrão: falso
	Solicitar pasta gerenciada	Se verdadeiro, a funcionalidade de copiar e colar respeita as restrições `allowOpenFromManagedToUnmanaged` e `allowOpenFromUnmanagedToManaged`. Padrão: falso
	iOS 15.2+	
	Permitir proteção de privacidade de e-mail	Se falso, desativa a proteção de privacidade de e-mail no dispositivo. Disponível em iOS 15.2 e posteriores. Quando a configuração Permitir Proteção de Privacidade de E-Mail é instalada e habilitada no portal administrativo do Ivanti Neurons for MDM, a botão Proteger Atividade de E-Mail fica habilitado no dispositivo, e as seguintes opções ficam visíveis: • **Ocultar endereço IP** - o remetente do e-mail não pode vincular o e-mail à sua atividade on-line ou determinar sua localização • **Bloquear todo o conteúdo remoto** - impede que o remetente do e-mail veja suas atividades de e-mail Padrão: verdadeiro
	iOS 15.4+	

Categoria	Configuração	O que fazer
	Permitir proteção de tela automática da Apple TV (tvOS 15.4 e posteriores)	Se falso, desativa o protetor de tela automático da Apple TV. Disponível em tvOS 15.4 e posteriores. Padrão: verdadeiro
	iOS 16.0+	
	Permitir instalação do Rapid Security Response	Para desabilitar as respostas. O usuário não pode instalar respostas de segurança rápidas.
	Permitir remoção do Rapid Security Response	Para impedir que o usuário possa desfazer as respostas. O usuário não pode remover respostas de segurança rápidas.
Aplicativos	**Todas as versões do iOS**	Permitir acesso aos aplicativos nos dispositivos.
	Permitir instalação de apps	Selecione para permitir que o usuário instale aplicativos da Apple App Store. Desmarque para desabilitar a App Store e remover seu ícone da tela inicial.
	Uso total da câmera	Selecione para permitir que o usuário opere a câmera. Desmarque para desabilitar a câmera e remover seu ícone da tela inicial.
	Permitir uso do Safari	Selecione para permitir o uso do navegador Safari. Desmarque para desabilitar o navegador Safari, remover seu ícone da tela inicial e impedir que os usuários abram Web Clips.
	Habilitar preenchimento automático	Selecione para ativar o recurso de preenchimento automático para campos exibidos no Safari.

Categoria	Configuração	O que fazer
	Forçar aviso de fraude	Selecione para solicitar que o Safari tente impedir que o usuário acesse sites identificados como fraudulentos ou comprometidos.
	Habilitar JavaScript	Selecione para ativar o suporte do JavaScript para o Safari.
	Bloquear pop-ups	Selecione para bloquear pop-ups para o Safari.
	Todas as versões do iOS supervisionadas	
	Permitir remoção de apps	Selecione para permitir que usuários removam aplicativos do dispositivo.
	Permitir uso do Game Center	Selecione para permitir o acesso ao Game Center.
	Permitir adição de amigos do Game Center	Selecione para permitir que os usuários adicionem amigos ao Game Center.
	Permitir jogos com vários jogadores	Selecione para permitir que os usuários utilizem jogos que incluam outros usuários.
	Permitir iMessage	Selecione para permitir o uso do iMessage.
	Aceitar cookies	Selecione Nunca, Sempre ou De sites visitados.
	Permitir FaceTime	Selecione para permitir que o usuário execute o FaceTime se a câmera estiver habilitada.
	iOS 8 ou superior	

Categoria	Configuração	O que fazer
	Permitir que os aplicativos gerenciados usem a sincronização de cloud	Selecione para permitir que os aplicativos gerenciados usem a sincronização de cloud.
	Permitir continuação da atividade	Selecione para permitir continuação da atividade em aplicativos que suportam Handoff.
	iOS 8+ supervisionado	
	Permitir uso de podcasts	Selecione para permitir o uso de podcasts.
	iOS 9+	
	Permitir a confiança em novos autores de aplicativo corporativo	Selecione permitir acesso do usuário aos novos apps corporativos.
	iOS 9+ Supervisionado	
	Permitir App Store	Selecione para permitir que o usuário acesse a Apple App Store.
	Permitir download automático de aplicativo	Selecione para permitir que o aplicativo baixe arquivos, dados e atualizações com alertas para o usuário.
	Permitir novos aplicativos	Selecione para permitir o uso do aplicativo Notícias.
	iOS 9.3+ supervisionado	
	Permitir o iTunes Radio	Selecione para permitir o uso do rádio do iTunes.
	Permitir Apple Music	Selecione para permitir o uso do Apple Music.

Categoria	Configuração	O que fazer
	Permitir IDs do pacote de aplicativo listados	Selecione para permitir que apenas IDs do pacote listados na matriz sejam exibidos ou executáveis. Inclua o valor com.apple.webapp para permitir todos os webclips.
	Bloquear IDs do pacote de aplicativo	Selecione para evitar que IDs do pacote listados na matriz sejam exibidos ou executáveis. Inclua o valor com.apple.webapp para restringir todos os webclips.
	iOS 13.0+ supervisionado	
	Permitir uso da iTunes Store	Selecione para permitir o uso da iTunes Store. Desmarque para desabilitar a iTunes Music store e remover seu ícone da tela inicial.

Categoria	Configuração	O que fazer
iCloud	**Todas as versões do iOS**	Ativar acesso aos serviços do iCloud.
	Permitir backup	Selecione para permitir que o dispositivo faça o backup de dados através do serviço iCloud da Apple.
	Permitir sincronização de documentos	Selecione para permitir que os documentos sejam sincronizados através do serviço iCloud da Apple.
	Permitir compartilhamento de fotos	Selecione para permitir que as fotos sejam sincronizadas com outros dispositivos iOS através do iCloud da Apple.
	Permitir fluxos de foto compartilhados (proibir pode causar perda de dados)	Selecione para permitir a sincronização de fotos compartilhadas. Desmarcar essa opção poderá resultar na perda de fotos.
	Permitir sincronização do conjunto de chaves	Selecione para permitir a sincronização do seu conjunto de chaves.
	iOS 9+	
	Permitir Biblioteca de fotos do iCloud	Selecione para permitir acesso à biblioteca de fotos do iCloud.
	iOS 15+ supervisionado	
	Permitir retransmissão privada do cloud	Se falso, desativa a retransmissão privada do iCloud. Padrão: verdadeiro

Categoria	Configuração	O que fazer
Segurança e privacidade	**Todas as versões do iOS**	Ativar segurança e políticas de privacidade.
	Permitir atualizações de certificados no modo Over the air	Selecione para permitir atualizações Over-The-Air de certificados de raiz.
	Forçar limite e controle	Selecione para solicitar o uso do recurso de limite e controle.
	Todas as versões do iOS supervisionadas	
	Permitir instalação de perfil de configuração	Selecione para permitir que os usuários instalem certificados e perfis de configuração de forma interativa.
	Permitir conteúdo gerado por usuário auxiliar	Selecione para permitir que o Siri consulte conteúdo gerado pelo usuário da web.
	iOS 8+ supervisionado	
	Permitir que o usuário apague todo o conteúdo e configuração na UI Redefinir	Selecione para habilitar a opção "Apagar todos os Conteúdos e Configurações" na IU Reiniciar iOS no dispositivo.
	Permitir tempo de tela	Selecione para permitir tempo de tela (Configurações > Tempo de tela).
	Permitir envio de dados de diagnóstico para a Apple	Selecione para permitir o envio automático de dados de diagnóstico para a Apple.

Categoria	Configuração	O que fazer
	Permitir que usuário aceite certificados TLS não confiáveis	Selecione para permitir que o usuário do dispositivo aceite certificados HTTPS não confiáveis. Se essa opção não estiver selecionada, o dispositivo irá rejeitar automaticamente certificados HTTPS não confiáveis sem solicitar ao usuário do dispositivo.
	Forçar backups criptografados	Selecione para solicitar backups criptografados através do iTunes. Selecionado automaticamente devido aos requisitos de SCEP.
	Forçar usuário a inserir senha da iTunes Store em todas as transações	Selecione para forçar os usuários do dispositivo a inserir a senha do iTunes para cada transação da App Store. Se essa opção não estiver selecionada, o usuário do dispositivo poderá fazer várias transações em uma única autenticação.
	iOS 9+	
	Tratar AirDrop como destino não gerenciado	Selecione para permitir que o usuário acesse o compartilhamento de arquivos do AirDrop. Padrão: falso
	iOS 9+ Supervisionado	
	Permitir modificação de senha do dispositivo	Selecione para permitir que o usuário troque a senha do dispositivo.
	iOS 12+	
	Permitir que apps gerenciados gravem contatos em contas de contato não gerenciadas	Selecione para permitir que apps gerenciados gravem contatos em contas de contato não gerenciadas. Padrão: falso

Categoria	Configuração	O que fazer
	iOS 12+ Supervisionado	
	Permitir preenchimento automático de senhas	Selecione para permitir aos usuários utilizar o recurso Preenchimento automático de senha no iOS e ser solicitado a usar uma senha salva no Safari ou em apps.
	Permitir que dispositivos próximos compartilhem solicitações para uma senha	Selecione para permitir que o dispositivo do usuário solicite senhas de dispositivos nas proximidades.
	Permitir compartilhamento de senha	Selecione para permitir que os usuários compartilhem as senhas com o recurso Senhas do AirDrop.
	Permitir que apps não gerenciados leiam contatos de contas de contato gerenciadas	Selecione permitir que apps não gerenciados leiam de contas de contato gerenciadas. Padrão: falso

Categoria	Configuração	O que fazer
Classificações de conteúdo		Controlar acesso aos apps e às mídias.
	Permitir reprodução de músicas, podcasts e mídia do iTunes U explícitos (somente iOS 13+ supervisionado e tvOS 11.3 e posterior)	O conteúdo explícito é marcado pelos provedores de conteúdo, como as gravadoras, ao vender através da iTunes Store.
	Região das classificações	Selecione uma região da lista suspensa para alterar a região associada às seleções de classificação para aplicativos, programas de TV e filmes.

	Filmes	Selecione um limite de classificação para filmes armazenados no dispositivo: • Não permitir filmes • G • PG • PG-13 • R • NC-17 • Permitir todos os filmes
	Programas de TV	Selecione um limite de classificação para programas de TV armazenados no dispositivo: • Não permitir programas de TV • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • Permitir todos os programas de TV

	Aplicativos	Selecione um limite de classificação para aplicativos armazenados no dispositivo: • Não permitir apps • 4+ • 9+ • 12+ • 17+ • Permitir todos os apps

Para obter mais informações, consulte Como criar uma configuração

Exibição da sala de conferência

Aplicável a: tvOS 10.2 e versões mais recentes com suporte.

Essa configuração ativará o modo Exibição em sala de conferência no Apple TV. O modo Exibição em sala de conferência bloqueia o Apple TV nesse modo para impedir outros tipos de uso.

A partir do tvOS 10.2, você pode configurar os dispositivos Apple TV supervisionados para o modo Exibição em sala de conferência. A Exibição em sala de conferências bloqueia os dispositivos Apple TV designados em uma tela de papel de parede preto e baixa um protetor de tela padrão, a menos que uma imagem de plano de fundo e um protetor de tela sejam definidos manualmente nas configurações do dispositivo Apple TV. Este modo também pode exibir uma mensagem previamente configurada na configuração Exibição em sala de conferência.

A configuração Exibição em sala de conferência pode ser implantada automaticamente e os aplicativos podem ser instalados enquanto os dispositivos estiverem nesse modo. Um dispositivo definido para o modo Exibição em sala de conferência que é reiniciado retoma automaticamente a tela bloqueada sem mostrar primeiro a tela inicial.

Se um dispositivo Apple TV estiver rodando no modo Aplicativo único ou se o modo Aplicativo único for implantado com Exibição em sala de conferências, a Exibição em sala de conferências substituirá o modo Aplicativo único. Além disso, se um dispositivo Apple TV estiver conectado a uma rede via Ethernet, a Exibição em sala de conferência não exibirá automaticamente uma rede Wi-Fi para se conectar para compartilhamento do AirPlay. Esta instrução pode ser exibida na tela usando o campo Mensagem personalizada da configuração Exibição em sala de conferência.

Criando uma configuração Exibição em sala de conferência

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **conferência** no campo de pesquisa e clique na configuração **Exibição em sala de conferência**.
4. Digite um nome e descreva a configuração.

5. Especifique a **Mensagem personalizada**. Esta é a mensagem personalizada exibida na tela no modo Exibição em sala de conferências.
6. Clique em **Avançar** para configurar as definições de distribuição.
7. Clique em **Concluído**.

Para obter mais informações, consulte Como criar uma configuração.

Bloqueio e quiosque: modo administrador de dispositivo Android

A configuração Bloqueio e Quiosque: Modo Administrador de Dispositivo Android desabilita determinados recursos dos dispositivos Android e cria uma lista com os apps permitidos a serem disponibilizados aos usuários no Modo de Quiosque.

A configuração Modo Administrador de Dispositivo Android foi preterida e não é suportada em dispositivos com Android 8 e versões posteriores. Recomenda-se usar Bloqueios do Android Enterprise para Bloqueios de Quiosque em Android 8 e versões posteriores.

Você pode restringir a opção para modificar configurações ou apps quando um dispositivo Android estiver no modo de quiosque.

- Adicione apps e selecione as configurações na página Criar bloqueio e quiosque: Configuração do modo administrador do dispositivo Android.
- A opção para alterar as configurações usando o ícone Configurações será disponibilizado no modo de quiosque.
- Selecione apps sem escolher as opções de configuração de ajuste e o ícone de configurações não será exibido no modo de quiosque.
- Se você optar por não incluir apps na configuração, o ícone de configurações será exibido.

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Configurações de bloqueio: desabilita recursos de todos os dispositivos Android.	
Desabilitar Wi-Fi	Selecione para desativar o acesso a LANs sem fio.
Desabilitar câmera	Selecione para desativar o acesso à câmera.
Desabilitar Bluetooth	Selecione para desativar os recursos Bluetooth. tome cuidado ao usar essa opção. A Ivanti não recomenda desativar o áudio, pois o acesso "sem as mãos" ao Bluetooth está desativado. Os requisitos legais para o uso 'sem as mãos' de dispositivos ao dirigir está se difundindo cada vez mais.
Configurações do modo de quiosque: habilita o dispositivo para que ele seja utilizado como um quiosque, com a operação restrita a apenas alguns aplicativos específicos. As configurações de modo de quiosque não serão aplicadas a um dispositivo com Android 8.0 ou superior. Para esses dispositivos, o Status do quiosque na página de detalhes de um dispositivo relata UNSUPORTED_ON_DEVICE como o Status do quiosque.	
Ativar modo de quiosque	Selecione para configurar o Modo de quiosque em dispositivos Android.
Desabilitar configurações rápidas	Selecione para desabilitar as configurações rápidas no modo de quiosque.
Permitir acesso do usuário às configurações Wi-Fi	Selecionar para permitir que um usuário altere as configurações de Wi-Fi e acesse suas redes sem fio preferidas.

Permitir acesso do usuário às configurações do Bluetooth	Selecionar para permitir que um usuário altere as configurações de Bluetooth e emparelhe dispositivos Bluetooth adicionais.
Permitir acesso do usuário às configurações de localização	Selecione para permitir que o usuário acesse as configurações de localização.
Permitir que o usuário atrase as atualizações do aplicativo	Selecionar para permitir que um usuário atrase as atualizações do aplicativo.
PIN para sair do modo de quiosque	Insira o código de quatro dígitos que o usuário final deve digitar para sair do modo de quiosque.
Criar uma lista de apps permitidos: esses apps estarão disponíveis para os usuários no Modo de quiosque adicionando apps na lista de apps permitidos. Arraste e solte para organizar os aplicativos na ordem em que devem aparecer no iniciador do Modo de quiosque. A adição de um aplicativo na lista de aplicativos permitidos não instala o aplicativo no dispositivo. Distribua os aplicativos para os usuários ou grupos de usuários adequados no Catálogo de aplicativos.	
Apps integrados	Clique em +Adicionar para incluir apps nativos listados no grupo de apps permitidos no modo de quiosque. se você desabilitou o Discador ou a Câmera nas Configurações de bloqueio acima, eles não poderão ser adicionados à Lista de aplicativos permitidos.

App Catalog	Clique em +Adicionar para incluir apps listados no app catalog no grupo de apps permitidos no modo de quiosque.
Outros apps	Clique em +Adicionar para incluir o nome do pacote de um aplicativo que não está disponível na Google Play Store.
Apps permitidos no modo de quiosque	Clique em X para remover um aplicativo do grupo de apps permitidos no modo de quiosque. Arraste e solte para alterar a ordem na qual os apps aparecem em dispositivos quiosque.

para dispositivos Samsung com Knox Standard 4.0 ou mais, o recurso de multiusuário é automaticamente bloqueado em modo de quiosque.

Para dispositivos que não são da Samsung, o modo quiosque não recebe suporte em Android 8.0 ou superior. A Ivanti recomenda o uso de bloqueios do Android Enterprise para bloqueios no modo de quiosque no Android 8.0 ou versões superiores.

Tópicos relacionados:

- Configuração do modo de quiosque para Android
- Como criar uma configuração

Configuração do modo quiosque para Android

Esta seção contém os seguintes tópicos:

- Iniciar o modo quiosque remotamente
- Sair do modo de quiosque

Licença: Silver

O modo de quiosque para os dispositivos Android permite que você restrinja o uso de um dispositivo para apps específicos. O modo de quiosque deve ser utilizado para configurar dispositivos para os funcionários que utilizarão somente apps específicos para o trabalho.

Ao preparar dispositivos Android para o modo de quiosque ou o Proprietário do dispositivo com o modo de quiosque, você precisará criar uma lista de apps permitidos que deseja disponibilizar para os usuários no Modo de quiosque. Para dispositivos que utilizam o Proprietário do dispositivo, é possível adicionar aplicativos à lista de aplicativos permitidos arrastando e soltando para organizar os aplicativos na ordem em que eles devem aparecer no ativador do modo de quiosque ao configurar o aplicativo. Consulte Configuração de bloqueio de quiosque para obter mais informações.

Pré-requisitos

Antes de configurar o modo de quiosque para os dispositivos Android, assegure que você tenha executado as tarefas a seguir:

- Instalado o Go nos dispositivos.
- Configurado o catálogo de aplicativos com os apps necessários para a configuração do quiosque.
- Distribuído o catálogo de aplicativos aos dispositivos que serão executados no modo de quiosque.

  Dispositivos SonimXP5S não oferecem suporte ao modo quiosque.

- Instalado os apps necessários para a configuração do quiosque.
- (Opcional) Configure a atribuição de marca do quiosque Android.

O modo quiosque é compatível com Android 5.1 e 6.0. Dispositivos sem Samsung Knox devem ser colocados no modo Proprietário do Dispositivo para evitar o uso de aplicativos indesejados.

Importante: alguns dispositivos possuem recursos que podem fazer com que o dispositivo coloque imagens sobre a tela ou crie uma fuga do modo de quiosque. O recurso People Edge do Samsung Galaxy S6 Edge é um exemplo de tal recurso. Recomendamos que um administrador desative esses tipos de recursos antes que o dispositivo seja implantado.

Procedimento

1. Vá até **Configurações**.
2. Clique em **+Adicionar**.
3. Clique em **Bloqueio e quiosque: modo administrador do Android Enterprise**.
4. Na tela **Criar configurações**, preencha pelo menos a seção **Configurações do modo de quiosque**.
5. Na tela **Distribuição**, selecione os grupos de dispositivos que receberão essa configuração.
6. Clique em **Concluído**.
7. Para dispositivos que não são da Samsung, continue com as etapas a seguir:
   a. Acesse **Dispositivos** >**Dispositivos**.
   b. Selecione os dispositivos que você deseja habilitar para o modo de quiosque.
   c. Selecione **AçõesForçar Check-in**.
   d. Nos dispositivos, toque no botão **Modo de quiosque**.
   e. Pressione o botão **Início** no dispositivo.
   f. Se for exibida uma caixa de diálogo **Escolher iniciador**, toque em **Ir para o iniciador do quiosque** e selecione **Sempre**. Essa etapa é necessária para garantir que seja utilizado o iniciador correto para esse recurso. Caso contrário, será solicitado que o usuário selecione um iniciador.

Iniciando o modo quiosque remotamente

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Adicione a coluna Modo de quiosque à exibição.

3. Selecione dispositivos que possuem o Modo de quiosque ativado, mas não estão no Modo de quiosque no momento.
4. Selecione **Ações > Entrar no modo de quiosque**.

Sair do modo de quiosque

Você pode sair do modo quiosque no dispositivo se definir um PIN na configuração.

Procedimento

1. Toque no ícone **Configurações**.
2. Selecione **Sair do modo de quiosque**.
3. Toque no campo **PIN do quiosque** quando solicitado.
4. Insira o PIN do quiosque.

Você pode sair do modo de quiosque para um dispositivo específico do portal:

Procedimento

1. Acesse **Dispositivos > Dispositivos**.
2. Visualize os detalhes do dispositivo.
3. Selecione **Ações > Sair do modo de quiosque**.

Você também pode usar os métodos a seguir para sair do modo de quiosque:

- Excluir a configuração
- Desabilitar a configuração
- Remova o grupo de dispositivos da configuração

Configuração do quiosque de dispositivos compartilhados Android

Para implantações de trabalho de tarefa, as empresas podem oferecer dispositivos Android dedicados que são personalizados para uma função de usuário específica. Dependendo do perfil de um usuário, diferentes apps e configurações podem ser apresentados em um dispositivo. Por exemplo, um usuário em uma função técnica pode ter um conjunto específico de apps apresentados para uso, enquanto que outro usuário em um papel de manutenção pode ter acesso a diferentes conjuntos de apps.

O modo de quiosque de dispositivos compartilhados do Android age como um filtro de aplicativos para diferentes grupos de usuários que compartilham dispositivos. Um usuário que está conectado ao quiosque dos dispositivos compartilhados consegue apenas visualizar os apps adequados para a sua função. Uma das principais vantagens do quiosque de dispositivos compartilhados é que você pode permitir que diferentes grupos de usuários acessem diferentes conjuntos de apps do mesmo dispositivo. Quando um usuário faz logout de um modo de quiosque de dispositivos compartilhados do Android, seus apps e dados de usuário, incluindo históricos, são apagados e não são exibidos para próximo usuário que se conectar ao dispositivo (se o aplicativo for reinstalado). O quiosque de dispositivos compartilhados só está disponível para implantações corporativas do Android corporativo com contas gerenciadas do Google Play.

O quiosque de dispositivos compartilhados requer dois tipos de usuários, um usuário de preparação e um usuário de quiosque compartilhado e pelo menos duas políticas que correspondem a esses usuários. O usuário de preparação é usado para solicitar que a tela de login apareça em um dispositivo compartilhado. Além disso, o usuário de preparação é um tipo especial de administrador que permite que outros usuários façam login ao dispositivo de quiosque. Após o usuário do quiosque dos dispositivos compartilhados fazer login com sucesso, a política de preparação é substituída por uma política de quiosque compartilhada. O usuário de quiosque tem acesso aos apps instalados no dispositivo de acordo com a política atribuída a ele. Embora você possa criar várias políticas de quiosque compartilhadas, há apenas uma política de quiosque ativa em um dispositivo quiosque por vez. Quando o usuário de quiosque faz logout do quiosque compartilhado, o dispositivo volta para o usuário de preparação e, consequentemente, para a política de preparação.

O usuário de preparação pode apenas acessar a página de login. Como resultado, é preciso criar uma política de preparação que é dedica a este usuário. No entanto, os usuários de quiosque de dispositivos compartilhados podem acessar um conjunto de apps que você define na política deles. (Naturalmente, você também precisa instalar os aplicativos permitidos nos quiosques dos dispositivos compartilhados.) A política de quiosque de dispositivo compartilhado permite criar um filtro de aplicativos permitidos a partir de todos os aplicativos que você instalou anteriormente. Você não pode carregar diretamente os apps em uma política de quiosque compartilhada do Android. É costume dedicar uma política de quiosque dedicada a um tipo de usuário de quiosque dedicado ou grupo de usuário, dependendo da organização. Por exemplo, uma empresa pode ter funcionários do turno da manhã e do turno da noite que têm funções diferentes e exigem acesso a um conjunto separado de apps. Neste caso, você precisa criar uma política para o turno da manhã e para o turno da noite.

Para mais informações sobre a ativação de quiosque de dispositivos compartilhados, consulte "Bloqueio e Quiosque: Android Enterprise" na página 620.

Bloqueio e Quiosque: Android Enterprise

A configuração Bloqueio e quiosque: Android Enterprise desativa determinados recursos dos dispositivos com Android Enterprise e cria uma lista de apps permitidos que serão disponibilizados aos usuários no modo de quiosque.

Esta seção contém os seguintes tópicos:

- Configurações de bloqueio
- Perfil de trabalho
- Configurações de bloqueio de dispositivos gerenciados de trabalho
- Dispositivos Gerenciados com Perfil de Trabalho (Android 8 -10) e Perfil de Trabalho em dispositivos de Propriedade da Empresa (Android 11+)

Configurações de bloqueio

Configuração	Descrição
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Escolha o tipo de bloqueio	Selecione o tipo de configurações de bloqueio que deseja configurar: • Perfil de trabalho • Dispositivos gerenciados de trabalho (Configurações de Proprietário do dispositivo e de Modo de quiosque) • Configurações de bloqueio Dispositivo gerenciado com Perfil de trabalho/Perfil de trabalho no dispositivo de propriedade da empresa As Configurações de bloqueio Perfil de trabalho no dispositivo de propriedade da empresa aplicam-se somente a dispositivos Android 11 e versões posteriores. Somente um tipo é permitido por configuração. As opções exibidas dependem do tipo selecionado. Se as configurações Dispositivo gerenciado de trabalho (proprietário do dispositivo) e Dispositivo gerenciado pelo Work Profile em dispositivo de propriedade da empresa forem distribuídas ao mesmo dispositivo, o Dispositivo gerenciado com perfil de trabalho terá precedência.

Perfil de trabalho

Desabilitar determinados recursos nos dispositivos com Android Enterprise.

Configuração	O que fazer	Para dispositivos
Desabilitar captura de tela	Selecione para desativar o uso do recurso de captura de tela integrado do dispositivo.	• Android 5.0 +
Desabilitar o controle de apps	Selecione para impedir que um usuário modifique os aplicativos em Configurações ou nos inicializadores.	• Android 5.0 +
Proibir credenciais de configuração	Selecione para impedir que um usuário configure as credenciais de usuário.	• Android 5.0 +
Proibir recursos de copiar e colar de outros perfis	Selecione para impedir que informações sejam copiadas/coladas entre perfis.	• Android 5.0 +
Proibir modificação de contas	Selecione para impedir que um usuário adicione ou remova contas.	• Android 5.0 +
Proibir transmissão de arquivos	Selecione para impedir que um usuário use o NFC para transferir dados do aplicativo.	• Android 5.1+
Desabilitar compartilhamento de localização	Selecione para impedir que um usuário revele a localização do dispositivo a apps.	• Android 5.0 +
Não permitir recursos de depuração	Selecione para desabilitar recursos de depuração nos dispositivos. Por padrão, essa opção está ativada.	• Android 5.0 +

Configuração	O que fazer	Para dispositivos
Garantir verificação dos apps	Selecione para permitir recursos de verificação de aplicativos nos dispositivos. Por padrão, essa opção está ativada. quando essa opção for desativada, o dispositivo será retornado para seu comportamento padrão, que pode variar de um dispositivo para outro.	• Android 5.0 +
Desabilitar fontes desconhecidas no dispositivo	Selecione para evitar que o dispositivo instale apps provenientes de fontes de desconhecidas. a ativação dessa configuração no dispositivo depende de uma atualização esperada no Google Play.	• Android 5.0 +

Configuração	O que fazer	Para dispositivos
Restringir métodos de entrada	Selecione para restringir os nomes de pacotes IME permitidos designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote**. Os dispositivos terão tanto métodos de entrada de pacotes permitidos quanto os métodos de entrada padrão do sistema para usar. O usuário pode alternar entre métodos padrão de entrada do sistema e métodos de entrada de pacotes permitidos.	• Android 5.0 +

Configuração	O que fazer	Para dispositivos
	Para o Android 10 ou superior, a inserção na lista de permitidos é aplicável apenas aos apps IME no lado do Work Profile. Para versões mais antigas do Android, a inserção na lista de permitidos é aplicável a apps IME em todo o dispositivo (dentro e fora do Work Profile).	
Restringir serviços de acessibilidade	Selecione para restringir os serviços de acessibilidade de apps de trabalho designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote**. Se não houver pacotes na lista de permissão, apenas serviços de acessibilidade do sistema serão permitidos.	• Android 5.0 +
Desativar fontes desconhecidas dentro do perfil de trabalho	Selecionar para proibir o download de fontes desconhecidas no perfil de trabalho.	• Android 5.0 +

Configuração	O que fazer	Para dispositivos
Ativar/desativar apps do sistema	Selecione para habilitar e desabilitar a implementação de aplicativos do sistema designando duas listas de nomes de pacotes nos campos **Nome do pacote de aplicativo do sistema**. Use esse recurso para gerenciar o acesso aos aplicativos do sistema que não estão publicados na Google Play. Não há suporte para adicionar um aplicativo ao App Catalog e também a uma lista de aplicativos do sistema.	• Android 5.0 +
Desabilitar identificador de chamada	Define se as informações do identificador de chamada do perfil de trabalho serão exibidas no dispositivo no recebimento de chamadas.	• Android 6.0+
Desativar Compartilhamento de contato via Bluetooth	Selecione para evitar que o dispositivo compartilhe contatos com outros dispositivos via Bluetooth.	• Android 6.0+

Configuração	O que fazer	Para dispositivos
Desativar Compartilhamento de contato via Pesquisa	Selecione para evitar que os usuários pesquisem contatos de trabalho no discador de telefone pessoal.	• Android 7.0 +
Não permitir preenchimento automático	Selecione para não permitir preenchimento automático	• Android 8.0+
Não permitir as notificações do aplicativo de trabalho no perfil pessoal	Selecionar para restringir as notificações do Work Profile.	• Android 8.0+
Não permitir impressão	Selecionar para restringir a impressão de todos os apps.	• Android 9.0+
Não permitir compartilhamento no perfil	Selecionar para evitar que os usuários compartilhem dados pessoais em um perfil de trabalho no dispositivo.	• Android 9.0+

Configuração	O que fazer	Para dispositivos
Habilitar acesso aos calendários do perfil de trabalho	Selecione qualquer uma das opções a seguir para permitir todos os aplicativos ou selecione um conjunto de aplicativos no lado pessoal para acessar as informações de calendário presentes no Work Profile: • **Todos os apps no perfil pessoal** – Permitir que todos os apps acessem as informações de calendário presentes no Work Profile. • **Somente os seguintes apps no perfil pessoal** – No campo de texto abaixo, insira os IDs do pacote dos apps, separando-os por vírgula. Apenas esses aplicativos selecionados no lado pessoal terão acesso às informações de calendário presentes no Work Profile.	• Android 10.0+

Configuração	O que fazer	Para dispositivos
	Para acessar o calendário compartilhado, o aplicativo no lado pessoal precisa implementar APIs específicas.	
Ativar a inserção de apps na lista de permitidos entre perfis	Marque a caixa de seleção para permitir que os usuários compartilhem informações de aplicativos específicos de dentro do perfil de trabalho para o lado pessoal do dispositivo. No campo **Apps permitidos**, digite os IDs dos pacotes dos apps a serem permitidos, separados por vírgulas. Esta opção está desativada por padrão.	• Android 11.0+
Habilitar fatiamento de rede 5G	Selecione para fornecer a opção de fatiamento de rede 5G no perfil de trabalho dos dispositivos de propriedade da empresa. Esta opção está desativada por padrão.	• Android 12.0+

Configurações de bloqueio de dispositivos gerenciados de trabalho

Desabilitar determinados recursos em dispositivos de trabalho gerenciados (Proprietário do dispositivo) com Android 5.0+.

Configuração	Descrição
Desabilitar Wi-Fi	Selecione para desativar o acesso a LANs sem fio.
Desativar configurações Wi-Fi	Selecione para desativar o acesso às configurações sem fio.
Desabilitar câmera	Selecione para desativar o acesso à câmera.
Desabilitar Bluetooth (Android 8.0+)	Selecione para desativar os recursos Bluetooth. tome cuidado ao usar essa opção. A Ivanti não recomenda desativar o áudio, pois o acesso "sem as mãos" ao Bluetooth está desativado. Os requisitos legais para o uso 'sem as mãos' de dispositivos ao dirigir está se difundindo cada vez mais.
Desabilitar configurações de Bluetooth (Android 8.0+)	Selecione para desativar o acesso às configurações Bluetooth.
Desabilitar captura de tela	Selecione para desativar o uso do recurso de captura de tela integrado do dispositivo.
Silenciar volume principal	Selecione para silenciar o volume principal.
Desabilitar o controle de apps	Selecione para impedir que um usuário modifique os aplicativos em Configurações ou nos inicializadores.
Desabilitar credenciais	Selecione para impedir que um usuário configure as credenciais de usuário.
Desabilitar transmissões de emergência	Selecione para evitar transmissões de emergência.
Desabilitar redes móveis	Selecione para desativar o acesso às redes móveis. essa opção não poderá ser desabilitada se o Wi-Fi estiver desabilitado.

Configuração	Descrição
Desabilitar compartilhamento de internet	Selecione para desativar o compartilhamento de internet como uma opção para o uso da conexão de internet de um dispositivo para oferecer acesso a outro dispositivo.
Desabilitar VPN	Selecione para desativar as conexões de VPN.
Desabilitar restaurar configurações de fábrica	Selecione para impedir que os usuários redefinam as configurações de fábrica do dispositivo.
Ativar proteção de reinicialização para configurações de fábrica	Selecione para permitir que os usuários redefinam as configurações de fábrica do dispositivo. Você pode, caso queira, especificar uma lista de IDs de conta do Google autorizados (um valor inteiro) que podem provisionar o dispositivo depois da reinicialização para as configurações de fábrica, ou passar o mouse sobre o ícone de ajuda para ver como recuperar os IDs de conta autorizados.
Proibir modificação de contas	Selecione para impedir que um usuário adicione ou remova contas.
Proibir NFC (feixe de saída)	Selecione para impedir que um usuário use o NFC para transferir dados do aplicativo.
Desabilitar realização de chamadas	Selecione para evitar que um usuário realize chamadas.
Impedir inicialização segura (Android 6.0 e superior)	Selecione para impedir que um usuário reinicialize um dispositivo no modo de inicialização seguro.
Desabilitar compartilhamento de localização	Selecione para impedir que um usuário revele a localização do dispositivo a apps.
Não permitir recursos de depuração	Selecione para desabilitar recursos de depuração nos dispositivos. Por padrão, essa opção está ativada.

Configuração	Descrição
Garantir verificação dos apps	Selecione para permitir recursos de verificação de aplicativos nos dispositivos. Por padrão, essa opção está ativada. quando essa opção for desativada, o dispositivo será retornado para seu comportamento padrão, que pode variar de um dispositivo para outro.
Desabilitar SMS	Selecione para evitar que um usuário envie e receba mensagens SMS.
Desabilitar a desativação do mudo do microfone	Selecionar para evitar que um usuário desative o mudo do microfone do dispositivo.
Proibir ajuste de horário automático	Selecionar para evitar que um usuário habilite mudanças de horário automáticas.
Proibir ajuste de fuso horário automático	Selecione para evitar que um usuário habilite o ajuste de horário automático do dispositivo com mudanças de fuso horário.
Sincronizar horário com o servidor (Android 9.0+)	Selecione para permitir que os dispositivos sincronizem com os servidores do Ivanti Neurons for MDM pela primeira vez no registro e, depois disso, uma vez a cada 24 horas após cada check-in. Esta opção estará disponível apenas se **Desabilitar horário automático** estiver selecionada.
Definir fuso horário (Android 9.0+)	Especifique a sequência de fuso horário no formato de ID de fuso horário Olson (por exemplo, Pacífico/Midway).
Desabilitar roaming de dados	Selecione para desativar a troca de dados enquanto o dispositivo estiver em roaming.
Desabilitar suspensão do Wi-Fi	Selecionar para manter o Wi-Fi ativo enquanto o dispositivo está no modo de Repouso.

Configuração	Descrição
Restringir métodos de entrada	Selecione para restringir os nomes de pacotes IME permitidos designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote**. Os dispositivos terão tanto métodos de entrada de pacotes permitidos quanto os métodos de entrada padrão do sistema para usar. O usuário pode alternar entre métodos padrão de entrada do sistema e métodos de entrada de pacotes permitidos. Para o Android 10 ou superior, a inserção na lista de permitidos é aplicável apenas aos apps IME no lado do dispositivo. Para versões mais antigas do Android, a inserção na lista de permitidos é aplicável a apps IME em todo o dispositivo.
Restringir serviços de acessibilidade	Selecione para restringir os serviços de acessibilidade de apps de trabalho designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote**. Se não houver pacotes na lista de permissão, apenas serviços de acessibilidade do sistema serão permitidos.
Desativar transferência de arquivo por USB	Selecione para desativar a transferência de arquivo por USB.
Desativar mídia externa	Selecione para desativar a mídia externa.
Desativar proteção do teclado (sem efeito se o PIN/senha for definido)	Selecione para desativar a proteção. Essa opção não tem efeito se uma senha, PIN ou padrão estiver definido. Se uma senha, PIN ou padrão for definido após a proteção ser desativada, a proteção não ficará mais desativada.

Configuração	Descrição
Mantenha a tela ligada enquanto estiver conectado à energia.	Selecione para manter a tela LIGADA quando conectado à energia. A tela poderá esmaecer, mas não desligará enquanto o dispositivo estiver conectado à energia. Essa configuração somente terá efeito se a trava automática ou o tempo limite de inatividade na configuração da senha não for usado para definir um tempo limite.
Não permitir a criação de janelas	Selecione para evitar que os apps exibam determinados tipos de janelas de sobreposição, como alertas e notificações do sistema.
Ignorar as primeiras dicas de uso	Selecione para ativar a recomendação do sistema para apps ignorarem o tutorial do usuário e outras dicas introdutórias na primeira inicialização.
Não permitir fontes desconhecidas no dispositivo	Selecione para desautorizar o usuário a instalar aplicativos provenientes de fontes de desconhecidas.
Definir mensagem da tela de bloqueio (Android 7.0+)	Selecione para definir a mensagem de tela de bloqueio a ser exibida no dispositivo. Digite a mensagem de tela de bloqueio (máximo de 256 caracteres) no campo de texto. Ao ativar essa opção, o usuário é bloqueado de definir a mensagem em Configurações e a mensagem que é definida pelo administrador é exibida para o usuário. Se o administrador não fornecer nenhuma mensagem de tela de bloqueio depois de ativar "Definir mensagem de tela de bloqueio", o usuário é bloqueado de definir a mensagem em Configurações, mas nenhuma mensagem é exibida para o usuário.
Definir o brilho da tela	Selecione para definir o brilho da tela do seu dispositivo. • Manual: selecione para inserir um número manualmente (0 a 255) • Adaptável: selecione para permitir que o dispositivo defina o brilho Recomenda-se ativar a opção "Não permitir configuração do brilho" antes de definir o brilho da tela do seu dispositivo.

Configuração	Descrição
Definir tempo limite da tela	Selecione para definir a duração do tempo limite da tela (em segundos). Recomenda-se ativar a opção "Não permitir configuração do tempo limite da tela" antes de definir o brilho da tela do seu dispositivo.
Definir orientação da tela	Selecione para definir a orientação da tela. Você pode definir a orientação da tela em 0, 90, 180 ou 270 graus na lista suspensa. Por padrão, esta opção não fica selecionada. Para o aplicativo Go 89 e versões posteriores, você deve selecionar essa opção e definir o valor como 0 para manter o dispositivo em modo Retrato no Quiosque.
Ativar/desativar apps do sistema	Selecione para habilitar e desabilitar a implementação de aplicativos do sistema designando duas listas de nomes de pacotes nos campos **Nome do pacote de aplicativo do sistema**. Use esse recurso para gerenciar o acesso aos aplicativos do sistema que não estão publicados na Google Play. Não há suporte para adicionar um aplicativo ao App Catalog e também a uma lista de aplicativos do sistema.
Android 8.0+	
Não permitir preenchimento automático	Selecione para não permitir que o usuário use serviços de preenchimento automático.
Não permitir compartilhamento por Bluetooth	Selecione para não permitir que o usuário compartilhe Bluetooth de saída no dispositivo.
Desativar serviço de backup	Selecione para desativar o serviço de backup.
Android 9.0+	

Configuração	Descrição
Não permitir impressão	Selecione para não permitir que o usuário imprima.
Não permitir modo avião	Selecione para desativar o modo avião em todo o dispositivo.
Não permitir ambient display	Selecione para não permitir ambient display para o usuário.
Não permitir configuração do brilho	Selecione para não permitir que o usuário configure o brilho. Recomenda-se especificar "Definir modo de brilho da tela" antes de selecionar esta opção.
Não permitir configuração de data e hora	Selecione para não permitir configuração de data, hora e fuso horário.
Não permitir configuração do local	Selecione para não permitir que o usuário desative provedores de localização.
Não permitir configuração do tempo limite da tela	Selecione para não permitir que o usuário altere o tempo limite de desativação da tela. Recomenda-se especificar o valor "Definir tempo limite da tela" antes de selecionar esta opção.
Android 12.0+	
Habilitar USB apenas para carregamento	Selecione para habilitar a porta USB apenas para carregamento.
Android 13.0+	

Configuração	Descrição
Definir segurança mínima necessária do Wi-Fi	Use esta opção para definir a segurança mínima necessária do Wi-Fi: • Sem exigência de segurança mínima: selecione essa opção se não for necessária nenhuma segurança mínima • Segurança baseada em rede pessoal: selecione esta opção para bloquear redes Wi-Fi pessoais, como WEP, WPA/WPA2/WPA3, etc. • Segurança baseada em rede EAP corporativa: selecione esta opção para bloquear redes Wi-Fi baseadas em protocolo EAP • Segurança baseada em rede 192 corporativa: selecione esta opção para bloquear redes Wi-Fi corporativas EAP  Todos os dispositivos existentes que não atendam aos critérios mínimos serão desconectados.  Os detalhes do dispositivo exibirão o nível mínimo exigido de segurança do Wi-Fi (se disponível) em **Geral > Nível de segurança Wi-Fi**.
Configurações do modo de quiosque: o modo de quiosque aplica mais restrições aos dispositivos, incluindo o acesso limitado aos apps por meio de um iniciador personalizado.	

Configuração	Descrição
Ativar modo de quiosque	Selecione para configurar o modo de quiosque em dispositivos Android. • Quando um usuário faz login no Modo de quiosque compartilhado e faz logout, o nome do usuário permanece disponível com o Go client para logins futuros. No Modo de quiosque compartilhado, o Go client preserva sete nomes de usuários usados recentemente. • O modo de quiosque compartilhado agora é compatível com Autenticação IDP. Portanto, se o Ivanti Neurons for MDM estiver configurado com IDP, o modo de quiosque compartilhado poderá ser usado com a Autenticação IDP.

Configuração	Descrição
Ativar o modo de tarefa de bloqueio	Selecione para ativar o modo de tarefa de bloqueio nos dispositivos Android. Quando ativado, os dispositivos podem exibir proteções de teclado, barra de status e modo seguro. Essa opção está desativada por padrão. As configurações a seguir são configurações adicionais exibidas quando o modo de bloqueio de tarefa for ativado para o Android 9 ou para versões mais recentes com suporte: **Ícone Configurações** – Permite que os aplicativos tenham acesso às funções do sistema que são dependentes do aplicativo Configurações do dispositivo. Permitir as Configurações do dispositivo ajuda a evitar violações do Modo de tarefa de bloqueio em casos de pareamento Bluetooth de um aplicativo. É recomendado manter essa configuração ativada para aplicativos específicos. **Informação do sistema** – Exibe a data/hora, conectividade, bateria e modo de vibração na barra de status. Essa opção está desativada por padrão. **Proteção de teclado** (ativado por padrão) – Ativa a proteção do teclado durante o modo de bloqueio de tarefa. **Ações globais** (ativado por padrão) – Ativa o menu exibido quando o usuário pressiona o botão liga/desliga. Se esta opção estiver desativada, talvez o usuário não consiga desligar o dispositivo. **Botão Início** – Ativa o botão de início. Essa opção está desativada por padrão. Quando ativada, as seguintes opções adicionais são exibidas: • **Botão Visão geral** (desativado por padrão) – Ativa o botão Visão geral e a tela Visão geral durante o modo de bloqueio de tarefa • **Notificações** (desativado por padrão) – Ativa as notificações durante o modo bloquear tarefa. Isso inclui ícones de notificação na barra de status, notificações de aviso e o sombreamento de notificação expansível.

Configuração	Descrição
	Se a opção Botão Início não estiver ativada, o usuário não poderá usar o recurso de múltiplas janelas.
Inserir o Quiosque automaticamente (somente na configuração inicial)	Selecione para permitir o modo de quiosque automaticamente quando a configuração for aplicada.
Desabilitar configurações rápidas para dispositivos Android 5	Selecione para desativar as Configurações rápidas no modo de quiosque para os dispositivos em execução no Android 5.
Desabilitar configurações rápidas para Android 6+ e todos os dispositivos Samsung	Selecione para desativar as Configurações rápidas no modo de quiosque para dispositivos Android Enterprise da versão 6 até a versão mais recente para todos os dispositivos Samsung. Desativar essa configuração não bloqueia ícones e sons de notificação no dispositivo.
Permitir acesso do usuário às configurações Wi-Fi	Selecionar para permitir que um usuário altere as configurações de Wi-Fi e acesse suas redes sem fio preferidas.
Permitir acesso do usuário às configurações do Bluetooth	Selecionar para permitir que um usuário altere as configurações de Bluetooth e emparelhe dispositivos Bluetooth adicionais.
Permitir acesso do usuário às configurações de localização	Selecione para permitir que o usuário acesse as configurações de localização.

Configuração	Descrição
Permitir que o usuário atrase as atualizações do aplicativo	Selecionar para permitir que um usuário atrase as atualizações do aplicativo.
Permitir que o usuário acesse as configurações de data e hora	Selecione para permitir que o usuário acesse as configurações de data e hora.
Permitir que o usuário acesse as configurações de rede móvel	Selecione para permitir que o usuário acesse as configurações de rede móvel.
Permitir que o usuário selecione o idioma	Selecione para permitir que o usuário acesse as configurações de idioma.

Configuração	Descrição
Ativar dispositivo compartilhado	Em um quiosque de dispositivos compartilhados, o dispositivo é compartilhado juntamente com vários usuários finais. Esta opção permite que um dispositivo compartilhe enquanto o dispositivo está em modo de quiosque: • **Ativar login**: Esta opção é para usuários administradores de quiosque. Quando um dispositivo for configurado com essa opção, a tela de login de usuário será exibida, permitindo que um usuário final faça login no quiosque de dispositivos compartilhados. A opção Ativar login estará visível apenas se o usuário for criado como um usuário de Conta de dispositivo Android Enterprise (usuário de preparação). Selecione **Usar substituição de domínio** e insira o domínio adequadamente. Essa opção marca o nome de usuário para sufixo de domínio. Se o sufixo do domínio estiver ausente, o sistema anexará automaticamente o sufixo de domínio ao usuário. • **Ativar logout**: quando um dispositivo for configurado com essa opção, o usuário final conectado terá acesso aos apps permitidos. Esse usuário pode ver a opção para fazer logout, mas não pode sair do quiosque. Quando um usuário efetua o logout do quiosque de dispositivos compartilhados, outro usuário pode fazer login no quiosque de dispositivos compartilhados e visualizar os apps conforme configurado pelo administrador. • Os apps aparecem com um ícone de reciclagem, que é usado para reforçar a instalação de um aplicativo a cada login. Essa opção pode ser usada para os apps que são dados armazenados em cache local. O usuário pode sair do modo de quiosque se o administrador aprovar o PIN do quiosque de saída.

Configuração	Descrição
	• **Tempo limite**: Especifique a duração em horas. Por exemplo, quando a duração do tempo limite for configurada para 2 horas e o usuário final não fizer logout do quiosque dos dispositivos compartilhados, a ação de logout será automaticamente realizada no dispositivo após duas horas. O campo **Tempo limite** é exibido apenas quando a opção **Ativar logout** é selecionada e é opcional. Você também pode fazer logout dos usuários finais no modo de quiosque compartilhado clicando na opção **Sair do quiosque do Android corporativo** na página de detalhes do dispositivo.
Permitir autenticação FIDO (requer o aplicativo Google Chrome no dispositivo)	Selecione esta opção para usar a autenticação FIDO para usuários ao usar o quiosque compartilhado. Permitir que os usuários usem chaves FIDO para fazer login no dispositivo. O Google Chrome é o único navegador compatível e deve estar disponível no dispositivo para que a autenticação FIDO esteja disponível no quiosque compartilhado.
Permitir que o usuário configure o brilho e a rotação automática	Selecione para permitir que o usuário configure o brilho e a rotação automática.
Ativar várias janelas	Selecione para permitir a exibição de mais de um aplicativo ao mesmo tempo com dispositivos Samsung (quiosque do Proprietário do dispositivo). Para permitir várias janelas no modo bloquear tarefa, as seguintes opções do modo bloquear tarefa também devem ser ativadas: • **Botão Início** • **Botão Visão geral**
Atribuição de marca ao quiosque	Selecione as opções de atribuição de marca personalizadas ou padrão na lista suspensa.

Configuração	Descrição
PIN para sair do modo de quiosque	Insira o PIN de seis dígitos que o usuário deve digitar para sair do Modo de quiosque. O PIN deve ter no mínimo seis dígitos e no máximo dez dígitos. Esse PIN se aplica a todos os dispositivos no modo de quiosque. Anteriormente, o comprimento do PIN do quiosque era quatro dígitos. O usuário pode continuar a usar o PIN de quatro dígitos mesmo após fazer upgrade de uma versão anterior para o Ivanti Neurons for MDM 82. No entanto, se houver qualquer alteração na configuração, o comprimento do PIN deverá ser definido de acordo com o novo requisito (ou seja, no mínimo seis dígitos e no máximo dez dígitos). O aplicativo Go protegerá o dispositivo contra ataques de força bruta. Para obter mais informações, consulte a documentação do Go para Android.
Criar uma lista de apps permitidos: esses apps estarão disponíveis para os usuários no Modo de quiosque adicionando apps na lista de apps permitidos. Arraste e solte para organizar os apps na ordem em que devem aparecer no iniciador do Modo de quiosque. A adição de um aplicativo na lista de aplicativos permitidos não instala o aplicativo no dispositivo. Distribua os aplicativos para os usuários ou grupos de usuários adequados no Catálogo de aplicativos.	

Configuração	Descrição
Apps integrados	Clique em +Adicionar para incluir apps nativos listados no grupo de apps permitidos no modo de quiosque. Nas configurações dos Aplicativos permitidos no modo de quiosque, as seguintes opções estão disponíveis: • **Limpar dados do usuário do aplicativo**: ativar esta opção permite que todos os dados do aplicativo sejam apagados automaticamente sem nenhum aviso quando o usuário fizer logout do quiosque. Selecione **Ativar dispositivo compartilhado** nas configurações do modo Quiosque para que essa opção esteja disponível com os aplicativos. ◦ Os dados do aplicativo não são apagados do Google Chrome e do pacote de visualização da Web, mesmo se forem adicionados à lista de apps permitidos com a opção apagar dados do usuário ativada. Isso ocorre porque o quiosque pode travar se os dados do aplicativo forem apagados para esses dois pacotes. ◦ Os dados do aplicativo não são apagados de aplicativos do sistema para os quais o inicializador de aplicativos não está disponível (dentro e fora do quiosque). • **Tornar oculto**: ativar esta opção permite que o aplicativo seja acessado por outros aplicativos, mas não esteja disponível no inicializador de quiosque. se você desabilitou o Discador ou a Câmera nas Configurações de bloqueio acima, eles não poderão ser adicionados à Lista de aplicativos permitidos.
App Catalog	Clique em +Adicionar para incluir apps listados no app catalog no grupo de apps permitidos no modo de quiosque.

Configuração	Descrição
Outros apps	Clique em +Adicionar para incluir o nome do pacote de um aplicativo que não está disponível na Google Play Store. Para dispositivos Samsung, os administradores devem colocar na lista de permitidos os seguintes pacotes de discador/sistema para torná-los funcionais no Modo de quiosque para ativar a funcionalidade do discador no Modo de quiosque. • Chamada – com.samsung.android.incallui • Telefone – com.samsung.android.dialer (deve estar na lista de permitidos e o administrador deve selecionar a opção Ocultar para este pacote para evitar problemas com duas opções de discagem para o usuário) • Chamada – com.sec.phone • Configuração de chamada – com.samsung.android.app.telephonyui • Discagem assistida – com.sec.providers.assisteddialing • Backup/Restauração do registro de chamadas – com.android.calllogbackup • Armazenamento do discador – com.android.providers.telephony • Telefone – com.android.server.telecom • Telefone – com.android.phone • Chamada inteligente – com.samsung.android.smartcallprovider • Chamadas WiFi – com.sec.unifiedwfc
Apps permitidos no modo de quiosque	Clique em X para remover um aplicativo do grupo de aplicativos permitidos no modo de quiosque. Arraste e solte para alterar a ordem na qual os apps aparecem em dispositivos quiosque.

para dispositivos Samsung com Knox Standard 4.0 ou mais, o recurso de multiusuário é automaticamente bloqueado em modo de quiosque.

Dispositivos gerenciados com perfil de trabalho

Desativa alguns recursos em um dispositivo gerenciado com o perfil de trabalho para Android 8.0 ou superior.

Determinados recursos podem ser desativados para Perfil de trabalho em dispositivos de propriedade da empresa (aplicável a dispositivos Android 11 e versões posteriores).

Configuração	Descrição
Configurações de bloqueio do dispositivo gerenciado	
Desabilitar Wi-Fi	Selecione para desativar o acesso a LANs sem fio. (Não aplicável a dispositivos Android 11)
Desativar configurações Wi-Fi	Selecione para desativar o acesso às configurações sem fio.
Desabilitar câmera	Selecione para desativar o acesso à câmera.
Desabilitar Bluetooth	Selecione para desativar os recursos Bluetooth. tome cuidado ao usar essa opção. A Ivanti não recomenda desativar o áudio, pois o acesso "sem as mãos" ao Bluetooth está desativado. Os requisitos legais para o uso 'sem as mãos' de dispositivos ao dirigir está se difundindo cada vez mais.
Desabilitar configurações de Bluetooth	Selecione para desativar o acesso às configurações Bluetooth.
Silenciar volume principal	Selecione para silenciar o volume principal. (Não aplicável a dispositivos Android 11 e versões posteriores)
Desabilitar transmissões de emergência	Selecione para evitar transmissões de emergência.
Desabilitar redes móveis	Selecione para desativar o acesso às redes móveis. essa opção não poderá ser desabilitada se o Wi-Fi estiver desabilitado.
Desabilitar compartilhamento de internet	Selecione para desativar o compartilhamento de internet como uma opção para o uso da conexão de internet de um dispositivo para oferecer acesso a outro dispositivo.
Desabilitar VPN	Selecione para desativar as conexões de VPN. (Não aplicável a dispositivos Android 11 e versões posteriores)

Configuração	Descrição
Desabilitar reinicialização para configurações de fábrica	Selecione para impedir que os usuários redefinam as configurações de fábrica do dispositivo. (Não aplicável a dispositivos Android 11 e versões posteriores)
Ativar proteção de reinicialização para configurações de fábrica	Selecione para permitir que os usuários redefinam as configurações de fábrica do dispositivo. Você pode, caso queira, especificar uma lista de IDs de conta do Google autorizados (um valor inteiro) que podem provisionar o dispositivo depois da reinicialização para as configurações de fábrica, ou passar o mouse sobre o ícone de ajuda para ver como recuperar os IDs de conta autorizados.
Desabilitar realização de chamadas	Selecione para evitar que um usuário realize chamadas.
Impedir inicialização segura (Android 6.0 e superior)	Selecione para impedir que um usuário reinicialize um dispositivo no modo de inicialização seguro.
Não permitir recursos de depuração	Selecione para desabilitar recursos de depuração nos dispositivos. Por padrão, essa opção está ativada.
Garantir verificação dos apps	Selecione para permitir recursos de verificação de aplicativos nos dispositivos. Por padrão, essa opção está ativada. quando essa opção for desativada, o dispositivo será retornado para seu comportamento padrão, que pode variar de um dispositivo para outro.
Desabilitar SMS	Selecione para evitar que um usuário envie e receba mensagens SMS.
Desabilitar a desativação do mudo do microfone	Selecionar para evitar que um usuário desative o mudo do microfone do dispositivo.
Proibir ajuste de horário automático	Selecionar para evitar que um usuário habilite mudanças de horário automáticas.

Configuração	Descrição
Proibir ajuste de fuso horário automático	Selecione para evitar que o usuário habilite o ajuste de horário automático do dispositivo com mudanças de fuso horário.
Desabilitar roaming de dados	Selecione para desativar a troca de dados enquanto o dispositivo estiver em roaming.
Sincronizar horário com o servidor (Android 9.0+)	Selecione para permitir que os dispositivos sincronizem com os servidores do Ivanti Neurons for MDM pela primeira vez no registro e, depois disso, uma vez a cada 24 horas após cada check-in. Esta opção estará disponível apenas se **Desabilitar horário automático** estiver selecionada.
Definir fuso horário (Android 9.0+)	Especifique a sequência de fuso horário no formato de ID de fuso horário Olson (por exemplo, Pacífico/Midway).
Desabilitar suspensão do Wi-Fi	Selecionar para manter o Wi-Fi ativo enquanto o dispositivo está no modo de Repouso. (Não aplicável a dispositivos Android 11 e versões posteriores)
Restringir métodos de entrada	Selecione para restringir os métodos de entrada de aplicativos de trabalho designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote**. (Não aplicável a dispositivos Android 11) Os dispositivos terão tanto métodos de entrada de pacotes permitidos quanto os métodos de entrada padrão do sistema para usar. O usuário pode alternar entre métodos padrão de entrada do sistema e métodos de entrada de pacotes permitidos. No Android 10+, os métodos de entrada são aplicáveis somente ao lado do dispositivo, caso contrário, são restritos a todo o dispositivo.

Configuração	Descrição
Restringir serviços de acessibilidade	Selecione para restringir os serviços de acessibilidade de apps de trabalho designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote**. Se não houver pacotes na lista de permissão, apenas serviços de acessibilidade do sistema serão permitidos. No Android 10+, os métodos de entrada são restritos aos apps de trabalho, caso contrário, são restritos a todo o dispositivo.
Desativar transferência de arquivo por USB	Selecione para desativar a transferência de arquivo por USB.
Desativar mídia externa	Selecione para desativar a mídia externa.
Não permitir fontes desconhecidas no dispositivo	Selecione para evitar que o dispositivo instale apps provenientes de fontes de desconhecidas. a ativação dessa configuração no dispositivo depende de uma atualização esperada no Google Play.
Definir mensagem da tela de bloqueio (Android 7.0+)	Selecione para definir a mensagem de tela de bloqueio a ser exibida no dispositivo. Digite a mensagem de tela de bloqueio (máximo de 256 caracteres) no campo de texto. Ao ativar essa opção, o usuário é bloqueado de definir a mensagem em Configurações e a mensagem que é definida pelo administrador é exibida para o usuário. Se o administrador não fornecer nenhuma mensagem de tela de bloqueio depois de ativar "Definir mensagem de tela de bloqueio", o usuário é bloqueado de definir a mensagem em Configurações, mas nenhuma mensagem é exibida para o usuário.

Configuração	Descrição
Definir o brilho da tela	Selecione para definir o brilho da tela do seu dispositivo. • Manual: selecione para inserir um número manualmente (0 a 255) • Adaptável: selecione para permitir que o dispositivo defina o brilho Recomenda-se ativar a opção "Não permitir configuração do brilho" antes de definir o brilho da tela do seu dispositivo. Se o usuário tiver permissão para fazer alterações, essas configurações serão redefinidas para as configurações definidas pelo administrador no próximo check-in. Esta configuração não é suportada em dispositivos com Android 11 e versões posteriores no modo Perfil de Trabalho em Dispositivos de Propriedade da Empresa.
Definir tempo limite da tela	Selecione para definir a duração do tempo limite da tela (em segundos). Recomenda-se ativar a opção "Não permitir configuração do tempo limite da tela" antes de definir o brilho da tela do seu dispositivo. Se o usuário tiver permissão para fazer alterações, essas configurações serão redefinidas para as configurações definidas pelo administrador no próximo check-in. Esta configuração não é suportada em dispositivos com Android 11 e versões posteriores no modo Perfil de Trabalho em Dispositivos de Propriedade da Empresa.

Configuração	Descrição
Definir orientação da tela	Selecione para definir a orientação da tela. Você pode definir a orientação da tela em 0, 90, 180 ou 270 graus na lista suspensa. Esta configuração não é suportada em dispositivos com Android 11 e versões posteriores no modo Perfil de Trabalho em Dispositivos de Propriedade da Empresa.
Não permitir preenchimento automático (Android 8.0+)	Selecionar para desabilitar o preenchimento automático. (Não aplicável a dispositivos Android 11 e versões posteriores)
Não permitir compartilhamento por Bluetooth (Android 8.0+)	Selecione para não permitir que o usuário compartilhe Bluetooth de saída no dispositivo.
Desativar serviço de backup (Android 8.0+)	Selecione para desativar o serviço de backup. (Não aplicável a dispositivos Android 11 e versões posteriores)
Não permitir impressão (Android 9.0+)	Selecione para restringir a impressão em todos os aplicativos. (Não aplicável a dispositivos Android 11)
Não permitir modo avião (Android 9.0+)	Selecione para desativar o modo avião em todo o dispositivo.
Não permitir ambient display (Android 9.0+)	Selecione para não permitir ambient display para o usuário. (Não aplicável a dispositivos Android 11 e versões posteriores)
Não permitir configuração do brilho (Android 9.0+)	Selecione para impedir que o usuário configure o brilho (não aplicável a dispositivos Android 11). Recomenda-se especificar "Definir modo de brilho da tela" antes de selecionar esta opção.
Não permitir configuração de data e hora (Android 9.0+)	Selecione para não permitir configuração de data, hora e fuso horário.
Não permitir configuração do local (Android 9.0+)	Selecione para não permitir que o usuário desative provedores de localização.

Configuração	Descrição
Não permitir configuração do tempo limite da tela (Android 9.0+)	Selecione para não permitir que o usuário altere o tempo limite de desativação da tela. (Não aplicável a dispositivos Android 11 e versões posteriores) Recomenda-se especificar os valores de "Definir tempo limite da tela" antes de selecionar esta opção.
Não permitir diálogos de erro do sistema (Android 9.0+)	Selecione para não permitir caixas de diálogo de erro do sistema. (Não aplicável a dispositivos Android 11)
Desativar captura de tela (Android 11.0 e versões posteriores)	Selecione para desativar o uso do recurso de captura de tela integrado do dispositivo. Quando selecionado, a captura de tela é desativada no lado pessoal do dispositivo.
Android 12.0+	
Habilitar USB apenas para carregamento	Selecione para habilitar a porta USB apenas para carregamento.
Android 13.0+	

Configuração	Descrição
Definir segurança mínima necessária do Wi-Fi	Use esta opção para definir a segurança mínima necessária do Wi-Fi: • Sem exigência de segurança mínima: selecione essa opção se não for necessária nenhuma segurança mínima • Segurança baseada em rede pessoal: selecione esta opção para bloquear redes Wi-Fi pessoais, como WEP, WPA/WPA2/WPA3, etc. • Segurança baseada em rede EAP corporativa: selecione esta opção para bloquear redes Wi-Fi baseadas em protocolo EAP • Segurança baseada em rede 192 corporativa: selecione esta opção para bloquear redes Wi-Fi corporativas EAP Todos os dispositivos existentes que não atendam aos critérios mínimos serão desconectados. Os detalhes do dispositivo exibirão o nível mínimo exigido de segurança do Wi-Fi (se disponível) em **Geral > Nível de segurança Wi-Fi**.
Configurações de bloqueio do Work Profile	
Desabilitar captura de tela	Selecione para desativar o uso do recurso de captura de tela integrado do dispositivo.
Desabilitar o controle de apps	Selecione para impedir que um usuário modifique os aplicativos em Configurações ou nos inicializadores.
Proibir credenciais de configuração	Selecione para impedir que um usuário configure as credenciais de usuário.
Proibir recursos de copiar e colar de outros perfis	Selecione para impedir que informações sejam copiadas/coladas entre perfis.

Configuração	Descrição
Proibir modificação de contas	Selecione para impedir que um usuário adicione ou remova contas.
Proibir NFC (feixe de saída) (Android 5.1 ou superior)	Selecione para impedir que um usuário use o NFC para transferir dados do aplicativo.
Desabilitar compartilhamento de localização	Selecionar para impedir que sites e apps avisem o usuário do dispositivo para compartilhar sua localização.
Não permitir recursos de depuração	Selecione para desabilitar recursos de depuração nos dispositivos. Por padrão, essa opção está ativada.
Garantir verificação dos apps	Selecione para permitir recursos de verificação de aplicativos nos dispositivos. Por padrão, essa opção está ativada. quando essa opção for desativada, o dispositivo será retornado para seu comportamento padrão, que pode variar de um dispositivo para outro.
Desativar fontes desconhecidas dentro do perfil de trabalho	Selecionar para proibir o download de fontes desconhecidas no perfil de trabalho.
Ativar/desativar apps do sistema	Selecione para habilitar e desabilitar a implementação de aplicativos do sistema designando duas listas de nomes de pacotes nos campos **Nome do pacote de aplicativo do sistema**. Use esse recurso para gerenciar o acesso aos aplicativos do sistema que não estão publicados na Google Play. Não há suporte para adicionar um aplicativo ao App Catalog e também a uma lista de aplicativos do sistema.
Desativar ID do chamador (Android 6.0 +)	Define se as informações do identificador de chamada do perfil de trabalho serão exibidas no dispositivo no recebimento de chamadas.

Configuração	Descrição
Desativar o compartilhamento de contatos via Bluetooth (Android 6.0+)	Selecione para evitar que o dispositivo compartilhe contatos com outros dispositivos via Bluetooth.
Desativar o compartilhamento de contatos via Busca (Android 7.0+)	Selecione para evitar que os usuários pesquisem contatos de trabalho no discador de telefone pessoal.
Não permitir preenchimento automático (Android 8.0+)	Selecionar para desabilitar o preenchimento automático. (Não aplicável a dispositivos Android 11 e versões posteriores)
Não permitir as notificações do aplicativo de trabalho no perfil pessoal (Android 8.0+)	Selecionar para restringir as notificações do Work Profile.
Não permitir impressão (Android 9.0+)	Selecionar para restringir a impressão de todos os aplicativos. (Não aplicável a dispositivos Android 11 e versões posteriores)
Não permitir compartilhamento no perfil (Android 9.0+)	Selecionar para evitar que os usuários compartilhem dados pessoais em um perfil de trabalho no dispositivo.

Configuração	Descrição
Restringir métodos de entrada (Android 10.0+)	Selecione para restringir os nomes de pacotes IME permitidos designando uma lista de nomes de pacotes permitidos por meio do campo **Nome do pacote** (não aplicável a dispositivos Android 11 e versões posteriores). Os dispositivos terão tanto métodos de entrada de pacotes permitidos quanto os métodos de entrada padrão do sistema para usar. O usuário pode alternar entre métodos padrão de entrada do sistema e métodos de entrada de pacotes permitidos. Os métodos de entrada serão aplicados aos aplicativos IME instalados no lado do perfil de trabalho. Mesmo que os apps instalados no lado do dispositivo estejam na lista de permitidos para esse bloqueio, eles não estarão disponíveis para uso pelos apps no lado do Work Profile.
Habilitar acesso aos calendários do perfil de trabalho (Android 10.0 ou superior)	Selecione qualquer uma das opções a seguir para permitir todos os aplicativos ou selecione um conjunto de aplicativos no lado pessoal para acessar as informações de calendário presentes no Work Profile: • **Todos os apps no perfil pessoal** – Permitir que todos os apps acessem as informações de calendário presentes no Work Profile. • **Somente os seguintes apps no perfil pessoal** – No campo de texto abaixo, insira os IDs do pacote dos apps, separando-os por vírgula. Apenas esses aplicativos selecionados no lado pessoal terão acesso às informações de calendário presentes no Work Profile. Para acessar o calendário compartilhado, o aplicativo no lado pessoal precisa implementar APIs específicas.

Configuração	Descrição
Habilitar a inserção de apps na lista de permitidos entre perfis (Android 11.0+)	Marque a caixa de seleção para permitir que os usuários compartilhem informações de aplicativos específicos de dentro do perfil de trabalho para o lado pessoal do dispositivo. No campo **Apps permitidos**, digite os IDs dos pacotes dos apps a serem permitidos, separados por vírgulas. Esta opção está desativada por padrão.
Ativar tempo limite máximo do perfil (Android 11.0 e versões posteriores)	Selecione para definir uma janela de tempo máximo em que o Perfil de Trabalho pode ser desativado antes de o Ivanti Neurons for MDM suspender aplicativos pessoais no dispositivo. É possível definir um tempo entre 72 e 8.760 horas. 8.760 horas é equivalente a um ano. O valor padrão será definido para 72h se a opção for selecionada. O usuário do dispositivo visualiza uma mensagem solicitando a ativação do Work Profile para ativar apps suspensos. Disponível para dispositivos Android 11 ou versão posterior no Work Profile em dispositivos de propriedade da empresa.
Habilitar fatiamento de rede 5G (Android 12.0+)	Selecione para fornecer a opção de fatiamento de rede 5G no perfil de trabalho dos dispositivos de propriedade da empresa. Esta opção está desativada por padrão.

Para obter mais informações, consulte Como criar uma configuração

Bloqueio e quiosque: Samsung Knox padrão

Uma configuração do Bloqueio e quiosque: Samsung Knox padrão desabilita determinados recursos dos dispositivos Samsung Knox padrão e cria uma lista de apps permitidos que serão disponibilizados aos usuários no Modo de quiosque.

A Configuração Samsung KNOX Padrão foi preterida e não é suportada em dispositivos com Android 9 e versões posteriores.

Configurações de bloqueio

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Configurações de bloqueio do Samsung Knox: desabilitar determinados recursos somente em dispositivos Samsung Knox.	
Desabilitar Wi-Fi	Selecione para desativar o acesso a LANs sem fio.
Desabilitar câmera	Selecione para desativar o acesso à câmera.
Desabilitar Bluetooth	Selecione para desativar os recursos Bluetooth.
Permitir apenas Bluetooth Audio	Selecione para ativar apenas os recursos de áudio do Bluetooth.
Desabilitar dados móveis	Selecione para desativar a troca de dados quando os dispositivos se encostarem. essa opção não poderá ser desabilitada se o Wi-Fi estiver desabilitado.
Desabilitar GPS	Selecione para desativar o GPS.
Desabilitar discador do telefone	Selecione para desativar o aplicativo do telefone.
Desabilitar cartão SD	Selecione desativar o acesso ao cartão SD.
Desabilitar backup do Google	Selecione para desativar backups dos servidores Google.
Desabilitar função copiar/colar	Selecione para desativar o acesso às funções copiar/colar.

Desabilitar NFC	Selecione para desativar a troca de dados NFC (Near-field Communication) quando o dispositivo encostar em outro dispositivo.
Desabilitar microfone	Selecione para desativar o acesso do aplicativo ao microfone do dispositivo.
Desabilitar captura de tela	Selecione para desativar o uso do recurso de captura de tela integrado do dispositivo. Ativar esta opção não permite capturas de tela do Go. Tais capturas de tela não são permitidas.
Desabilitar vínculo via Bluetooth	Selecione para desativar o vínculo via Bluetooth como uma opção para o uso da conexão de internet de um dispositivo para oferecer acesso a outro dispositivo.
Desabilitar depuração USB	Selecione para desativar o recurso de depuração USB.
Desabilitar vínculo via USB	Selecione para desativar o vínculo via USB como uma opção para o uso da conexão de internet de um dispositivo para oferecer acesso a outro dispositivo.
Desabilitar vínculo via Wi-Fi	Selecione para desativar o vínculo via Wi-Fi como uma opção para o uso da conexão de internet de um dispositivo para oferecer acesso a outro dispositivo.
Desabilitar navegador nativo	Selecione para impedir que os usuários acessem o navegador do Android.
Desabilitar YouTube	Selecione para impedir que os usuários acessem o YouTube.
Desabilitar reinicialização para configurações de fábrica	Selecione para impedir que os usuários redefinam as configurações de fábrica do dispositivo.
Desabilitar atualização OTA	Selecione para desativar as atualizações over-the-air do firmware do dispositivo. Aviso: não desabilite **Desabilitar alterações das configurações** se **Atualização OTA** estiver habilitado. **Desabilitar alterações de configuração** quando **Atualização OTA** está ativado pode resultar em um dispositivo não funcional, pois as alterações de configuração são necessárias para a atualização.

Desabilitar roaming de voz	Selecione para desativar o acesso às chamadas de voz enquanto o dispositivo estiver em roaming.
Desabilitar reprodutor de mídia USB	Selecione para desativar o reprodutor de mídia USB.
Desabilitar Google Play	Selecione para desativar o acesso ao Google Play.
Desabilitar roaming de dados	Selecione para desativar a troca de dados enquanto o dispositivo estiver em roaming.
Desativar fontes desconhecidas	Selecione para desativar a instalação de aplicativos de qualquer lugar, menos da Google Play Store, exceto para o aplicativo Go.
Desativar a remoção de privilégios do Administrador do Dispositivo	Selecione para proibir que os usuários desativem os privilégios de administrador do dispositivo do Go.
Desabilitar alterações das configurações	Selecione para desativar o acesso ao aplicativo de Configurações do dispositivo. Aviso: não desabilite **Desabilitar alterações das configurações** se **Atualização OTA** estiver habilitado. **Desabilitar alterações de configuração** quando **Atualização OTA** está ativado pode resultar em um dispositivo não funcional, pois as alterações de configuração são necessárias para a atualização.
Configurações do modo de quiosque: o modo de quiosque aplica mais restrições aos dispositivos, incluindo o acesso limitado aos aplicativos por meio de um iniciador personalizado.	
Aplicável às versões do Android até 8.1. Para as versões 9.0 do Android, use a configuração Quiosque em Dispositivo Gerenciado Android Enterprise.	
Ativar modo de quiosque	Selecione para configurar o Modo de quiosque em dispositivos Android.

Permitir acesso do usuário às configurações Wi-Fi	Selecionar para permitir que um usuário altere as configurações de Wi-Fi e acesse suas redes sem fio preferidas.
Permitir acesso do usuário às configurações do Bluetooth	Selecionar para permitir que um usuário altere as configurações de Bluetooth e emparelhe dispositivos Bluetooth adicionais.
Permitir que o usuário atrase as atualizações do aplicativo	Selecionar para permitir que um usuário atrase as atualizações do aplicativo.
Configurações de localização via GPS	Selecione uma das configurações de localização de GPS a seguir: • Desativar localização • Ativar localização • Permitir seleção pelo usuário
PIN para sair do modo de quiosque	Insira o código de quatro dígitos que o usuário final deve digitar para sair do modo de quiosque.
Criar uma lista de apps permitidos: esses apps estarão disponíveis para os usuários no Modo de quiosque adicionando apps na lista de apps permitidos. Arraste e solte para organizar os aplicativos na ordem em que devem aparecer no iniciador do Modo de quiosque. A adição de um aplicativo na lista de aplicativos permitidos não instala o aplicativo no dispositivo. Distribua os aplicativos para os usuários ou grupos de usuários adequados no Catálogo de aplicativos.	
Apps integrados	Clique em +Adicionar para incluir apps nativos listados no grupo de apps permitidos no modo de quiosque. se você desabilitou o Discador ou a Câmera nas Configurações de bloqueio acima, eles não poderão ser adicionados à Lista de aplicativos permitidos.

App Catalog	Clique em +Adicionar para incluir apps listados no app catalog no grupo de apps permitidos no modo de quiosque.
Outros apps	Clique em +Adicionar para incluir o nome do pacote de um aplicativo que não está disponível na Google Play Store.
Apps permitidos no modo de quiosque	Clique em X para remover um aplicativo do grupo de apps permitidos no modo de quiosque. Arraste e solte para alterar a ordem na qual os apps aparecem em dispositivos quiosque.

Usar o modo de quiosque no Android 4.4, ou em versões mais recentes com suporte ou dispositivos Samsung que comportam diversos usuários, bloqueará automaticamente o recurso de multiusuário.

Para obter mais informações, consulte Como criar uma configuração

Firewall do macOS

Licença: Gold

O firewall Mac OS gerencia as configurações de Firewall de aplicativo, localizadas no no painel Preferências de segurança nos dispositivos Mac OS.

Aplicável a: macOS 12.3+

- **Permitir que softwares internos recebam conexões de entrada** - se verdadeiro, permite que softwares internos recebam conexões de entrada.
- **Permitir que softwares assinados baixados recebam conexões de entrada** - se verdadeiro, permite que softwares assinados baixados recebam conexões de entrada.

Aplicável a: macOS 12.0+

- **Habilitar registro em log** - se verdadeiro, habilita o registro em log
- **Especificar o tipo de log**
  - **Limitar**
  - **Resumo**
  - **Detalhe**

Aplicável para: macOS 10.12+

Quando você clica em **Habilitar firewall**, é possível selecionar uma ou mais das opções a seguir:

- **Bloquear todas as entradas** - se verdadeiro, habilita o bloqueio de todas as conexões de entrada
- **Ativar modo furtivo** - se verdadeiro, ativa o modo furtivo
- **Aplicativos** - a lista de aplicativos com conexões controladas pelo firewall

- A configuração deve existir em um perfil com escopo do sistema. Se mais de um perfil tiver esta configuração, a união de configurações mais restrita será usada.
- As opções **Permitir softwares transferidos e assinados automaticamente** e **Permitir softwares integrados automaticamente** não são suportadas. No entanto, ambas as opções serão forçadas a serem habilitadas quando esta configuração estiver disponível.

- O Administrador pode ativar o modo furtivo especificando um dispositivo que não pode ser descoberto pelo comando ping.

Restrições do macOS

Licença: Gold

As restrições do macOS determinam quais restrições estão habilitadas em dispositivos macOS.

É possível configurar os seguintes recursos para que estejam habilitados ou não habilitados em dispositivos macOS:

Versão do macOS	Apenas
10.11+	• Permitir câmera • Permitir sincronização de documentos do iCloud **recursos supervisionados:** • Permitir Resultados da Internet no Spotlight
10.11.2+	Permitir consulta de definição
10.12+	• Permitir sincronização do conjunto de chaves do iCloud • Permitir Voltar ao Meu Mac • Permitir Buscar Mac • Permitir compartilhamento em Notas, Lembretes ou LinkedIn • Permitir sincronização de Favoritos • Permitir o serviço iCloud para correio do macOS • Permitir o serviço de Calendário do iCloud para macOS • Permitir o serviço de Agenda do iCloud para macOS • Permitir o serviço de lembrete do iCloud • Permitir desbloqueio automático **Somente supervisionado:** Permitir Apple Music

Versão do macOS	Apenas
10.12.4+	• Permitir desbloqueio com impressão digital
10.13+	• Permitir compartilhamento de arquivos do iTunes • Permitir cache de conteúdo • Permitir modificação de papel de parede **recursos supervisionados:** • Permitir AirPrint • Permitir descoberta de iBeacon no AirPrint • Forçar requisito de TLS confiável de AirPrint • Permitir AirDrop • Permitir Game Center
10.13.4+	**Somente supervisionado:** Adiar atualizações de software por um intervalo de tempo (30 a 90 dias) Padrão: 30 dias.
10.14+	**recursos supervisionados:** Permitir que dispositivos próximos compartilhem solicitações de senha

Versão do macOS	Apenas
10.14.4+	• Permitir capturas de tela • Permitir observação de tela remota **recursos supervisionados:** • Permitir a entrada automática na sala de aula • Permitir que a sala de aula solicite permissão para sair das aulas • Permitir que o Classroom bloqueie um aplicativo e o dispositivo sem aviso • Permitir forçar a observação não solicitada da tela de sala de aula gerenciada
11.0+	**Somente supervisionado:** Permitir forçar atraso das Atualizações de Software do Aplicativo
11.3+	Tempo limite de impressão digital aplicado **Padrão**: 48 horas **Pré-requisito**: o Touch ID deve ser configurado no dispositivo

Versão do macOS	Apenas
11.3+	**Somente supervisionado:** • Atraso de instalação diferida da atualização de software forçada do SO principal • Atraso de instalação diferida da atualização de software forçada do SO secundário • Atraso de instalação diferida da atualização de software forçada do não SO • Forçar atualizações de software principais atrasadas
12+	**Somente supervisionado:** • Permitir apagar conteúdo e configurações • **allowCloudPrivateRelay**: se você definir Retransmissão Privada ATIVA em um dispositivo macOS, o tráfego de rede será criptografado para que a atividade na internet seja privada e segura. Essa restrição requer um dispositivo supervisionado.
macOS 13.0+	

Versão do macOS	Apenas
	• **Permitir instalação do Rapid Security Response** - para desabilitar as respostas. O usuário não pode instalar respostas de segurança rápidas. • **Permitir remoção do Rapid Security Response** - para impedir que o usuário possa desfazer as respostas. O usuário não pode remover respostas de segurança rápidas. • **Permitir controle universal** - ◦ Se definida como Verdadeiro, a configuração permite que você use os dispositivos de entrada do dispositivo primário para controlar o dispositivo de exibição secundário. ◦ Se definida como Falso, você pode adicionar um dispositivo de exibição secundário, mas não pode controlá-lo com os dispositivos de entrada primários. • **Permitir instalação de perfil de configuração de IU** - se definida como Falso, a configuração não permite a instalação de perfil, configuração ou certificados no dispositivo macOS. • **Permitir modo restrito de USB** - se definida como Verdadeiro, a configuração impede o dispositivo de usar dispositivos de entrada conectados remotamente. As opções em Permitir Conexão de Acessórios ficam esmaecidas no dispositivo.

Restrições de Mac OS app Store

Licença: Gold

As Restrições da app Store do macOS definem quais recursos estão habilitados na app Store do macOS.

É possível configurar as seguintes opções:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Definição da configuração	
Versão do macOS	**Apenas**
10.9+	Restringir instalações de aplicativos a usuários administradores.
10.10+	• Restringir instalações de aplicativos somente para atualizações de software. • Desabilitar adoção de aplicativos por usuários. • Desabilitar notificações de atualização de software.
10.11+	Restringir instalação de aplicativos para aplicativos instalados de MDM e atualizações de software.

Distribuir configuração

Procedimento

1. Defina as opções usando a tabela anterior.
2. Clique em **Avançar**.
3. Selecione a opção **Habilitar essa configuração**.
4. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
5. Clique em **Concluído**.

Restrições de gravação de disco do Mac OS

Licença: Gold

As Restrições de Gravação de Disco do macOS gerenciam as restrições de gravação de disco no MacOS. Você pode definir as Configurações do Finder do macOS para ativar ou desativar as opções de gravação de disco do aplicativo Finder no macOS.

É possível configurar as seguintes opções:

Configuração	**O que fazer**
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Definição da configuração	
Configuração	**O que fazer**
Permitir gravação de disco	• LIGAR • DESLIGAR • Exigir autenticação

Distribuir configuração

Procedimento

1. Defina as opções usando a tabela anterior.
2. Clique em **Avançar**.
3. Selecione a opção **Habilitar essa configuração**.
4. Selecione uma das opções de distribuição a seguir:

- Todos os dispositivos
- Nenhum dispositivo (padrão)
- Personalizada

5. Clique em **Concluído** .

Controle de mídia permitido

Licença: Gold

A configuração de Controle de mídia permitido gerencia a montagem, desmontagem e ejeção no logout para diversas mídias físicas no Mac OS.

É possível configurar as seguintes opções:

<table>
<tr><th>Configuração</th><th>O que fazer</th></tr>
<tr><td>Nome</td><td>Insira um nome que identifique essa configuração.</td></tr>
<tr><td>Descrição</td><td>Insira uma descrição que esclareça o propósito dessa configuração.</td></tr>
<tr><td colspan="2">Definição da configuração</td></tr>
<tr><td>Controle de montagem para tipos de mídia</td><td></td></tr>
<tr><td colspan="2">Desligue o controle de montagem para cada tipo de mídia e defina as configurações de montagem. Se você desligar o controle de montagem, a configuração padrão do SO será aplicada.</td></tr>
<tr><td>Tipo de mídia</td><td>Configurações de montagem</td></tr>
<tr><td>• CD
• DVD
• BD</td><td>• Somente leitura com autenticação
• Negar montagem
• Ejetar mídia</td></tr>
<tr><td>• CD em branco
• DVD em branco
• BD em branco
• DVD-RAM
• Imagem de disco
• Disco rígido interno
• Disco rígido externo
• Disco de rede</td><td>• Somente leitura
• Negar montagem
• Ejetar mídia
• Autenticar</td></tr>
<tr><td colspan="2">• O disco rígido externo inclui USB HDD, armazenamento de unidade flash USB e cartões SD.
• Mídias de somente leitura, como CD, DVD e BD são montadas como somente leitura por padrão.</td></tr>
<tr><td colspan="2">Controle de desmontagem para tipos de mídia</td></tr>
</table>

<table>
<tr><th>Configuração</th><th>O que fazer</th></tr>
<tr><td colspan="2">Desligue o controle de desmontagem para cada tipo de mídia e defina as configurações de desmontagem. Se você desligar o controle de desmontagem, a configuração padrão do SO será aplicada. Tenha cuidado ao definir a configuração Negar desmontagem para tipos de mídia.</td></tr>
<tr><td>Tipo de mídia</td><td>Configurações de montagem</td></tr>
<tr><td>CD
DVD
BD
CD em branco
DVD em branco
BD em branco
DVD-RAM
Imagem de disco
Disco rígido interno
Disco rígido externo
Disco de rede</td><td>Negar desmontagem
Autenticar</td></tr>
<tr><td colspan="2">Configurações de ejetar no logout</td></tr>
</table>

Configuração	O que fazer
Tipos de mídia a serem automaticamente ejetados quando o usuário realiza o logout.	
Tipo de mídia	
• CD • DVD • BD • CD em branco • DVD em branco • BD em branco • DVD-RAM • Imagem de disco • Disco rígido externo • Disco de rede	

Distribuir configuração

Procedimento

1. Defina as opções usando a tabela anterior.
2. Clique em **Avançar**.
3. Selecione a opção **Habilitar essa configuração**.
4. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
5. Clique em **Concluído**.

Configurações do Finder do Mac OS

Licença: Gold

Configurações de gerenciamento do Finder do Mac OS do aplicativo Finder no Mac OS.

É possível configurar as seguintes opções:

Configuração	**O que fazer**
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Definição da configuração	
Configuração	**O que fazer**
Desativar suporte de gravação de disco no Finder	• LIGAR • DESLIGAR

Distribuir configuração

Procedimento

1. Defina as opções usando a tabela anterior.
2. Clique em **Avançar**.
3. Selecione a opção **Habilitar essa configuração**.
4. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizada
5. Clique em **Concluído** .

Política de extensão Kernel de macOS

Aplicável a: macOS 10.13.2 ou a versões mais recentes com suporte.

Controla restrições e configurações para carregar Extensões Kernel aprovadas pelo usuário.

Como criar uma configuração de Política de extensão Kernel de macOS

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **kernel** no campo de pesquisa e clique na configuração **Política de extensão Kernel de macOS**.
4. Nomeie e descreva a configuração.
5. Selecione a opção **Permitir substituições do usuário** para permitir que os usuários aprovem extensões de kernel adicionais não explicitamente permitidas pela seguinte configuração.
6. Na seção Identificadores de equipe permitidos e Extensões de kernel, clique em **+ Adicionar** para adicionar os identificadores de equipe e as extensões de kernel permitidos. Uma extensão de kernel é o identificador de pacote. Para cada identificador de equipe, você pode adicionar vários nomes de extensão de kernel assinados de modo válido na janela pop-up.
7. Clique em **Adicionar**.
8. Clique em **Avançar** para configurar as definições de distribuição.
9. Clique em **Concluído**.

Para obter mais informações, consulte Como criar uma configuração

Mobile@Work para macOS

Esta seção contém os seguintes tópicos:

- Configuração e fluxo de trabalho da execução de scripts do Mobile@Work para macOS
- Como criar uma configuração Mobile@Work para macOS
- Habilitação da integração de usuários para dispositivos macOS
- Como criar uma configuração Script do Mobile@Work para macOS
- "Execução de uma desinstalação limpa do Mobile@Work para macOS" na página 690

O Ivanti Neurons for MDM permite que você crie seus próprios scripts shell macOS, que você então pode carregar para o Ivanti Neurons for MDM e executar em dispositivos macOS gerenciados.Para informações sobre a criação, upload e gerenciamento de repositório de scripts, consulte Todos os scripts.

O usuário de um dispositivo macOS pode iniciar a desativação do dispositivo usando o Mobile@Work para macOS 1.1 ou posterior. Para acessar a opção de desativação, clique em **Desinstalar** na tela Sobre o Mobile@Work. No Ivanti Neurons for MDM, você pode verificar o status do dispositivo na página **Dispositivos** e na página de detalhes do dispositivo.

Mobile@Work para macOS 1.5 ou posterior abre o Apps@Work imediatamente após o registro sem esperar a conclusão do registro MDM.

No Mobile@Work para macOS, clique em um bloco de aplicativo para exibir a página Detalhes do aplicativo para esse aplicativo. A página inclui a descrição do aplicativo, capturas de tela, classificações e revisões.

O Mobile@Work para macOS notifica o servidor Ivanti Neurons for MDM no relatório de inventário se os aplicativos internos Packager para macOS estão instalados ou não instalados.

Pré-requisitos

No App Catalog, o cliente Mobile@Work para macOS está disponível como um aplicativo comercial. Antes de executar scripts shell em dispositivos macOS, instrua os usuários a registrar seus dispositivos no Ivanti Neurons for MDM usando o Mobile@Work para macOS.

Procedimento

1. Baixe o Mobile@Work para o aplicativo macOS. Está disponível como arquivo PKG em https://support.mobileiron.com/support/CDL.html. Consulte este artigo do fórum de clientes Ivanti para saber como obter credenciais para o site de download.
2. Carregue o arquivo PKG para Mobile@Work para macOS para um servidor seguro. Esse servidor deve estar acessível a usuários do dispositivo.
3. Compartilhe o URL do arquivo de instalação para o Mobile@Work para macOS com os usuários do dispositivo usando e-mail ou mensagem.
4. Instrua os usuários a:
    a. Baixar e instalar o Mobile@Work para macOS nos dispositivos.
    b. Registre os dispositivos no Ivanti Neurons for MDM usando o Mobile@Work para macOS.

Configuração e fluxo de trabalho da execução de scripts do Mobile@Work para macOS

Procedimento

1. Configure e distribua uma configuração Mobile@Work para macOS.
2. Defina e distribua uma configuração de script do Mobile@Work para macOS para carregar o script no Ivanti Neurons for MDM. Os scripts são criptografados e assinados usando um certificado assinado, que é exclusivo por locatário. A chave para descriptografar o script é enviada ao dispositivo junto com o URL de download para o script, que é criptografado e assinado.
3. O Ivanti Neurons for MDM executa os scripts em dispositivos macOS usando o Mobile@Work para macOS. O Mobile@Work para macOS sonda Ivanti Neurons for MDM periodicamente para verificar se há algum script aguardando execução. Se houver scripts na fila, o Mobile@Work baixará e executará os scripts em dispositivos macOS conforme as configurações definidas no Ivanti Neurons for MDM.
4. O Mobile@Work para macOS retorna os resultados da execução do script para Ivanti Neurons for MDM, que são mostrados nos registros do dispositivo. Você pode consultar os logs do dispositivo na página de detalhes do dispositivo macOS na guia **Logs**.

Como criar uma configuração Mobile@Work para macOS

Uma configuração de sistema padrão para a configuração do Mobile@Work para macOS está disponível. Porém, não é distribuída a nenhum dispositivo por padrão.

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **trabalho** no campo de pesquisa e, então, clique na configuração **Mobile@Work para macOS**.
4. Nomeie e descreva a configuração.
5. Insira **Tempo máx. de execução** em segundos para especificar por quanto tempo um script pode ser executado. O valor padrão é de 60 segundos.
6. Insira **Tamanho máx. da resposta** em kilobytes (KB) para especificar o limite de tamanho máximo da resposta da saída do script retornado para Ivanti Neurons for MDM. Esses são os dados stdout ou stderr retornados ao executar o script. O valor padrão é de 1 KB.
7. Insira a **Frequência de check-in** em minutos para especificar com que frequência o aplicativo Mobile@Work para macOS deve fazer check-in no Ivanti Neurons for MDM. O tempo padrão é 15 minutos.
8. (Opcional) Você pode habilitar a integração do usuário para dispositivos macOS usando a seção Habilitação da integração de usuários para dispositivos macOS.
9. Clique em **Avançar** para configurar as definições de distribuição.
    a. Escolha um nível de distribuição:
    b. **Para todos** – O aplicativo é adicionado a todos os dispositivos de usuário compatíveis.
    c. **Para ninguém** – O aplicativo é preparado para distribuição posteriormente.
    d. **Distribuição personalizada** – Selecione qualquer uma das opções a seguir:
        - **Usuário/Grupos de usuários** – O aplicativo é distribuído apenas para os usuários ou grupos de usuários que você escolher.
          Clique na guia **Usuários** para selecionar os usuários.
          Clique na guia **Grupos de usuários** para selecionar os grupos de usuários.
        - **Dispositivo/Grupos de dispositivos** – O aplicativo é distribuído apenas para os dispositivos ou grupos de dispositivos que você escolher
          Clique na guia **Dispositivos** para selecionar os dispositivos.
          Clique na guia **Grupos de dispositivos** para selecionar os grupos de dispositivos.

10. Clique em **Concluído**.

Habilitação da integração de usuários para dispositivos macOS

Você pode ativar a integração do usuário para dispositivos macOS durante o processo automatizado de registro de dispositivos da seguinte maneira:

- Assim que a inscrição do dispositivo é concluída, o Mobile@Work para macOS (versão 1.68 ou posterior) é transferido para o dispositivo juntamente com os perfis, configurações e aplicativos.
- O cliente Mobile@Work para macOS e outros apps são enviados aos dispositivos apenas se:
  - Os apps forem PKG internos ou públicos do Apple Apps and Books.
  - A configuração da instalação silenciosa para os apps for definida como verdadeira. A configuração está disponível na página **Apps** > Detalhes do aplicativo > **Configuração do aplicativo** > **Instalar no dispositivo**.
  - A prioridade para os apps é definida como Alta. Por padrão, a prioridade do aplicativo cliente Mobile@Work para macOS é definida como alta (e não pode ser modificada), **pois sem ela o processo de integração do usuário poderia falhar**.
  - Os apps são configurados para serem distribuídos aos dispositivos, grupos de usuários ou grupos de dispositivos.
- Após a instalação e registro do Mobile@Work para macOS, o dispositivo macOS entra no modo quiosque (o usuário não tem controle do dispositivo) até que os demais perfis, configurações e apps sejam configurados e instalados. O progresso é exibido em etapas.

Para Mobile@Work para macOS 1.73 ou versões posteriores se compatível com o Ivanti Neurons for MDM, os seguintes recursos adicionais são compatíveis:

- O processo de integração do usuário é concluído logo após a conclusão do Registro de dispositivo para um dispositivo. O processo de integração do usuário não iniciará após expirar a janela de tempo para disparar a integração do usuário (normalmente 20 minutos após o registro do dispositivo), mesmo se um administrador habilitar a integração do usuário na configuração do Mobile@Work. Isso impede que um dispositivo entre no modo de quiosque da integração de usuário quando o dispositivo estiver em uso normal.
- O processo de integração do usuário é exibido em etapas no cliente Mobile@Work para macOS. As configurações serão instaladas como parte da primeira etapa.

- Os apps de alta prioridade serão instalados inicialmente. Cada aplicativo de alta prioridade será contado como uma etapa. Os aplicativos Packager não contam como parte das etapas.
- Os apps restantes continuarão a ser instalados em segundo plano, mesmo após a conclusão da integração do usuário. Os aplicativos são marcados como instalados depois que a instalação é inicializada em um dispositivo ou depois que o aplicativo é de fato instalado no dispositivo.
- Após a integração do usuário, você pode ir para a página de detalhes do dispositivo para confirmar as configurações e apps enviados para cada dispositivo. Mais informações estão disponíveis nos registros.

Procedimento

1. Crie uma configuração Mobile@Work para macOS usando Como criar uma configuração Mobile@Work para macOS.
2. Selecione a opção **Habilitar integração do usuário**.
3. Forneça os seguintes detalhes:
   - **Valor do tempo limite de integração do usuário** – Insira o tempo aproximado que o dispositivo levará para instalar o aplicativo e as definições durante a configuração inicial. Por padrão, o processo de admissão do usuário em um dispositivo macOS se encerra em 120 segundos, o que você pode modificar conforme necessário.
   - **URL da página de aterrissagem do usuário** – Informe o URL da página inicial que o usuário verá ao final da integração.
4. Clique em **Avançar** para configurar as definições de distribuição.
5. Clique em **Concluído**.

Como criar uma configuração Script do Mobile@Work para macOS

Você pode criar e distribuir diversas configurações de script Mobile@Work para macOS para os dispositivos. Usando essa configuração, você pode selecionar um script do repositório (**Admin > Todos os scripts**) para distribuir para o Mobile@Work para macOS.

Você pode agendar execuções de script nos dispositivos com o Mobile@Work para macOS 1.66 ou versões posteriores. Se você agendar uma execução de script para dispositivos com versões do cliente do Mobile@Work para macOS anteriores a 1.66, então, o script é executado apenas uma vez. Se o cliente Mobile@Work para macOS for atualizado de 1.4 para 1.66, então, todas as configurações do cliente macOS serão redistribuídas para os dispositivos.

Pré-requisitos

- Acesse **Admin** > **Todos os scripts** para carregar e gerenciar scripts que podem ser usados nessa configuração e distribuídos para os dispositivos.
- Configure e distribua uma configuração do Mobile@Work para macOS nos dispositivos. Caso contrário, a configuração Script do Mobile@Work para macOS ficará no estado Erro.

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **trabalho** no campo de pesquisa e, então, clique na configuração **Script do Mobile@Work para macOS**.
4. Nomeie e descreva a configuração.
5. No campo **Selecionar script**, insira o nome do script para encontrar e selecionar o script na lista suspensa.
6. A seção Entrada de script exibe os rótulos de entrada de script e as variáveis de script associadas ao script. Se você precisar substituí-las, digite as variáveis de script alternativas (por exemplo, {$userWorkEmailAddress}) e os respectivos valores padrão alternativos (por exemplo, fulano@empresa.com).
7. Na seção Execução de script, selecione uma das opções de programação a seguir:
    - Executar uma vez na implementação
    - Execução recorrente

8. Se você escolher Execução recorrente, especifique os seguintes detalhes:
    - Fuso horário a ser usado (selecione a hora local do dispositivo ou UTC). O script será executado na hora selecionada nesse campo.
    - Começar execução em (selecione a data de início).
    - Terminar execução em (selecione a data de término que deve ser igual ou posterior à data de início).
    - Executar script (selecione Diariamente ou Semanalmente e insira a hora no formato de 24 h com minutos e dias se aplicável).
9. Clique em **Avançar** para configurar as definições de distribuição.
10. Clique em **Concluído**.

Execução de uma desinstalação limpa do Mobile@Work para macOS

Se você tiver habilitado a opção **Remover apps no cancelamento do registro(aplicável somente a apps gerenciados)** durante a instalação do Mobile@Work para macOS e iniciar o dispositivo a ser desativado a partir do portal administrativo do Ivanti Neurons for MDM, então, o aplicativo Mobile@Work para macOS e o script de desinstalação serão apenas excluídos do dispositivo. Para evitar que os processos e os scripts sejam executados no backend, assegure que, durante o registro de novos usuários ou a desativação de usuários existentes do dispositivo, você desmarque a opção a seguir no portal de administrador do Ivanti Neurons for MDM para assegurar que o script de desinstalação seja executado e exclua os processos e scripts associados do backend.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Apps** > **Mobile@Work** > **Configurações do aplicativo** > **Lista de resumo de configurações do aplicativo** > **Configurações do aplicativo Apple** >**Definições da configuração de gerenciamento do aplicativo Apple**.
3. Na página **Definições de configuração**, desmarque a opção a seguir:
    - **Remover apps em cancelamento do registro (aplicável somente a apps gerenciados)**.

Tópicos relacionados:

- Admin > Todos os scripts
- Como criar uma configuração

Configurações das regras de atualizações de software do macOS

Administradores podem configurar a política de atualização de software de um dispositivo definindo as "Regras de atualizações de software do MacOS" abaixo.

Aplicável para: macOS 10.7+

Procedure

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **macOS** no campo de pesquisa e clique na configuração **Configurações de atualizações de software do macOS**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Selecione as configurações necessárias das "Regras de atualizações de software do MacOS" abaixo.
5. Clique em **Avançar**.
6. Selecione a opção **Ativar esta configuração**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizado.
8. Clique em **Concluído**.

Regras de atualizações de software do MacOS

Administradores podem selecionar da lista de regras da seguinte maneira:

Usuários não podem alterar essas configurações quando essas regras forem aplicadas ao dispositivo.

- Permitindo instalação do software anterior ao lançamento.
- Automaticamente:
  - Verificar atualizações
  - Fazer download de novas atualizações quando estiverem disponíveis
  - Instalar atualizações do macOS
  - Instalar atualizações de aplicativo da app store
  - Instalar arquivos de dados do sistema e atualizações de segurança.
- Restringir instalações de aplicativos a usuários administradores.
- Opção de adicionar a URL do catálogo de atualizações do software (sem suporte para macOS 11+).

Preferência de certificado

Aplicável a: macOS 10.12 ou a versões mais recentes com suporte.

Identifique um item da Preferência de certificado no conjunto de chaves do usuário que faça referência a um Conteúdo de certificado incluído no mesmo perfil.

Essa configuração é utilizada para associar um certificado a um endereço de e-mail ou a uma URL. Após vincular um certificado a um endereço de e-mail, o aplicativo de e-mail o usará para essa conta. Se um Certificado SSL para um site não for confiável, adicionar uma preferência de certificado garantirá que o navegador não vai alertá-lo com uma mensagem de aviso quando você tentar acessar o site.

Criação de uma configuração de preferência de certificado

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **preferência** no campo de pesquisa e clique na configuração **Preferência de certificado**.
4. Nomeie e descreva a configuração.
5. Na seção de Configuração, no campo **Nome**, insira um nome ou ID de e-mail para o qual o certificado preferido é solicitado.
6. No campo **Certificado UUID**, selecione um certificado.
7. Clique em **Avançar** para configurar as definições de distribuição.
8. Clique em **Concluído**.

Tópicos relacionados:

- "Preferência de identidade" na página 700
- Como criar uma configuração

Active Directory (macOS)

Aplicável a: macOS 10.9 ou a versões mais recentes com suporte.

Configure opções avançadas para vincular dispositivos macOS a um domínio do Active Directory (AD) para acessar serviços de software que dependem do AD para autenticação e segurança.

Esta seção contém os seguintes tópicos:

- Criando uma configuração do Active Directory
- Configurações do Active Directory

Criando uma configuração do Active Directory

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **privacidade** no campo de pesquisa e clique na configuração **Active Directory**.
4. Nomeie e descreva a configuração.
5. Insira as configurações do Active Directory que constam na tabela a seguir.
6. Clique em **Avançar** para configurar as definições de distribuição.
7. Clique em **Concluído**.

Configurações do Active Directory

Configuração	O que fazer
Configurações do Active Directory – Básico	
Nome do host	(Obrigatório) Digite o nome do host, que é o domínio do Active Directory no qual entrar.
Nome de Usuário	Digite o nome de usuário da conta usada para entrar no domínio.
Senha	Digite a senha da conta usada para entrar no domínio.
Unidade organizacional do AD	Digite a unidade organizacional (OU) na qual o objeto do computador de entrada está adicionado.
Estilo de montagem do AD	Selecione uma das opções a seguir para indicar o protocolo de início de rede a ser usado: • AFP • SMB
Configurações do Active Directory – Avançado	
Habilitar a chave ADCreateMobileAccountAtLogin	Habilite ou desabilite a chave ADCreateMobileAccountAtLogin. Opção adicional: Crie a conta de dispositivo móvel no login.
Habilitar a chave ADWarnUserBeforeCreatingMA	Habilite ou desabilite a chave ADWarnUserBeforeCreatingMA. Opção adicional: Avise ao usuário antes de criar a conta de dispositivo móvel.

Habilitar a chave ADForceHomeLocal	Habilite ou desabilite a chave ADForceHomeLocal. Opção adicional: Force o diretório inicial local.
Habilitar a chave ADUseWindowsUNCPath	Habilite ou desabilite a chave ADUseWindowsUNCPath. Opção adicional: Use o caminho UNC do AD para derivar o local de origem da rede.
Habilitar a chave ADAllowMultiDomainAuth	Habilite ou desabilite a chave ADAllowMultiDomainAuth. Opção adicional: Permita a autenticação de qualquer domínio na floresta.
Shell do usuário padrão	Digite o shell padrão do usuário, como /bin/bash.
Mapeie o UID do usuário ao atributo	Selecione para mapear o UID do usuário ao atributo especificado.
Mapeie o GID do usuário ao atributo	Selecione para mapear o GID do usuário ao atributo especificado.
Mapeie GID do grupo ao atributo	Selecione para mapear o GID do grupo ao atributo especificado.
Servidor de domínio preferencial	Prefira este servidor de domínio.
Convenção de namespace	Selecione uma das seguintes convenções de nomenclatura de contas de usuário: • Domínio (padrão) • Floresta

Assinatura de pacote	Selecione uma das seguintes opções de assinatura de pacote: • Permitir (padrão) • Desativar • Exigir
Criptografia de pacote	Selecione uma das seguintes opções de criptografia de pacote: • Permitir (padrão) • Desativar • Exigir • SSL
Permita a administração por grupos especificados do Active Directory	Selecione para permitir administração por grupos especificados do Active Directory. Clique em **Adicionar** para adicionar um ou mais grupos.
Restrinja o DNS dinâmico	Selecione para restringir atualizações de DNS dinâmico nas interfaces especificadas (por exemplo, en0, en1, etc.). Clique em **Adicionar** para adicionar um ou mais nomes de interface.
Altere o intervalo de senha	Especifique a frequência (em dias) para exigir a troca da senha da conta de confiança do computador. O valor zero indica desabilitado.

Para obter mais informações, consulte Como criar uma configuração

Preferência de identidade

Aplicável a: macOS 10.12 ou a versões mais recentes com suporte.

Identifique um item de Preferência de identidade no conjunto de chaves do usuário que faça referência a um conteúdo de identidade incluído no mesmo perfil.

Em um dispositivo macOS, uma Preferência de identidade permite que você escolha a identidade (par chave-valor) que deseja usar com um site. Após ter pressionado uma Preferência de identidade (que consiste em URL e identidade) para o dispositivo, é possível vê-la listada em **Acesso do conjunto de chaves -> Todos os itens** (o "Tipo" será "Preferência de identidade"). Da próxima vez que tentar se conectar a essa URL pelo Safari, o dispositivo apresentará o certificado configurado.

Ivanti Neurons for MDM cria uma configuração de Preferência de identidade do sistema padrão com uma carga útil para a URL da App Store e o certificado para uso.

Ao acessar o App Catalog do macOS usando o Safari no macOS 10.12 e versões posteriores, será solicitada a senha do sistema ao usuário para armazenar o certificado de identidade em cache. Os usuários precisam selecionar "Permitir sempre" na primeira vez para evitar solicitações subsequentes ao acessar o App Catalog do macOS.

O Safari com uma versão do macOS anterior a 10.12 e outros navegadores mostrarão solicitações de senha do sistema e certificado ao acessar o App Catalog do macOS em uma nova sessão do navegador de dispositivos macOS.

Criação de uma configuração de preferência de identidade

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **preferência** no campo de pesquisa e clique na configuração **Preferência de identidade**.
4. Nomeie e descreva a configuração.
5. Na seção de Configuração, no campo **Nome**, insira um ID de e-mail, um nome de host DNS ou um nome que identifique o serviço de forma única.
6. No campo **Certificado UUID**, selecione um certificado.

7. Clique em **Avançar** para configurar as definições de distribuição.
8. Clique em **Concluído**.

Tópicos relacionados:

- "Preferência de certificado" na página 694
- Como criar uma configuração

Criação de conta automática do Office 365 (macOS)

Aplicável a:

- Dispositivos macOS com suporte.
- Versões recomendadas para apps do Microsoft Office 365: 16.13.x ou posteriores.

Configurar as informações e opções do usuário para definir a configuração inicial de todos os aplicativos do Microsoft Office 365.

Esta seção contém os seguintes tópicos:

- Como criar a configuração de Criação de conta automática do Office 365
- Configurações de Criação de conta automática do Office 365

Como criar a configuração de Criação de conta automática do Office 365

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **office** no campo de pesquisa e clique em **Criação de conta automática do Office 365**.
4. Nomeie e descreva a configuração.
5. Insira as configurações de Criação de conta automática do Office 365 que constam na tabela a seguir.
6. Clique em **Avançar** para configurar as definições de distribuição.
7. Clique em **Concluído**.

Configurações de Criação de conta automática do Office 365

Configuração	O que fazer
Endereço de email de ativação do Office	Insira o endereço de e-mail do usuário.
Entrada automática do Office	Selecione para ocultar janelas de primeira execução. Apenas solicita ao usuário informações necessárias, como a autenticação do O365.
Padrão para local Abrir/Salvar	Selecione para forçar a abrir/salvar painel em 'No meu Mac' em vez de 'Locais on-line'.
Mostre o que há de novo na inicialização	Selecione para exibir informações sobre novos recursos na inicialização.
Estado de execução de macros do Visual Basic	Selecione uma das opções a seguir: • Desativado com avisos • Desativado sem avisos • Ativado sem avisos
Desabilite dylibs externos do Visual Basic	Selecione para desabilitar dependências externas do Visual Basic.
Permitir que o Visual Basic associe o sistema	Selecione para permitir que macros usem DECLARE para vincular à API do SO system(). Esta API permite que macros executem processos externos arbitrários e passem dados arbitrários na linha de comando.
Desativar o Visual Basic para associar ao popen	Selecione para permitir que macros usem DECLARE para vincular à API do SO popen(). Esta API permite que macros executem processos externos arbitrários e passem dados arbitrários na linha de comando.
Desativar o Visual Basic Mac Script	Selecione para permitir que macros chamem a API de Visual Basic de script Apple.

Para obter mais informações, consulte Como criar uma configuração

Autenticar

Aplicável a:

- macOS 10.13 e versões mais recentes com suporte.
- Windows 10 e versões mais recentes com suporte.

Use a configuração do Authenticate para permitir a autenticação sem senha para os serviços em cloud e/ou login no desktop. Cada dispositivo terá apenas uma configuração do Authenticate.

Pré-requisitos

- A licença Zero Sign-On é obrigatória.
- O Ivanti Neurons for MDM deve ser registrado com o Access (o perfil do Access deve ser configurado).

- Depois de definir a configuração do Authenticate, você não pode cancelar o registro do perfil do Access, pois este será referenciado pela configuração do Authenticate.
- Se o perfil do Access tiver alguma alteração, redistribua a configuração do Authenticate para os dispositivos macOS. Para dispositivos Windows, copie e use os novos valores de CLI nos apps novos.

Criação de uma configuração do Authenticate

Procedure

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **auth** no campo de pesquisa e clique na configuração **Authenticate**.
4. Nomeie e descreva a configuração.
5. Na lista suspensa, selecione um **Certificado de identidade do desktop**.

6. Selecione uma ou ambas as opções de SO a seguir:
    - macOS
    - Windows
7. Para macOS:
    a. Na região de Dados personalizados, clique em **+Adicionar** para adicionar chaves e valores de sequências para os dados personalizados a serem obtidos dos dispositivos.
    b. Clique em **Avançar** para configurar as definições de distribuição.
    c. Clique em **Concluído**.
8. Para dispositivos Windows 10, esta configuração ajuda a gerar argumentos de linha de comando para o aplicativo MSI do Authenticator para Windows da seguinte maneira:
    a. Clique em **Concluído** para concluir a configuração do Authenticate.
    b. Na página **Configurações**, visualize a configuração do Authenticate para copiar o texto da linha de comando exibido. Este texto é necessário para distribuir o aplicativo Authenticate para dispositivos Windows.

Quando a configuração do Authenticate é aplicada a dispositivos Windows, a configuração permanece no estado de instalação pendente. Você pode ignorar isso, pois não haverá impacto na funcionalidade.

Para obter mais informações, consulte Como criar uma configuração

Catálogo de aplicativos da Apple

Aplicável para: iOS e macOS

A configuração do Catálogo de aplicativos da Apple gerencia o acesso ao Catálogo de aplicativos da Apple por meio de um clipe da web. A partir do Ivanti Neurons for MDM versão 83, você pode fazer a transição para a experiência nativa do Apps@Work pelo aplicativo Go. Para locatários recém-criados, a configuração do Webclip Apps@work não é distribuída por padrão aos dispositivos iOS instalados por meio do iReg ou do cliente. O administrador deve distribuir manualmente a configuração do webclip aos dispositivos registrados por meio do iReg ou do cliente.

Procedimento

Os administradores podem editar a distribuição dessa configuração definida pelo sistema da seguinte forma:

1. Vá até **Configurações**.
2. Clique no **App Catalog da Apple**.
3. Clique em **Editar distribuição**.
4. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos - Todos os dispositivos compatíveis receberão esta configuração.
    - Nenhum dispositivo - Desativa o acesso ao App Catalog da Apple ou programa essa configuração para uma distribuição posterior.
    - Personalizado - Define os grupos de dispositivos específicos que receberão esta configuração.
5. Clique em **Salvar**.

Domínios Gerenciados

Licença: Silver

Um domínio de configuração gerenciado permite que você especifique quais domínios são confiáveis para o Mail e o Safari em dispositivos iOS 8+. Assim que a configuração for aplicada ao dispositivo, os domínios que não estão especificados na configuração serão destacados (não confiáveis) no Mail e no Safari no dispositivo. Use essa configuração combinada com uma configuração de restrições para controlar os downloads de dados permitidos no Safari.

Configurações de domínios gerenciados

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Domínios de E-mail Gerenciados	Clique em **+Adicionar** para inserir um domínio, tal como minhaempresa.com.
Domínios de Web Gerenciados	Clique em **+Adicionar** para inserir um domínio, tal como minhaempresa.com.

Para obter mais informações, consulte Como criar uma configuração

Configuração da senha

Um dos primeiros recursos configurados no Ivanti Neurons for MDM (usando o assistente de inicialização) é a configuração da senha. Essa configuração define o recurso de bloqueio de tela nos dispositivos.

Configurações da senha

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Permitir valores simples	Restringe se o PIN ou a senha contém dígitos ou caracteres ordenados. **Para iOS e Android:** selecione para permitir pin ou senhas que sejam menos seguras, porque contêm sequências de caracteres repetidas, crescentes ou decrescentes. Exemplos: 1111, 1234, abcd. Desmarcar esta opção para dispositivos Android exigirá senhas com PINs complexos. Por exemplo: os usuários não podem configurar sequências de caracteres repetidos, crescentes ou decrescentes. **Para o Windows 10 Mobile:** selecione para permitir senhas menos seguras contendo sequências numéricas repetidas ou ascendentes. Exemplos: 1111, 1234

Exigir valor alfanumérico	Exige que a senha tenha pelo menos uma letra e um número. **Para iOS e Android**: selecione para garantir que as senhas incluam letras e números. **Para Windows 10 Mobile:** selecione para garantir uma senha forte baseada no padrão da Microsoft.
Tamanho mínimo da senha	Selecione um número da lista para definir um tamanho mínimo da senha. **Para Windows 10 Desktop**: as contas locais exigirão o tamanho mínimo de senha de 6.
Número mínimo de caracteres complexos	**Para iOS e Android**: selecione um número na lista para definir um número mínimo de caracteres que não sejam números ou letras. **Para o Windows 10 Mobile:** não compatível. **Para Windows 10 Desktop**: as contas locais exigirão três caracteres complexos.
Duração máxima da senha	Insira um número de dias após os quais o usuário do dispositivo deve reinicializar a senha. Se você não quiser definir uma duração para a senha, deixe esse campo em branco.
Bloqueio automático	Selecione um intervalo da lista para definir por quanto tempo o dispositivo pode permanecer inativo antes que a tela seja bloqueada automaticamente.

Qualquer método de bloqueio	**Apenas Android**. Permite que o usuário escolha qualquer método de bloqueio, incluindo o padrão de desbloqueio. As configurações de senha acima não serão aplicadas a esse dispositivo.
Histórico da senha	Insira um número para definir a quantidade de senhas exclusivas que um usuário deve inserir antes de reutilizar uma senha. Por exemplo, se você definir esse campo para 4, o usuário deve definir a senha 4 vezes antes de poder reutilizar a primeira senha.
Período de tolerância para bloqueio do dispositivo	Selecione um intervalo da lista para definir o tempo entre a exibição da tela de bloqueio e o ponto no qual o usuário do dispositivo precisará inserir a senha para desbloqueá-lo. **Windows 10 Mobile não suportado.**
Número máximo de tentativas com falha	Selecione um número da lista para definir quantas vezes o usuário do dispositivo pode inserir consecutivamente a senha errada antes que o dispositivo seja redefinido e apagado. **Aviso:** os dispositivos serão apagados se o usuário exceder o número máximo de tentativas de senha. Seja cauteloso ao usar essa opção.
(somente macOS) Aplicar regra de senha no próximo login	Selecione para permitir que o macOS solicite ao usuário que altere a senha de acordo com a política de senha no próximo login. Por padrão, esta opção não fica selecionada. Aplica-se ao macOS 10.13 e versões posteriores.

(somente macOS) Minutos até a redefinição de login com falha	Especifique quantos minutos até a redefinição do login após o número máximo de tentativas de login malsucedidas ser atingido. Certifique-se de que o valor em Número máximo de tentativas com falha esteja configurado para ativar esse campo. Disponível em macOS 10.10 e posteriores.
SmartLock	**Para dispositivos com Android 5.0, exceto em perfis de trabalho do Android corporativo:** **Para Android 6.0 ou mais recente:** Permite ou proíbe que um usuário selecione o recurso SmartLock para desbloquear um dispositivo. O recurso SmartLock desbloqueia automaticamente um dispositivo em determinadas circunstâncias, como a proximidade do usuário ao dispositivo, dispositivo em um local ou quando o dispositivo é emparelhado com um dispositivo confiável.
Desbloqueio por Impressão Digital	**Para dispositivos com Android 5.0, exceto em perfis de trabalho do Android corporativo:** **Para Android 6.0 ou mais recente:** Permite ou proíbe que o usuário selecione uma Impressão digital para desbloquear um dispositivo.

Notificações da tela de bloqueio (apenas para Android corporativo)	**Ativar as notificações para dispositivos gerenciados no trabalho (para Proprietário de dispositivo)** Permitir ou bloquear notificações na tela de bloqueio de dispositivos gerenciados de trabalho **Ativar notificações não alteradas para o perfil de trabalho** **Para Android 6.0 ou mais recente:** Permitir ou bloquear notificações não alteradas na tela de bloqueio para dispositivos de perfil de trabalho. Depois de ativar essa configuração, você receberá a notificação, mas o conteúdo será exibido como "Conteúdo ocultado pela política". O conteúdo (notificação por push/e-mail) só poderá ser visualizado no aplicativo.

Para obter mais informações, consulte Como criar uma configuração

Preferência de privacidade (macOS)

Aplicável a: macOS 10.14 ou a versões mais recentes com suporte.

Configure quais aplicativos têm permissão para obter acesso aos serviços do sistema, arquivos do sistema e recursos do sistema. Esta configuração controla as configurações em um dispositivo macOS em Preferências do sistema > Segurança e privacidade > Privacidade.

Como criar uma configuração de preferência de privacidade

Procedure

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **privacidade** no campo de pesquisa e clique na configuração **Preferência de privacidade**.
4. Nomeie e descreva a configuração.

5. Navegue até um dos aplicativos relacionados na página. Veja Documentação da Apple para informações relacionadas.

    a. Para o macOS 10.14+, os aplicativos e configurações disponíveis para configuração incluem:

        - Acessibilidade – especifica as políticas para o aplicativo por meio do subsistema Acessibilidade.
        - Catálogo de endereços – especifica as políticas para informações de contato gerenciadas pelo Contacts.app.
        - Eventos da Apple – especifica as políticas para o aplicativo enviar AppleEvents restritos para outro processo.
        - Calendário – especifica as políticas para informações de calendário gerenciadas pelo Calendar.app.
        - Câmera – uma câmera do sistema. O acesso à câmera não pode ser dado em um perfil; só pode ser negado.
        - Microfone – um microfone do sistema. O acesso ao microfone não pode ser concedido em um perfil; só pode ser negado.
        - Fotos – as imagens gerenciadas pelo aplicativo Fotos em ~/Pictures/.photoslibrary.
        - Pós-evento – especifica as políticas para o aplicativo usar APIs CoreGraphics para enviar CGEvents ao fluxo de eventos do sistema.
        - Lembretes – especifica as políticas para informações de lembretes gerenciadas pelo aplicativo Lembretes.
        - Política do sistema (todos os arquivos) – permite que o aplicativo acesse todos os arquivos protegidos, incluindo os arquivos de administração do sistema.
        - Política do sistema (arquivos do administrador) – permite que o aplicativo acesse alguns arquivos usados na administração do sistema.

b. Para o macOS 10.15+, os aplicativos e configurações disponíveis para configuração incluem:

- Uso de arquivos – Permite que um aplicativo Provedor de arquivos saiba quando o usuário está usando arquivos gerenciados pelo Provedor de arquivos.
- Ouvir evento de todos os processos – permite que o aplicativo use as APIs CoreGraphics e HID para ouvir (receber) eventos CGEvents e HID de todos os processos. O acesso a esses eventos não pode ser fornecido em um perfil; só pode ser negado. Desmarque a opção Permitido.
- Acessar biblioteca de mídia – permite que o aplicativo acesse o Apple Music, atividades de música e vídeo e biblioteca de mídia.
- Captura de tela da tela do sistema – Permite que o aplicativo capture (leia) o conteúdo da tela do sistema. O acesso ao conteúdo não pode ser concedido em um perfil; só pode ser negado. Desmarque a opção Permitido.
- Reconhecer e enviar dados de fala para a Apple – Permite que o aplicativo use o recurso Reconhecimento de fala do sistema e envie dados de fala para a Apple.
- Acessar arquivos na pasta Área de trabalho do usuário – Permite que o aplicativo acesse arquivos na pasta Área de trabalho do usuário.
- Acessar arquivos na pasta Documentos do usuário – Permite que o aplicativo acesse arquivos na pasta Documentos do usuário.
- Acessar arquivos na pasta Downloads do usuário – Permite que o aplicativo acesse arquivos na pasta Downloads do usuário.
- Acessar arquivos em volumes de rede – Permite que o aplicativo acesse arquivos em volumes de rede.
- Acessar arquivos em volumes removíveis – Permite que o aplicativo acesse arquivos em volumes removíveis.

6. Para cada aplicativo que você deseja configurar, clique em **Ações > Adicionar**.

7. Digite os valores das seguintes chaves de dicionário de identidade:
    - Identificador – Nome das configurações. Por exemplo: "us.zoom.ZoomPresence."
    - Tipo de identificador – selecione ID do pacote ou Caminho. Por exemplo: "ID do pacote".
    - Requisito de código – especifique o valor para ID do pacote ou Caminho. Por exemplo: "identifier "us.zoom.ZoomPresence" and anchor apple generic."
    - Código estático (verdadeiro ou falso)
    - Permitido (verdadeiro ou falso)
    - Comentar
8. Clique em **Salvar**.
9. (Opcional) Em qualquer aplicativo, clique em **Ações > Excluir** para remover configurações de preferência de privacidade.
10. Clique em **Avançar** para configurar as definições de distribuição.
11. Clique em **Concluído**.

Para obter mais informações, consulte Como criar uma configuração

Privacidade do cliente

Configure para coletar dados anônimos de usuários finais, incluindo informações sobre dispositivo e uso, que permitirão que problemas do produto sejam identificados e que a alta qualidade dos serviços seja mantida.

Aplicável a:

- Mobile@Work para macOS 1.67 ou versões mais recentes com suporte.
- Go para iOS 3.5.0 ou versões mais recentes com suporte.

Como criar uma configuração de privacidade de cliente MI

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **privacidade** no campo de pesquisa e clique na configuração **Privacidade do cliente**.
4. Nomeie e descreva a configuração.
5. Em Ativações com base no local, selecione a opção **Ativar SLC**. O serviço de localização com alteração significativa oferece uma alternativa mais econômica em termos de consumo de energia para distribuir atualizações de localização ao aplicativo Go para iOS somente quando a posição do usuário mudar em um valor significativo, após o mínimo de 15 minutos (intervalo padrão). Se esse serviço for ativado, quando houver uma alteração de localização, o aplicativo Go despertará no segundo plano e fará o registro.
6. Em Coleta de dados via MixPanel, selecione a opção **Ativar status do MixPanel**, se estiver desativada. Por padrão, essa opção está habilitada.
7. Clique em **Avançar** para configurar as definições de distribuição.
8. Clique em **Concluído**.

Para obter mais informações, consulte Como criar uma configuração

Configuração de privacidade

Uma configuração de privacidade define se:

- os dados de localização são coletados no dispositivo e enviados para o sistema de gerenciamento de dispositivo
- de gerenciamento podem apagar o dispositivo
- o inventário de aplicativos é coletado em relação a todos os aplicativos ou somente em relação aos que aparecem no catálogo de aplicativos

Configurações de privacidade

A ação de apagamento do dispositivo e a coleta de inventário de todos os aplicativos no dispositivo não são aplicáveis aos dispositivos registrados pelo usuário.

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Coletar dados de localização	Selecione para habilitar a coleta de dados de localização. Visualize a localização do dispositivo na página **Dispositivos**. • Para dispositivos iOS, o local exibido para um dispositivo é baseado apenas na localização da rede. • Para dispositivos Android, a localização é baseada na localização da rede e do GPS (se disponível). • Em dispositivos Windows, a localização é baseada nos valores de latitude e longitude obtidos durante o check-in do dispositivo. Quando o conjunto de localização estiver disponível em um dispositivo, a localização atual é atualizada a cada 4 horas. Os dados de localização são removidos do sistema de gerenciamento do dispositivo quando o dispositivo é desativado ou a configuração de privacidade é desabilitada ou removida. Os usuários do dispositivo podem desativar a coleta de dados de localização no dispositivo.

Desativar Ação apagar dispositivo	Selecione para evitar que os administradores apaguem o dispositivo. Considere a possibilidade de selecionar essa opção para os dispositivos que são de propriedade do usuário (propriedade do funcionário).
Solicitar ao usuário para ativar os serviços de localização	Selecione para permitir que os usuários ativem opcionalmente a capacidade de permitir ou não o uso de serviços de localização, incluindo localização de dispositivos, Wi-Fi e MTD, conforme necessário. No caso de dispositivos totalmente gerenciados, isso pode ser concedido automaticamente se o administrador optar por desabilitar a opção.

Coletar inventário de aplicativo	Selecione **Coletar Inventário de Aplicativos** para coletar informações sobre todos os aplicativos instalados no dispositivo, independentemente de estarem no catálogo de aplicativos ou não. Selecione **Para aplicativos no dispositivo que estejam no Catálogo de Aplicativos** para coletar informações apenas sobre os aplicativos instalados no dispositivo e presentes no catálogo de aplicativos. Selecione **Para todos os apps no dispositivo** para coletar informações sobre todos os apps no dispositivo. Essa opção é aplicável a dispositivos Windows 10+. Os seguintes inventários do tipo de fonte do aplicativo são exibidos e selecionados por padrão. • **Ativar inventário fora da App Store** - para aplicativos internos (aplicativos universais) enviados pelo MDM ou instalados pelo usuário final diretamente no dispositivo ao descompactar manualmente o aplicativo e instalá-lo localmente. • **Ativar inventário da App Store** - para aplicativos instalados da Microsoft Store manualmente ou via frente de loja Apps@work. • **Ativar inventário do sistema** - para os aplicativos relatados como pré-instalados junto com o SO Windows 10 da Microsoft.

	• **Ativar inventário Win32** - para o sistema, aplicativos baseados em 32, como MSI, EXE, etc., instalados por meio do MDM ou diretamente no dispositivo pelo usuário final. Você também pode selecionar apenas os inventários do tipo de fonte do aplicativo para coletar informações sobre aplicativos seletivos. Os aplicativos instalados do MDM serão mostrados no Inventário de aplicativo, mesmo que não da App Store ou caso o inventário Win32 não esteja selecionado. O inventário de .EXEs também é coletado quando a configuração de privacidade estiver usando a configuração padrão para coletar o inventário de aplicativos apenas para o App Catalog. O inventário deve ser coletado consistentemente para todos os aplicativos durante a coleta apenas de aplicativos do App Catalog. O inventário de aplicativos modernos, MSI e EXE disponíveis no App Catalog; será puxado apenas quando pelo menos um aplicativo pertencente a cada uma dessas variantes for distribuído.

Configurações para dispositivos Android Enterprise (7.0+)	
Configure as definições abaixo para estabelecer a política de privacidade para dispositivos Android Enterprise.	
Nome da organização	Insira o nome da organização que gerencia o dispositivo.
Cor da organização	Selecione a cor da organização que pode ser exibida no plano de fundo da tela do usuário.
Mensagem curta	Insira uma mensagem curta para ser exibida quando o usuário tentar usar uma função que foi bloqueada pelo administrador.
Mensagem longa	Insira uma mensagem longa que deve ser exibida quando o usuário clicar na mensagem curta. Essa mensagem oferece mais detalhes sobre a restrição fornecida para o usuário.

Para obter mais informações, consulte Como criar uma configuração

Informações de declaração de privacidade do cliente

Aplicável a: Android, Android Enterprise e dispositivos iOS, ou versões mais recentes com suporte.

Configuração para distribuir a Informação de política de privacidade para os usuáriosno Go client. Essa é uma configuração definida pelo sistema que pode ser editada para configurar apenas as configurações de distribuição.

As informações exibidas para o usuário incluem os detalhes configurados como parte das seguintes configurações:

- Privacidade
  - Coletar dados de localização
  - Coletar inventário de aplicativo
  - Android 7.0 +
    - Nome da organização
    - Cor da organização
    - Mensagem curta
    - Mensagem longa
- Privacidade do cliente
  - SLC – Mudança significativa de local para acionar periodicamente o dispositivo
  - Intervalo mínimo de acionamento com base em localização
  - Ativar status do MixPanel
- Direitos de acesso ao Gerenciamento de dispositivo móvel (MDM) (não aplicável a dispositivos registrados pelo usuário)
  - Bloqueio de dispositivo e remoção de senha
  - Apagamento do dispositivo
  - Informações de rede (números de telefone/SIM, endereços MAC)

Atualizações de software

Aplicável a:

- Dispositivos supervisionados iOS 10.3+ e tvOS 12.0+
- Dispositivos macOS
- Dispositivos Windows 10+

  Crie e distribua regras para atualizações de SO.

  Esta seção contém os seguintes tópicos:

  - Configurar atualizações de software para dispositivos iOS/tvOS
  - Configurar atualizações de software para dispositivos macOS DEP e não DEP
  - Configurar atualizações de software para dispositivos Windows

Configurar atualizações de software para dispositivos iOS/tvOS

Procedimento

Para permitir que os dispositivos iOS/tvOS recebam atualizações de OS eles devem estar no modo supervisionado:

1. Vá até **Configurações**.
2. Clique em **+ Adicionar**.
3. Clique em **Atualizações de software**.
4. Clique em **iOS/tvOS** para visualizar a seção Definição de configuração.
5. Selecione a opção **Permitir que atualizações de SO sejam instaladas automaticamente em dispositivos supervisionados**.
6. Selecione uma das opções a seguir:
   - Atualizar para a versão mais recente
   - Atualize para a versão específica, por exemplo, insira o número da versão iOS como 11.3.0.

7. Selecione uma das ações de instalação a seguir:
    - Padrão
    - Somente download
    - Instalar ASAP
8. Selecione as seguintes opções de tempo para que as atualizações:
    - Horário de início
    - Horário de término
    - Fuso horário
9. Clique em **Avançar**.
10. Selecione a opção **Habilitar essa configuração**.
11. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizada
12. Clique em **Concluído** .

- Ao instalar uma versão específica de atualização de SO para dispositivos iOS, você deve selecionar uma versão que esteja disponível para o dispositivo. Se você selecionar uma versão inválida ou não disponível, a atualização de software do dispositivo será ignorada.
- Se o dispositivo tiver uma senha, depois que o MDM enviar a atualização para o dispositivo, o dispositivo colocará a atualização na fila e o usuário será solicitado a inserir sua senha para iniciar a instalação.
- Habilite `enforcedSoftwareUpdateDelay` em "Restrições do iOS" na página 584 para garantir que a verificação manual para atualizações de software nos dispositivos não exclua as versões específicas baixadas por esta configuração.

Configurar atualizações de software para dispositivos macOS DEP e não DEP

O perfil de registro de dispositivo faz parte do Apple Business Manager, que permite aos clientes comprar dispositivos em massa e registrá-los automaticamente no MDM durante a ativação. Para mais informações, consulte "Registro de dispositivos" na página 1278.

O procedimento a seguir ajuda a enviar atualizações de SO para dispositivos macOS DEP e não DEP.

Procedimento

1. Vá até **Configurações**.
2. Clique em **+ Adicionar**.
3. Clique em **Atualizações de software**.
4. Clique em **macOS** para visualizar a seção Definição de configuração.
5. Selecione a opção **Ativar atualizações de software do macOS**.

6. Selecione o tipo de atualizações para o dispositivo. Para cada uma dessas atualizações, você também pode selecionar atualizações que não exigem reinicialização.
    - Atualizações de SO
    - Atualizações críticas
    - Atualizações dos dados de configuração
    - Atualizações de firmware

- Atualizações não críticas

> O administrador pode gerenciar (instalar/agendar) atualizações do macOS não críticas habilitando a opção **Habilitar atualizações não críticas**. Esta opção é desabilitada por padrão para os locatários existentes e precisa ser habilitada pelo administrador explicitamente após a atualização, se necessário.

> Em **Atualizações do SO**, os administradores podem atualizar o dispositivo para uma versão específica do macOS.

> Todas as atualizações do macOS podem ser configuradas conforme as ações a seguir:
>
> - Padrão
> - Notificação apenas
> - Instalar depois
> - Reinício forçado após a instalação
> - Somente download
> - Instalar ASAP

- Prioridade
  Padrão - Baixa
  Valores possíveis: Baixa, Alta
- Máximo de diferimentos do usuário
  Valor possível: inteiro
  Suportado apenas se a opção Instalar Depois estiver selecionada.

7. Selecione as seguintes opções de tempo para que as atualizações:
   - Horário de início
   - Horário de término
   - Fuso horário
8. Clique em **Avançar**.

9. Selecione a opção **Habilitar essa configuração**.
10. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizada
11. Clique em **Concluído** .

Configurar atualizações de software para dispositivos Windows

Procedimento

Para configurar seu planejamento de atualização da instalação do Windows:

1. Vá até **Configurações**.
2. Clique em **+ Adicionar**.
3. Clique em **Atualizações de software**.
4. Clique em **Windows** para visualizar a seção Definição de configuração.
5. Insira as seguintes opções, dependendo da versão dos seus dispositivos Windows.
6. Clique em **Avançar**.
7. Selecione a opção **Habilitar essa configuração**.
8. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizada
9. Clique em **Concluído** .

Atualizações de software para dispositivos Windows 10 ou superior

- Fontes de atualização – Selecione uma das fontes a seguir:
  - WSUS Corporativo
  - Microsoft Update e/ou Enterprise WSUS
- URL para Servidor Enterprise WSUS
- Servidor alternativo de atualização da Microsoft na intranet
- Permitir atualizações de "Fornecedores confiáveis" – Limite as fontes de atualização apenas aos fornecedores confiáveis.
- Estratégia de atualização automática – Selecione uma das opções no menu suspenso.
- Dia de instalação planejado – Defina a frequência das atualizações.
- Hora de instalação planejada – Selecione uma hora de instalação para as atualizações.
- Permitir o download automático de atualizações em conexões limitadas – Ative ou desative a opção.
- Não permitir que políticas de adiamento de atualização realizem verificações no Windows Update – Ative ou desative a opção.
- Prazo de reinício engajado – Selecione o número de dias para reiniciar o prazo.
- Prazo de adiamento de reinício engajado – Selecione o número de dias para adiamento do prazo de reinício engajado.
- Programação de transição de reinício engajado – Selecione o número de dias para reiniciar a programação de transição.
- Atualizar/preencher URLs de conteúdo vazio.
- Limite de download de aplicativo MO – Selecione uma das opções a seguir:
  - Não ignorar o limite de downloads de MO para apps e suas atualizações
  - Ignorar o limite de download de MO (permitir download ilimitado) para apps e suas atualizações

- Limite de download de atualização MO – Selecione uma das opções a seguir:
  - Não ignorar o limite de downloads de MO para atualizações do SO
  - Ignorar o limite de download de MO (permitir download ilimitado) para atualizações de SO
- Gerenciar versões de prévia – Selecione uma das opções a seguir:
  - Desativar versões de prévia
  - Desativar versões de prévia quando a versão seguinte for liberada ao público
  - Ativar versões de prévia
- Reiniciar automaticamente a programação de notificações de aviso para atualizações – Selecione os minutos até reiniciar automaticamente a notificação de aviso.
- Lembrete de aviso de reinicialização – Selecione as horas para definir o lembrete de aviso de reinicialização.
- Programação de atualização automática – Selecione a frequência das atualizações automáticas.
- Reiniciar automaticamente a notificação de atualizações – Ative o reinício automático de notificações de atualizações.

Atualizações de software para dispositivos anteriores ao Windows 10.0.14393

As configurações a seguir não funcionarão se a opção Restrição de telemetria estiver desabilitada em um dispositivo:

- Pausar upgrades/atualizações – Ative para adiar as mudanças até uma data posterior.
- Adiar atualizações por – Escolha para adiar por até 4 semanas.
- Adiar upgrades – Ative para adiar upgrades.
- Adiar upgrades por – Escolha para adiar por até 8 meses.

Atualizações de software para dispositivos Windows com a versão 10.0.14393 ou superior

- Ramificação a partir da qual instalar as atualizações – Permite que o administrador de TI defina de qual ramificação um dispositivo recebe suas atualizações.

    - Ramificação atual
    - Ramificação corporativa atual
- Atualizações (upgrades) de recursos – Suportado somente no Windows 10 Professional, Windows 10 Enterprise e Windows 10 Education.
    - Pausar atualizações
    - Adiar por – Escolha para adiar por até 180 dias.
- Atualizações de qualidade – Suportado somente no Windows 10 Professional, Windows 10 Enterprise, Windows 10 Education e Windows 10 Mobile Enterprise.
    - Pausar atualizações
    - Adiar por – Escolha para adiar por até 30 dias.

Atualizações de software para dispositivos Windows versão 10.0.17083+

- Atualizações de recurso:
    - Período de desinstalação de atualização de recurso – Selecione o número de dias de prazo para desinstalação de uma atualização de recurso.

Atualizações de software para dispositivos Windows 10.0.17763+

- Desativar acesso de usuários a "Pausar atualizações"
- Desativar o acesso de usuários a UXWU (Windows Update Scan, download e instalação)
- Nível de notificação de atualização – Selecione uma das opções a seguir:
    - Usar as notificações padrão do Windows Update
    - Desativar todas as notificações, excluindo avisos de reinicialização
    - Desativar todas as notificações, incluindo avisos de reinicialização

- Atualizações de recurso:
  - Prazo para reinício automático de instalação de atualizações – Selecione o número de dias do prazo para reiniciar automaticamente a instalação de atualizações.
  - Prazo de reinício engajado – Selecione o número de dias do prazo de reinício engajado.
  - Prazo de adiamento de reinício engajado – Selecione o número de dias para adiamento do prazo de reinício engajado.
  - Programação de transição de reinício engajado – Selecione o número de dias para reiniciar a programação de transição.

Configuração de preferências de segurança

Os administradores podem gerenciar e controlar as mudanças de usuários de configurações de firewall, bloqueio de mensagens e alterações de senhas no dispositivo com a Configuração de preferências de segurança.

Aplicável para: macOS 10.10+

Procedure

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **Segurança** no campo de pesquisa e clique na configuração **Preferências de segurança**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Selecione as configurações necessárias:
    - Desativar alterações nas configurações de firewall
    - Desativar alterações na mensagem de bloqueio
    - Desativar alterações na senha
5. Clique em **Avançar**.
6. Selecione a opção **Ativar esta configuração**.
7. Selecione uma das seguintes opções de canal para aplicar a configuração:
    - Canal do dispositivo (mais comum)
    - Canal do usuário (usuário atualmente registrado)
8. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizado.
9. Clique em **Concluído**.

Servidor de tempo

Aplicável a: macOS 10.12.4 e a versões mais recentes com suporte.

Criar a configuração de servidor de tempo para permitir que os dispositivos se conectem aos servidores de tempo personalizados.

Criar uma configuração do Servidor de tempo

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **tempo** no campo de pesquisa e, então, clique na configuração **Servidor de tempo**.
4. Digite um nome e descreva a configuração.
5. Especifique **Servidor NTP**.
6. Especifique a string **Fuso horário** no formato de ID de fuso horário Olson (por exemplo, Pacífico/Midway). Para obter o formato de fuso horário Olson, execute o comando "`/usr/sbin/systemsetup -listtimezones`" no dispositivo macOS do administrador.
7. Clique em **Avançar** para configurar as definições de distribuição.
8. Clique em **Concluído**.

Para obter mais informações, consulte Como criar uma configuração

Filtro de conteúdo da Web

Licença: Silver

Uma configuração de filtro de conteúdo da web limita o acesso a dispositivos iOS 7+.

Configurações do filtro de conteúdo da Web

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Sites permitidos	**Conteúdo adulto limitado:** selecione esta opção se quiser bloquear o acesso a sites com base nos filtros automáticos do iOS. Esses filtros tentam, com alto nível de precisão, bloquear sites com conteúdo impróprio. **Somente sites específicos:** selecione esta opção se quiser listar manualmente os sites acessíveis. **Plug-in (somente iOS8 supervisionado):** selecione esta opção para usar um plug-in de terceiros.

URLs permitidas	Essa opção estará disponível somente se você selecionou Limitar conteúdo adulto. Insira as URLs permitidas. Cada URL deve começar com: • http:// • https:// Se quiser permitir tanto http:// quanto https:// para o mesmo site, inclua duas URLs separadas. Todas as URLs com os caracteres iniciais correspondendo com a URL permitida são acessíveis. Por exemplo: http://www.algumsitedeempresa.com permite o acesso ao seguinte: • http://www.algumsitedeempresa.com • http://www.algumsitedeempresa.com/trabalhos Essas URLs estarão disponíveis mesmo se os filtros automáticos do iOS as bloquearem.

Usar URLs da lista de negações	Essa opção estará disponível somente se você selecionou Limitar conteúdo adulto. Insira os URLs bloqueados. Cada URL deve começar com: • http:// • https:// Se você quiser bloquear tanto http:// quanto https:// para o mesmo site, inclua uma linha para cada URL. Todas os URLs com os caracteres iniciais correspondendo ao URL bloqueado serão bloqueados. Por exemplo: http://www.algumsitedeempresa.com bloqueia o acesso ao seguinte: • http://www.algumsitedeempresa.com • http://www.algumsitedeempresa.com/trabalhos Essas URLs estarão bloqueadas mesmo se os filtros automáticos do iOS as bloquearem.
Marcadores permitidos	Esta opção está disponível apenas se você selecionou Somente Sites Específicos. Opcionalmente, insira a pasta em que o indicador deve ser adicionado no Safari. Por exemplo: /Vendas/Produtos/ Se ela não existir, o indicador será adicionado ao diretório de marcadores padrão.

Filtrar Nome	Esta opção está disponível apenas se você selecionou Plug-in. Insira o texto que será exibido para identificar esse filtro.
Identificador	Esta opção está disponível apenas se você selecionou Plug-in. Insira o ID do pacote do plug-in fornecendo o serviço de filtragem.
Endereço de Serviço	Esta opção está disponível apenas se você selecionou Plug-in. Opcional: Insira qualquer endereço de servidor necessário para uso pelo plug-in. Consulte a documentação para que o plug-in determine se esse valor é necessário.
Organização	Esta opção está disponível apenas se você selecionou Plug-in. Opcional: Insira qualquer cadeia de organização necessária pelo plug-in. Consulte a documentação para que o plug-in determine se esse valor é necessário.

Nome de Usuário	Esta opção está disponível apenas se você selecionou Plug-in. Opcional: Insira qualquer nome de usuário necessário pelo serviço de plug-in. Consulte a documentação para que o plug-in determine se esse valor é necessário.
Senha	Esta opção está disponível apenas se você selecionou Plug-in. Opcional: Insira qualquer senha necessária pelo serviço de plug-in. Consulte a documentação para que o plug-in determine se esse valor é necessário.
Certificado	Esta opção está disponível apenas se você selecionou Plug-in. Opcional: Insira qualquer certificado necessário pelo serviço de plug-in para que ele faça a autenticação do usuário. Consulte a documentação para que o plug-in determine se esse valor é necessário.

Filtrar Tráfego Webkit	Esta opção está disponível apenas se você selecionou Plug-in. Selecione para incluir tráfego Webkit no filtro.
Filtrar Tráfego Socket	Esta opção está disponível apenas se você selecionou Plug-in. Selecione para incluir tráfego Socket no filtro.
Dados personalizados	Esta opção está disponível apenas se você selecionou Plug-in. Opcional: Adicione qualquer pare de valor/chave necessária pelo serviço de plug-in. Consulte a documentação para que o plug-in determine se esse valor é necessário.

Para obter mais informações, consulte Como criar uma configuração.

Firewall do Windows

A configuração do Firewall do Windows permite ajustar as configurações do perfil de firewall do Windows, bem como o conjunto desejado de regras personalizadas a serem aplicadas no dispositivo. Essa configuração pode ser usada para gerenciar dispositivos não de domínio e reduzir o risco de ameaças à segurança da rede em todos os sistemas conectados à rede corporativa.

Definir a configuração do Firewall do Windows

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Firewall**.
3. Clique no ícone do **Windows**.
4. Insira um nome para a configuração.
5. Insira uma descrição para a configuração do firewall.

6. Na seção Definições de Configuração, especifique as configurações restantes conforme descrito na tabela a seguir.

Configuração	O que fazer
Perfis	
Ativar	Deslize o botão para ON para ativar o perfil.
Tipo	Exibe o tipo de perfil. Exemplo: domínio.
Ação padrão de entrada	Selecione uma opção para uma ação padrão que deva ser realizada no tráfego de entrada. **Permitir**: para permitir o tráfego **Bloquear**: para bloquear o tráfego.
Ação padrão de saída	Selecione a ação padrão que deve ser realizada em tráfego de saída. **Permitir**: para permitir o tráfego **Bloquear**: para bloquear o tráfego.

7. Para adicionar Regras, clique em **+Adicionar** e defina as seguintes configurações:

Configuração	O que fazer
Regras	
LIGAR	Deslize o botão para ativar o perfil.
Nome da regra	Insira um nome que identifique essa regra.
Descrição	Insira uma descrição que esclareça o objetivo dessa regra.
Direção	Selecione a direção do tráfego à qual a regra deve ser aplicada: • **Entrada**: para o tráfego de entrada • **Saída**: para tráfego de saída • **Ambas**: ambas as direções.
Ação	Selecione a ação a ser realizada • **Permitir**: para permitir o tráfego • **Bloquear**: para bloquear o tráfego.
Perfil	Selecione os perfis aos quais a regra deve ser aplicada: • **Todos** • **Domínio** • **Privado** • **Público**
Aplicativo	Digite o nome da família do pacote (PFN) ou caminho completo para o executável do aplicativo.

Configuração	O que fazer
Protocolo	Selecione qualquer um dos protocolos a seguir ao qual a regra deva ser aplicada: • **TCP** • **UDP** • **ICMP**
Intervalos de endereço local	Digite os intervalos de endereço IPv4/IPv6 locais ou máscaras de sub-rede.
Intervalos de porta local	Digite uma lista separada por vírgulas de portas ou intervalos de portas remotas. Exemplo: 20,50,100-120.

Configuração	O que fazer
Intervalos de endereço remoto	Digite os intervalos de endereço IPv4/IPv6 remotos ou máscaras de sub-rede.
Intervalos de porta remota	Digite uma lista separada por vírgulas de portas ou intervalos de portas remotas. Exemplo: 20,50,100-120.
Tipos de interface	Selecione qualquer uma das seguintes opções de tipo de interface: • **Todos** • **Acesso remoto** • **Sem fio** • **Lan** • **Banda larga móvel** A opção padrão **Todos** será aplicada se nenhuma opção de tipo de interface for selecionada.

8. Clique em **Avançar**.
9. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
10. Clique em **Concluído**.

Proteção de informações do Windows

Licença: Gold

Aplicável a: Windows 10+

Uma configuração de Proteção de informações do Windows (WIP) define as configurações WIP para proteger os dados corporativos. Esta configuração pode ser aplicada a dispositivos registrados em gerenciamento. Você também pode exibir detalhes de WIP para um dispositivo configurado na página de visão geral desse dispositivo.

Configuração da proteção das informações do Windows no Windows

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Proteção de informações do Windows**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela a seguir.
6. Clique em **Avançar**.
7. Selecione uma distribuição para essa configuração.

Categoria	Configuração	O que fazer
	Nome	Insira um nome que identifique essa configuração.
	Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Informações corporativas	**Todas as versões (Windows 10+ Desktop e Mobile)**	
	Nomes de domínio protegidos	Especifique a lista de identidades para as quais as políticas de proteção de dados estão configuradas. Os e-mails e outros dados associados a estas identidades serão considerados corporativos e protegidos. • Esta é uma lista de domínios separados por | com o primeiro domínio na lista considerado como a principal identidade para fins de Windows UI. • Por exemplo: "domain1.com|domain2.co.uk"

	Nomes de Domínio de rede	Especifique a lista de domínios que compõem os limites corporativos. Os dados de um destes domínios que são enviados para um dispositivo serão considerados dados corporativos e protegidos. • Estes locais serão considerados um destino seguro para os dados corporativos a serem compartilhados. • Esta é uma lista de domínios separados por vírgulas. • Por exemplo: "mail.domain3.com, domain4.com"

	Recursos de Cloud	Contém uma lista de domínios de recursos corporativos hospedados na nuvem que precisam ser protegidos. As conexões para estes recursos são consideradas dados corporativos. Especifique um ou mais nomes de domínio com endereços opcionais de proxy entre parênteses. • Por exemplo: "domainname1.com, domainname2 (10.0.0.1)". • Se um proxy estiver emparelhado com um recurso da nuvem, o tráfego para o recurso da nuvem será roteado pela rede corporativa por meio do servidor de proxy especificado (na Porta 80). • Todos os endereços de proxy especificados neste campo também devem ser inseridos no seguinte campo Servidores internos de proxy.

	Intervalo de IP	Estabelece os intervalos de IP corporativos que definem os computadores na rede corporativa. Os dados provenientes desses computadores serão considerados corporativos e protegidos. Estes locais serão considerados um destino seguro para os dados corporativos a serem compartilhados. Esta é uma lista dos intervalos IPv4 e IPv6 separados por vírgulas. • Esta é uma lista dos intervalos IPv4 e IPv6 separados por vírgulas. • Selecione a opção **Intervalos de IP são autoritativos** quando o cliente tiver que aceitar a lista configurada e não usar heurística para tentar encontrar outras sub-redes.
	Recursos neutros	Especifica a lista de nomes de domínio que podem ser usados como recurso de trabalho ou pessoal.

	Servidores de proxy	Especifica a lista de servidores proxy separados por vírgulas. Qualquer servidor nesta lista é considerado não-corporativo. • Por exemplo: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • Selecione a opção **Servidores proxy são autoritativos** quando o cliente tiver que aceitar a lista configurada de proxies e não tentar detectar outros proxies de trabalho.
	Servidores internos de proxy	Especifica a lista de servidores proxy internos separados por vírgulas. • Por exemplo "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • Estes proxies foram configurados pelo administrador para se conectarem a recursos específicos na Internet. Eles são considerados locais da rede corporativa. Os proxies são aproveitados somente na configuração da política de EnterpriseCloudResources para forçar o tráfego para os Recursos de Cloud correspondentes por meio destes proxies.
Proteção de dados	**Todas as versões (Windows 10+ Desktop e Mobile)**	

	Nível de imposição	Escolha um dos seguintes níveis de imposição: • Desativado - Sem proteção (dados criptografados anteriormente ficarão sem criptografia). • Silencioso - Criptografe os dados e as atividades de auditoria no dispositivo após os dados serem protegidos. O usuário não é alertado sobre qualquer informação relacionada a aplicativos/dados negativos. • Substitutivo - Similar ao modo Silencioso. Além disso, se um aplicativo ou dados forem usados incorretamente, o usuário será solicitado a prosseguir ou cancelar a operação que o usuário está executando atualmente. • Bloqueado - Semelhante ao modo Silencioso. Além disso, se um aplicativo ou dados forem usados incorretamente, a operação que o usuário está executando atualmente será bloqueada e o usuário será avisado sobre a razão para o bloqueio da operação.

		Exceto no modo Desativado, todos os dados ou aplicativos que não deveriam usar dados ou recursos corporativos serão registrados no dispositivo. Esses dados podem ser removidos do dispositivo usando outro provedor de serviços de configuração (CSP).
	Certificado de recuperação de dados	Especifique um certificado de recuperação que pode ser usado para a recuperação de dados de arquivos criptografados. • Ele é o mesmo que o certificado de agente de recuperação de dados (DRA) para criptografar sistema de arquivos (EFS). Entretanto, este certificado é entregue através do MDM e não através da política de grupo. Você também pode selecionar uma ou mais das seguintes opções: • Permitir descriptografia do usuário • Revogar em cancelamento de registro • Mostrar ícones de EDP • Exigir proteção sob bloqueio (apenas Windows 10 Móvel)
RMS	**Todas as versões (Windows 10+ Desktop e Mobile)**	

	Permitir Azure RMS	Especifique se deseja permitir a criptografia do Azure Rights Management (Azure RMS) para WIP.
	ID do modelo de RMS	Especifique TemplateID GUID para usar para a criptografia do RMS. O modelo do RMS permite que os administradores configurem os detalhes sobre quem tem acesso ao arquivo protegido pelo RMS e por quanto tempo eles têm acesso.
Controle de aplicativo	**Todas as versões (Windows 10+ Desktop e Mobile)**	
	Especifique uma coleção de apps que são desenvolvidos na página **Apps > App Catalog** com um valor de WIP. Especifique as definições de regras para os apps usando o seguinte conjunto de parâmetros:	
	Tipo de aplicativo	Selecione um dos seguintes tipos de aplicativo: • Publisher/PFN Equals – É aplicável ao Windows 10 Mobile e o Windows 10 Desktop com suporte a PFN. • EXE/Win32 Equals - é aplicável apenas para o Windows Desktop.
	Identificador de aplicativo	Selecione o aplicativo das escolhas exibidas para adicioná-lo ao Identificador de Aplicativos. Você também pode clicar em **Pesquisar apps**.
	Descrição do aplicativo	Insira uma descrição para o aplicativo.

Restrições do Windows

As restrições do Windows determinam quais recursos serão habilitados nos dispositivos desktops e móveis do Windows.

Configurações de restrições do Windows

Categoria	Configuração	O que fazer
	Nome	Insira um nome que identifique essa configuração.
	Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Recursos do dispositivo	**Todas as versões (Windows 10 Desktop e Mobile, Windows 8.1 Desktop e Mobile)**	
	Desativar o descarregamento do Wi-Fi	Selecionar para impedir que o dispositivo acesse redes compatíveis para transportar dados destinados para redes sem fio autorizadas.
	Desativar compartilhamento da internet	Selecione para impedir que o dispositivo acesse a Internet por meio de outro dispositivo sem fio.
	Desativar localização	Selecione para desativar os serviços de localização.
	Desativar o roaming de dados do celular	Selecione para desativar roaming de dados quando o dispositivo estiver no modo celular.
	Desabilitar Bluetooth	Selecione para impedir que o dispositivo estabeleça conexões do Bluetooth.
	Desativar VPN durante o roaming ou em uma rede celular	Selecione para impedir que o dispositivo estabeleça conexões de VPN quando não estiver no modo Wi-Fi.
	8.1 Somente Windows Phone 8.1	
	Desativar relatórios do ponto de acesso do Wi-Fi	Selecione para impedir que o dispositivo envie relatórios automáticos do ponto de acesso para a Microsoft.
	8.1+ Windows Phone 8.1 e Windows 10 Mobile	
	Desativar o Wi-Fi	Selecione para impedir que o dispositivo acesse redes sem fio.
	Desativar a configuração manual do Wi-Fi	Selecione para impedir que o dispositivo acesse redes sem fio diferentes daquelas

		definidas pelo Ivanti Neurons for MDM.
	Desabilitar NFC	Selecione para impedir que o dispositivo estabeleça comunicações de rádio com outro dispositivo ao se aproximar ou tocar em outro dispositivo.
	Desativar instalação de certificado de raiz manual	Selecione para impedir a desinstalação de certificados de raiz e intermediários pelo usuário final .
Telemetria - Permitir que o dispositivo envie dados de telemetria de diagnóstico e uso.	**Windows 10 apenas**	
	Nível de telemetria	Selecione um dos seguintes níveis de telemetria de relatórios de dados: • **Segurança** - Envie informações sobre a Experiência do usuário conectado, Configurações de componentes de telemetria, a Ferramenta de remoção de software malicioso e o Windows Defender. • **Básico** - Envie informações básicas do dispositivo que incluam dados relacionados à qualidade, compatibilidade de aplicativo, dados de uso do aplicativo e dados do nível de segurança. • **Avançado** - Envie mais informações que incluam uso e desempenho do Windows, Windows Server, System Center e apps. Também inclui dados avançados de confiabilidade e dados dos níveis básico e de segurança. • **Completo (Padrão)** - Envie todos os dados para identificar e ajudar a corrigir os problemas, além de dados dos níveis de segurança, básico e avançado.

Prevenção de Perda de Dados (DLP)	**Todas as versões (Windows 10 Desktop e Mobile, Windows 8.1 Desktop e Mobile)**	
	Desabilitar câmera	Selecione para impedir que o usuário final use o aplicativo câmera.
	Desativar acesso ao cartão (SD) de armazenamento	Selecione para impedir que o dispositivo acesse um cartão de armazenamento.
	8.1 Somente Windows Phone 8.1	
	Desativar "Salvar como" off-line	Selecione para impedir que o usuário final use o comando Salvar como com os arquivos do Office Hub.
	Desativar compartilhamento off-line	Selecione para impedir que o usuário final compartilhe os arquivos do Office Hub.
	8.1+ Windows Phone 8.1 e Windows 10 Mobile	
	Desativar copiar e colar	Selecione para impedir que o usuário final copie e cole dados entre aplicativos.
	Desabilitar captura de tela	Selecione para impedir que o usuário final use o recurso de captura de tela no dispositivo.
	Desativar gravação de voz	Selecione para impedir que o usuário final use o recurso de gravação de voz.
	Desativar armazenamento em massa USB	Selecione para impedir que o usuário final acesse o armazenamento do dispositivo a partir de uma área de trabalho por meio de um USB.
Uso de dados	**Windows 10+**	
	Custo das conexões 3G	Selecione uma das opções a seguir: • **Irrestrito** - A conexão é ilimitada e não é restrita por cobranças de uso e limitações de capacidade. • **Fixo** - A conexão é restrita por cobranças de uso e limitações de capacidade após determinado limite de dados. • **Variável** - A conexão é cobrada por bytes.
	Custo das conexões 4G	

Defender	**Windows 10+**	
	Desative a funcionalidade de monitoramento em tempo real do Defender	Selecione para desativar a funcionalidade de monitoramento em tempo real do Windows Defender
DeviceGuard	**Windows 10+**	
	Desativar segurança baseada em virtualização (VBS)	Selecione para impedir que a segurança baseada em virtualização forneça suporte para serviços de segurança.
	Proteção de credencial com segurança baseada em virtualização	Selecione uma das opções a seguir: • **Desativado** - Desative a proteção de credencial com segurança baseada em virtualização. • **Ativado com a trava UEFI** - Ative a proteção de credencial com segurança baseada em virtualização com trava de Interface Unificada de Firmware Extensível (UEFI). • **Ativado sem trava** - Ative a proteção de credencial com segurança baseada em virtualização sem a trava UEFI.
	Nível de segurança de plataforma (requer recursos de segurança de plataforma)	Selecione uma das opções a seguir: • **VBS com Reinicialização segura** - Selecione esta opção para ativar a segurança baseada em virtualização com reinicialização segura. • **VBS com Reinicialização segura e Acesso direto à memória** - Selecione esta opção para ativar a segurança baseada em virtualização com reinicialização segura e acesso direto à memória.
Privacidade	**Windows 10+**	
	Desativar ID de publicidade	Selecione para desativar o ID de publicidade.
	Desativar a publicação	Selecione para impedir que os Apps/SO

	do feed de atividades pelos Apps/SO	apliquem no feed de atividade.
Windows e Aplicativo	**Todas as versões (Windows 10 Desktop e Mobile, Windows 8.1 Desktop e Mobile)**	
	Desativar contas da Microsoft para serviços que não sejam de e-mail	Selecione para impedir que o usuário final use contas da Microsoft para autenticar serviços que não sejam de e-mail.
	Desativar contas que não sejam da Microsoft	Selecione para impedir que o usuário final configure e-mail usando contas que não sejam da Microsoft.
	Desativar o assistente pessoal Cortana	Selecione para impedir que o usuário final acesse o assistente pessoal da Microsoft.
	Desativar pesquisas baseadas em localizações	Selecione para impedir que pesquisas utilizem a localização do dispositivo.
	Desativar desbloqueio do desenvolvedor	Selecione para impedir que o usuário final habilite o sideloading de aplicativos. O modo padrão, quando um dispositivo é registrado no MDM, é habilitado no SideLoad.
	11+ Enterprise Edition	
	Configuração do ícone Chat do Teams na barra de tarefas	Selecione uma das opções a seguir: • **Mostrar:** o ícone Chat aparece na barra de tarefas por padrão. Os usuários podem exibi-lo ou ocultá-lo em Configurações. • **Ocultar:** o ícone Chat é oculto por padrão. Os usuários podem exibi-lo ou ocultá-lo em Configurações. • **Desativado:** o ícone Chat não é exibido, e os usuários não podem exibi-lo ou ocultá-lo em Configurações.

		• **Não configurado:** o ícone Chat se comporta de acordo com o padrão da sua edição do Windows. As alterações não entram em vigor até que o dispositivo Windows seja reiniciado.
	Windows Phone 10+	
	Desativar a atualização automática de apps da Microsoft Store	Desativar para impedir a atualização automática de apps da Microsoft Store.
	Desativar a inicialização de todos os apps da Microsoft Store que vieram pré-instalados ou que foram baixados	Selecione para impedir que usuários finais inicializem todos os apps pré-instalados ou baixados da Microsoft Store. Compatível apenas com as edições Enterprise e Education do Windows.
	Permitir que os apps sejam executados em segundo plano	Selecione uma das opções a seguir: • **Usuário em controle**: Permite que o usuário controle a execução de apps em segundo plano. • **Permitir força**: Permite a execução de apps em segundo plano. • **Negar força**: evita a execução de apps em segundo plano.
	Somente Windows Phone 8.1	
	Desativar armazenamento de imagens do recurso Pesquisa Visual	Selecione para impedir que o usuário final salve imagens das pesquisas do Bing Vision.
	8.1+ Windows Phone 8.1 e Windows 10 Mobile	
	Desativar a Microsoft Store	Selecione para impedir que o usuário final acesse a app store da Microsoft.
	Desativar o Internet Explorer	Selecione para impedir que o usuário final acesse o Internet Explorer.
	Desativar alertas da	Selecione para impedir a exibição de alertas da

	Central de Ações	Central de Ações acima da tela de bloqueio.
Configurações do navegador seguro	**10+ Windows 10 Desktop e Mobile**	
	Desativar pop-ups do navegador em computadores	(somente para Desktop) Selecione para desabilitar as janelas de navegação pop-up no navegador da Microsoft Edge.
	Desativar Gerenciador de senhas	Selecione para desativar o salvamento e o gerenciamento de senhas locais nos dispositivos.
Outras restrições	**Todas as versões (Windows 10 Desktop e Mobile, Windows 8.1 Desktop e Mobile)**	
	Desabilitar a capacidade de cancelar registro do UEM e excluir a conta do local de trabalho.	Selecione para impedir que o usuário final cancele o registro do UEM e exclua a imagem da conta da empresa.
	Windows Phone 10+	
	Desativar o usuário para reinicialização de fábrica do dispositivo usando o painel de controle e a combinação de teclas do hardware	Selecione para evitar que o usuário final defina o período de carência do bloqueio do dispositivo.
	Exigir que os usuários se conectem à rede durante a configuração do dispositivo (é necessário o perfil de piloto automático)	Selecione essa opção para permitir que o TenantLockdown bloqueie todos os dispositivos Windows registrados usando o recurso Autopilot.
	8.1+ Windows Phone 8.1 e Windows 10 Mobile	
	Exigir criptografia do dispositivo	Selecione para ativar a criptografia de armazenamento interno. Depois de ativada, essa opção não poderá ser alterada pelo servidor UEM.
	Não permitir que o usuário ajuste o período de cortesia de bloqueio	Selecione para impedir que o usuário ajuste o período de cortesia de bloqueio.

Os dispositivos Windows 8.1 não reportam o número de série.

Restrições para desktop Windows

Aplicável a: desktops Windows 10

Esta seção contém os seguintes tópicos:

- Configurar restrições para desktop Windows
- Criação de uma lista de permitidos para dispositivos de armazenamento removíveis

Os administradores podem controlar informações do SO em dispositivos desktop Windows 10 restringindo o acesso do usuário às seguintes áreas em um dispositivo:

- Painel de controle
- Gerenciador de tarefas
- Explorador de arquivos
- Editor de registro

As funções acima permitem que o usuário faça muitas alterações ao dispositivo. Usando esse recurso, os administradores podem restringir o acesso a esses controles no nível do sistema e, portanto, proteger o acesso.

Este recurso exige o Bridge. Consulte "Ivanti Bridge" na página 429 para detalhes.

Configurar restrições para desktop Windows

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Restrições para desktop Windows**.
3. Insira um nome para a configuração.
4. Insira uma descrição.

Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela a seguir.

5.

Configuração	O que fazer
Gerenciador de Tarefas	Marque a caixa de seleção **Negar acesso** para a configuração à qual o acesso deve ser negado.
Painel de Controle	
Editor de Registro	
Explorador de Arquivos	Marque a caixa de seleção **Restringir funcionalidades** para restringir as funcionalidades do Explorador de Arquivos. Exemplo: remoção da unidade de mapeamento de rede. Clique no link fornecido para ver a lista de funcionalidades restritas.
Armazenamento removível	
Acessar o modo de Armazenamento removível	• **Restringir acesso de leitura**: isso impede qualquer acesso e é a configuração mais restritiva. • **Restringir acesso de gravação**: permite acesso limitado, mas impede a remoção não autorizada de dados e a capacidade de adicionar vírus, etc. ao dispositivo.

6. Clique em **Avançar**.

7. Selecione uma das opções de distribuição a seguir:

   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar

8. Clique em **Concluído**.

> Para a configuração entrar totalmente em vigor, o dispositivo deve ser reinicializado após a configuração ser aplicada.

Criação de uma lista de permitidos para dispositivos de armazenamento removíveis

Se você quiser criar uma lista de dispositivos de armazenamento permitidos, conclua as seguintes etapas primeiro:

- Anexe a um PC os dispositivos de armazenamento USB que você deseja permitir.
- Abra o Gerenciador de Dispositivos e clique no controlador de USB.
- Veja as configurações de cada controlador para obter informações sobre o dispositivo.
- Armazene as informações do dispositivo a serem usadas ao criar sua lista de permitidos.

Para criar uma lista de permitidos para dispositivo de armazenamento removível:

Procedimento

1. Na página de configuração **Restrições para desktop Windows**, clique em **+Adicionar** na seção **Armazenamento removível permitido**.
2. Na janela **Adicionar IDs de hardware**, insira o ID do hardware para um ou mais dispositivos que você queira adicionar à lista de permitidos.
3. Clique em **Adicionar IDs de hardware**. A lista de IDs de hardware permitidos é exibida na seção **Armazenamento removível permitido**.

> Para editar ou excluir um ID de hardware da lista, selecione a opção Editar ou Excluir na coluna **Ações**.
> Para a configuração entrar totalmente em vigor, o dispositivo deve ser reinicializado após a configuração ser aplicada.

Configurações da área de trabalho do Windows 10

As configurações da área de trabalho do Windows 10 permitem personalizar as configurações da área de trabalho e enviá-las a dispositivos Windows 10. Usando esta configuração, você pode configurar os seguintes ajustes da área de trabalho:

- Imagem de fundo da área de trabalho
- Imagem da tela de bloqueio
- Carregar um protetor de tela personalizado
- Atalhos da área de trabalho

Este recurso exige o Bridge. Consulte "Ivanti Bridge" na página 429 para detalhes.

Procedimento

1. Em **Configuração**, clique em **+Adicionar**.
2. Selecione a configuração **Configurações da área de trabalho do Windows 10**. A página **Configurações da área de trabalho do Windows 10** é exibida.
3. No campo **Nome**, digite um nome apropriado para as configurações.

4. (Opcional) Clique no link +**Adicionar descrição** para adicionar uma descrição à configuração.

5. Na seção **Configuração**, configure as definições a seguir:

Configuração	Descrição
Entrega de arquivo	Selecione alguma das seguintes opções de entrega de arquivo para Configurações da área de trabalho: • **Carregar arquivo** - carregar configurações para o Ivanti Neurons for MDM. • **URL de substituição** – Informe URLs de substituição com os arquivos de configuração para download.
Configurações de papel de parede da área de trabalho	Clique em **Escolher arquivo** para localizar e carregar uma imagem de papel de parede. Os formatos de arquivo suportados são BMP, JPG, JPEG, PNG.
Configurações de papel de parede da tela de bloqueio (A configuração do papel de parede da tela de bloqueio **NÃO** é suportada em dispositivos Windows 10 Pro)	Clique em **Escolher arquivo** para localizar e carregar uma imagem de papel de parede. Os formatos de arquivo compatíveis são BMP, JPG, JPEG e PNG.

Configuração	Descrição
Configurações de proteção de tela	Clique em **Escolher arquivo** para localizar e carregar um arquivo de proteção de tela. Transfira apenas arquivos .SCR compatíveis com Windows. Selecione **Proteger com senha em Proteção de Tela** se quiser definir a senha para desbloquear o modo Proteção de Tela. Selecione o **Tempo limite da proteção de tela** (em minutos).

Configuração	Descrição
Atalhos da área de trabalho	Clique em **Adicionar atalho** para configurar atalhos para adicionar às áreas de trabalho de dispositivos. A janela **Adicionar atalho** é exibida. Preencha a tabela usando as seguintes opções: • **Local** – Digite o local onde o atalho deve aparecer no dispositivo Windows. • **Caminho de destino** – Digite o caminho local, o caminho UNC ou a letra da unidade à qual o atalho levará. O caminho de destino também pode ser uma URL. • **Argumentos** – Digite os argumentos que devem ser usados ao abrir o arquivo de destino. • **Diretório de trabalho** – Digite o caminho da pasta que contém os arquivos necessários para o destino. • **Arquivo de ícone** – Transfira arquivos .ico válidos do Windows. Após configurar as opções, clique em **Adicionar atalho**.

6. Clique em **Avançar**.

7. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
8. Clique em **Concluído**.

Configuração do Windows Hello para Empresas

Esta configuração permite que os administradores configurem o Windows Hello nos dispositivos. Para configurar o Windows Hello, é necessário configurar um PIN para fazer login no dispositivo.

Aplicável a: Windows 10

ProcedureProcedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **Windows** no campo de pesquisa e, então, clique na configuração de **Windows Hello para Empresas**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Coloque o botão de alternância **Ativar/Desativar Windows Hello para Empresas para dispositivos Windows 10** em **Ligado**.

   > A configuração é definida como Ligada por padrão. A desativação do Windows Hello para Empresas não remove PINs dos dispositivos.

5. Selecione a **Complexidade do PIN**.
6. Selecione as configurações necessárias:
   - Requer um Trusted Platform Module (TPM) para Windows Hello para Empresas
   - Usar certificados do Windows Hello para Empresas como certificados de cartão inteligente
   - Usar gestos biométricos, como de face e impressão digital, como uma alternativa ao gesto de PIN para o Windows Hello para Empresas
   - Requer um antispoofing avançado para reconhecimento facial na autenticação por face do Windows Hello
   - Bloqueio dinâmico
   - Permite que usuários façam login com uma chave de segurança FIDO2.
7. Clique em **Avançar**.

8. Selecione a opção **Ativar esta configuração**.
9. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizado.
10. Clique em **Concluído**.

Play Integrity (anteriormente Certificação SafetyNet)

O Play Integrity (anteriormente SafetyNet) ajuda a avaliar a segurança e a compatibilidade de dispositivos Android usando as APIs Play Integrity do Google. Quando configurada, permite analisar dispositivos, após um intervalo de tempo regular, para determinar se foram adulterados ou não.

Procedimento

1. Na aba **Configuração**, clique em **+Adicionar**.
2. Selecione a configuração **Play Integrity**. A página **Configuração Play Integrity** é exibida.
1. No campo **Nome**, digite um nome apropriado para a Configuração Play Integrity.
2. Clique no link +**Adicionar descrição** para adicionar uma descrição para a configuração. Esse campo é opcional.
3. Na seção **Definições de configuração**, digite o intervalo de tempo mínimo (em horas) que deve ser aplicado para avaliar a segurança e a verificação de compatibilidade em dispositivos. O valor deve estar entre 1 e 24.
4. Clique em **Próximo** e selecione uma das seguintes opções de distribuição:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
5. Clique em **Concluído**.

Senha de Android avançada e tela de bloqueio

A configuração de Senha de Android avançada e tela de trava para dispositivos Android permite manter os dispositivos seguros. Essa configuração é aplicada aos dispositivos para definir a senha e a configuração da senha do Perfil de trabalho no dispositivo de propriedade da empresa.

Quando essa configuração é aplicada a um dispositivo, nenhuma configuração de Senha ou Desafio de trabalho (Work Challenge), se existir, será aplicada ao dispositivo.

Para o Perfil de trabalho e o Perfil de trabalho no Dispositivo de propriedade da empresa, a Qualidade da senha é descontinuada em dispositivos Android 12+ para a senha no nível do dispositivo. Além disso, as configurações de Qualidade da Senha são convertidas automaticamente em configurações de Complexidade da Senha pelo Go app se o administrador não tiver habilitado as configurações de Complexidade da Senha.

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Senha de Android avançada e tela de bloqueio**.
3. Digite um nome e uma descrição para a configuração.
4. Na seção **Definição da Configuração**, configure os seguintes parâmetros:

Configuração	O que fazer
Senha do dispositivo	
Exigir senha do dispositivo	Coloque a opção de alternância em **LIGADO**.
Complexidade da senha (Android v12.0+)	

O parâmetro **Complexidade da senha** tem prioridade mais alta do que o parâmetro **Qualidade da senha**. Quando a opção **Exigir senha do dispositivo** estiver ATIVADA e a **Complexidade da senha** estiver definida, o parâmetro **Qualidade da senha** será ignorado.

Habilitar complexidade de senha	Coloque a opção de alternância em **LIGADO** e selecione uma das opções a seguir: • **Nenhuma** – Para evitar o uso de qualquer complexidade de padrão ou de PIN ou de sequência alfanumérica ou alfabética. • **Baixa** – Para definir uma senha numérica ou com um padrão com no mínimo quatro dígitos. • **Média** – para definir uma senha com uma das seguintes opções: Numérica (com no mínimo quatro dígitos), Alfabética (com no mínimo 4 caracteres) ou Alfanumérica (com no mínimo 4 caracteres). • **Alta** – para definir uma senha com uma das seguintes opções: Numérica (com no mínimo 8 dígitos), Alfabética (com no mínimo 6 caracteres) ou Alfanumérica (com no mínimo 6 caracteres).

Qualidade da senha	Selecione a qualidade da senha entre as seguintes opções da lista suspensa: • **Biométrico** – permite métodos biométricos de desbloqueio, como reconhecimento facial. • **Algo** – requer uma senha, mas não define uma restrição de tipo. • **Numérica** – requer uma senha que inclua pelo menos caracteres numéricos. • **Numérica complexa** – requer uma senha que inclua pelo menos caracteres numéricos e não tenha repetição (por exemplo, 4444) ou sequências em ordem (por exemplo, 1234). • **Alfabética** – requer uma senha que inclua pelo menos caracteres alfabéticos ou outros símbolos. • **Alfanumérica** – requer uma senha que inclua pelo menos caracteres numéricos e alfabéticos (ou outros símbolos). • **Complexa** – requer uma senha que inclua caracteres numéricos, alfabéticos e especiais.
Comprimento mínimo	Mova o seletor para especificar a extensão mínima de uma senha para impedir que o usuário crie senhas curtas e não seguras. Intervalos de números entre 4 e 16.

Ciclo de vida da senha	Insira os valores para os seguintes campos: • **Expiração** – especifica a expiração da senha em dias. • **Extensão do histórico** – especifica o número de senhas antes que um usuário possa reutilizar qualquer senha determinada. • **Máx. de tentativas fracassadas** – o número máximo de vezes que um usuário pode inserir uma senha incorreta antes que os dados corporativos sejam apagados do dispositivo. • **Tempo limite de inatividade** – insira um tempo máximo pelo qual o usuário pode ficar inativo antes de um tempo limite da sessão.

Gerenciar recursos do Keyguard	Ative os recursos de proteção necessários usando as seguintes opções de caixa de seleção: • **Ativar impressão digital** • **Ativar câmera segura** • **Ativar todas as notificações** Aplicável para o modo de proprietário do dispositivo. • **Ativar todos os agentes de confiança** **Aplica-se apenas ao modo Administrador e Proprietário do dispositivo.** • **Ativar leitura de íris** Aplicável apenas a Android 9.0+ ou Samsung. • **Ativar desbloqueio facial** Aplicável apenas a Android 9.0+ ou Samsung.

Gerenciar trava inteligente (Android 6.0 +)	Coloque a opção de alternância em **LIGADO** para gerenciar a configuração de Trava inteligente.
	
	Ative a configuração de Trava inteligente exigida usando as seguintes opções de caixa de seleção:
	
	• **Ativar desbloqueio por Bluetooth**
	  • Desativar dispositivos de áudio/vídeo
	  • Desativar dispositivos de computador
	  • Desativar dispositivos de saúde
	  • Desativar dispositivos de imagem
	  • Desativar dispositivos diversos
	  • Desativar dispositivos de rede
	  • Desativar dispositivos periféricos
	  • Desativar dispositivos de celular
	  • Desativar dispositivos de brinquedo
	  • Desativar dispositivos sem categoria
	  • Desativar dispositivos vestíveis
	• **Ativar desbloqueio por NFC**
	  • Ativar a tag Não seguro
	  • Ativar a tag Seguro
	• **Ativar locais (localização)**

	• Ativar locais personalizados (além de Casa) • **Ativar desbloqueio facial (incluindo desbloqueio facial Samsung)** • **Ativar desbloqueio no corpo** • **Ativar desbloqueio por voz**
Senha do Work Profile (Challenge) (Android 7.0+)	
Exigir senha do Work Profile (Challenge)	Coloque a opção de alternância em **LIGADO**.
Complexidade da senha (Android v12.0+)	

Habilitar complexidade de senha	Coloque a opção de alternância em **LIGADO** e selecione uma das opções a seguir: • **Nenhuma** – Para evitar o uso de qualquer complexidade de padrão ou de PIN ou de sequência alfanumérica ou alfabética. • **Baixa** – Para definir uma senha numérica ou com um padrão com no mínimo quatro dígitos. • **Média** – para definir uma senha com uma das seguintes opções: Numérica (com no mínimo quatro dígitos), Alfabética (com no mínimo 4 caracteres) ou Alfanumérica (com no mínimo 4 caracteres). • **Alta** – para definir uma senha com uma das seguintes opções: Numérica (com no mínimo 8 dígitos), Alfabética (com no mínimo 6 caracteres) ou Alfanumérica (com no mínimo 6 caracteres).

Qualidade da senha	Selecione a qualidade da senha entre as seguintes opções da lista suspensa: • **Biométrico** – permite métodos biométricos de desbloqueio, como reconhecimento facial. • **Algo** – requer uma senha, mas não define uma restrição de tipo. • **Numérica** – requer uma senha que inclua pelo menos caracteres numéricos. • **Numérica complexa** – requer uma senha que inclua pelo menos caracteres numéricos e não tenha repetição (por exemplo, 4444) ou sequências em ordem (por exemplo, 1234). • **Alfabética** – requer uma senha que inclua pelo menos caracteres alfabéticos ou outros símbolos. • **Alfanumérica** – requer uma senha que inclua pelo menos caracteres numéricos e alfabéticos (ou outros símbolos). • **Complexa** – requer uma senha que inclua pelo menos caracteres numéricos, alfabéticos e especiais.

Ciclo de vida da senha	Insira os valores para os seguintes campos: • **Expiração** – especifica a expiração da senha em dias. • **Extensão do histórico** – especifica o número de senhas antes que um usuário possa reutilizar qualquer senha determinada. • **Máx. de tentativas fracassadas** – o número máximo de vezes que um usuário pode inserir uma senha incorreta antes que os dados corporativos sejam apagados do dispositivo. • **Tempo limite de inatividade** – insira um tempo máximo pelo qual o usuário pode ficar inativo antes de um tempo limite da sessão. **Tempo limite de autenticação forte** (aplicável apenas a dispositivos Android 8.0+ em Proprietário do perfil, Proprietário do dispositivo e Dispositivo gerenciado com perfil de trabalho) – especifica a duração (em minutos) após a qual expirará o desbloqueio com uma autenticação secundária (impressão digital, biometria). Esse campo se aplica apenas se **Biometria** ou **Algo** for selecionado como uma opção **Qualidade da senha**.

	O limite mínimo é de 60 minutos e o limite máximo é de 4.320 minutos. Se o campo é definido como em branco, nada é definido no dispositivo.
Gerenciar recursos do Keyguard	Ative os recursos de proteção necessários usando as seguintes opções de caixa de seleção: • **Ativar impressão digital** • **Ativar câmera segura** • **Ativar todos os agentes de confiança** • **Ativar leitura de íris** Aplicável apenas a Android 9.0+ ou Samsung. • **Ativar desbloqueio facial** Aplicável apenas a Android 9.0+ ou Samsung.

5. Clique em **Avançar**.
6. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
7. Clique em **Concluído**.

Proteção avançada contra ameaças do Windows

A configuração Proteção avançada contra ameaças do Windows permite que dispositivos desktop usem o serviço Proteção avançada contra ameaças do Microsoft Windows (ATP) do Azure.

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Proteção avançada contra ameaças do Windows**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela a seguir.

Configuração	O que fazer
Blob de integração ou remoção	Cole o blob de integração ou remoção do site ATP Security Center

6. Clique em **Avançar**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
8. Clique em **Concluído**.

Autenticação baseada em certificado

Ivanti Neurons for MDMé compatível com a autenticação baseada em certificado, que permite aos administradores fazer login usando certificados digitais e um nome de host especificado pelo locatário (personalizado). Depois de serem ativados e configurados, os administradores podem fazer login usando certificados digitais em vez da autenticação básica (nome de usuário e senha).

Esse recurso está desativado por padrão. Para ativar este recurso em seus locatários, os administradores devem entrar em contato com o Suporte. Este recurso está disponível apenas em ambientes de cluster NA3, e apenas se for ativado pelo suporte. Verifique se o seu nome de usuário e a sua senha de superadministrador foram testados e estão prontos, porque assim que a autenticação com base em certificado for ativada, essas credenciais serão as únicas que você poderá usar para fazer login até que tenha configurado com êxito seu domínio personalizado.

Procedimento

1. Na guia **Admin**, selecione **Configuração de host personalizado**.
2. Na página Configuração de host personalizado, configure as seguintes opções:

Configuração	O que fazer
Criar domínio personalizado	Digite o nome do domínio personalizado. Este é o nome de domínio que possivelmente mais se alinha à sua identidade corporativa e no qual você pode fazer login usando certificados digitais.
Fazer upload de certificados de CA de emissores confiáveis	Clique em **Escolher arquivo** para selecionar e fazer upload do certificado de CA que emite certificados para seus administradores. Para ativar a verificação de revogação de certificados, selecione a opção **Ativar configurações de validação do status do certificado para este certificado** (opcional). Esta opção é ativada por padrão. Para desativar a revogação de certificados, desmarque esta opção. Clique em **Adicionar mais** para adicionais mais certificados. Certifique-se de que o formato do certificado seja .p7b, .pem, .der, .crt ou .cer.

Configuração	O que fazer
Mapeamento do atributo do certificado	O mapeamento do atributo do certificado configura o mapeamento dos elementos de identidade do certificado para os atributos da conta do administrador. No campo **Do certificado**, selecione um dos seguintes elementos do certificado: • **Nome da entidade NT** • **Nome RFC 822** No campo **Para variável**, selecione qualquer um dos seguintes atributos da conta do administrador: • **UPN do usuário** • **$UserEmailAddress** • **$EDIPI**

3. Clique em **Salvar**.

   Pode levar alguns minutos para que seu host personalizado torne-se acessível.

Configurações do recurso do usuário

Esta seção contém os seguintes tópicos:

Configuração CalDAV

Uma configuração CalDAV define o acesso a um calendário da web usando a internet CalDAV padrão.

Configurações CalDAV

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome do host e porta	Insira o nome do host e a porta para o servidor do calendário.
URL principal	Insira a URL para acessar os serviços de calendário.
Usuário	Insira o nome de usuário para o acesso.
Senha	Insira a senha para o acesso.
Usar SSL	Selecione para usar somente uma camada de soquete segura para comunicações entre o dispositivo e o servidor.
VPN por aplicativo	**Pré-requisito**: configure o Tunnel ou qualquer configuração VPN por aplicativo antes de realizar a configuração de VPN por aplicativo em CalDAV. No menu suspenso, selecione a configuração de VPN por aplicativo pré-configurada. **Aplicável a**: iOS 14+

Para obter mais informações, consulte Como criar uma configuração

Configuração CardDAV

Um CardDAV define o acesso a um livro de endereços da web usando a internet CalDAV padrão.

Configurações CardDAV

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome do host e porta	Insira o nome do host e a porta para o servidor do livro de endereços.
URL principal	Insira a URL para acessar os serviços de livro de endereços.
Nome de Usuário	Insira o nome de usuário para o acesso.
Senha	Insira a senha para o acesso.
Usar SSL	Selecione para usar somente uma camada de soquete segura para comunicações entre o dispositivo e o servidor.
VPN por aplicativo	**Pré-requisito**: configure o Tunnel ou qualquer configuração VPN por aplicativo antes de realizar a configuração de VPN por aplicativo em CardDAV. No menu suspenso, selecione a configuração de VPN por aplicativo pré-configurada. **Aplicável a**: iOS 14+
iOS 10+	
Regras de serviço de comunicação	Escolha um aplicativo padrão para usar a fim de fazer chamadas de áudio para contatos do sistema CardDAV.

Para obter mais informações, consulte Como criar uma configuração

Configuração do Google

A configuração de conta do Google conecta os dispositivos iOS 9.3.2 ou Android 6.0+, ou versões mais recentes com suporte, às contas do Google. O Android corporativo é obrigatório para as Contas Google. A configuração pode definir muitos endereços de e-mail do Google e outros serviços do Google que o usuário ativar após a autenticação.

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Conta do Google**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela a seguir:

6.

Configuração	O que fazer
iOS 9.3.2+ , Android 6.0+	
Nome	Insira um nome que identifique essa configuração.
Descrição da conta	Insira o nome de exibição da conta.
Nome da conta	Insira o nome completo do usuário da conta.
Endereço de e-mail	Insira o endereço de e-mail do Google da conta.

VPN por aplicativo	**Pré-requisito**: configure o Tunnel ou qualquer configuração VPN por aplicativo antes de realizar a configuração de VPN por aplicativo em Conta do Google. No menu suspenso, selecione a configuração de VPN por aplicativo pré-configurada. **Aplicável a**: iOS 14+
iOS 10+	
Regras de serviço de comunicação	Selecione uma das opções de aplicativo padrão para usar a fim de fazer chamadas de áudio para contatos no sistema Google: • **No App Catalog e no Apps do sistema**: Para pesquisar, digite as primeiras letras do nome do aplicativo. • **Digite o ID do pacote (apenas para aplicativos do sistema Apple)**: digite o ID do pacote de aplicativo do sistema. ID do pacote deve começar por "com.apple".

7. Clique em **Avançar**.
8. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
9. Clique em **Concluído**.

Quando uma configuração de conta do Google é aplicada ao dispositivo, o Go client solicita que o usuário faça login no Google.

Para obter mais informações, consulte Como criar uma configuração

Configuração de e-mail

Uma configuração de e-mail define e-mails POP ou IMAP nos dispositivos.

Configurações do e-mail

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Descrição da conta	Insira o texto que você deseja usar para identificar essa conta de e-mail.
Tipo de conta	Selecione IMAP ou POP. Se você selecionar IMAP, também é possível inserir o prefixo do caminho. O provedor de serviços da internet (ISP) pode fornecer informações sobre o tipo de conta que está disponível. Normalmente, é necessário um prefixo quando todas as pastas IMAP estiverem listadas na Caixa de entrada. ISPs que precisam de prefixos normalmente fornecem informações sobre o prefixo específico para configurar.
Nome de exibição do usuário	Insira o texto que você deseja usar para identificar a conta de e-mail do usuário. Observe que o usuário também pode definir esse valor no dispositivo.
Endereço de e-mail	Insira uma variável para especificar o endereço de e-mail para a conta.
Permitir movimentação	Selecione se você não deseja impedir que o e-mail seja movido desta conta.

Habilitar S/MIME	Selecione para ativar o suporte à criptografia S/MIME. Depois, selecione os certificados de autenticação e criptografia. Requer armazenamento em cache de certificados. Verifique se o cache está ativado na Autoridade de certificação usada pela configuração do Certificado de identidade. **iOS 10.3 ou superior:** Selecione uma das opções a seguir para os campos **Assinatura S/MIME** e **Criptografia S/MIME**: • Desligar • Ligar • Seleção do usuário **iOS 12.0+:** • Permitir que o usuário substitua configurações de assinatura de S/MIME • Permitir que o usuário selecione a identidade de assinatura de S/MIME • Permitir que o usuário substitua configurações de criptografia de S/MIME • Permitir que o usuário selecione a identidade de criptografia de S/MIME **Ativar assinatura e criptografia S/MIME por mensagem** se necessário.

Permitir caixa postal	Selecione para permitir o Mail Drop nesta conta. O Mail Drop permite que o usuário envie e-mails com anexos pesados ao armazenar o anexo no iCloud e colocar um link para acessá-lo no e-mail. Para obter mais informações sobre o Mail Drop acesse: https://support.apple.com/
VPN por aplicativo	A capacidade de associar diversos perfis diferentes de VPN por aplicativo em domínios de e-mail é suportada pela Apple. As configurações de e-mail IMAP e POP3 agora são compatíveis com VPN por aplicativo. **Pré-requisito**: configure o Tunnel ou a configuração VPN por aplicativo antes de realizar a configuração de e-mail VPN por aplicativo. Selecione **Criar configuração VPN por aplicativo** no menu suspenso.

E-mail de entrada

Configuração	**O que fazer**
Servidor de e-mail e porta	O provedor de serviços da internet (ISP) pode fornecer esse endereço.
Nome de Usuário	Insira o nome de usuário para acessar o servidor de e-mail de entrada. Normalmente, ele é igual ao endereço de e-mail. Seu ISP pode fornecer o formato.
Tipo de autenticação	Selecione o tipo de autenticação definido pelo ISP.
Senha	Insira a senha para acessar o servidor de e-mail de entrada.
Usar SSL	Selecione para usar somente uma camada de soquete segura para comunicações entre o dispositivo e o servidor.

E-mail de saída

Configuração	O que fazer
Servidor de e-mail e porta	O provedor de serviços da internet (ISP) pode fornecer esse endereço.
Nome de Usuário	Insira o nome de usuário para acessar o servidor de e-mail de saída. Normalmente, ele é igual ao endereço de e-mail. Seu ISP pode fornecer o formato.
Tipo de autenticação	Selecione o tipo de autenticação definido pelo ISP.
Senha	Insira a senha para acessar o servidor de e-mail de saída.
Senha de envio igual a senha de recebimento	Selecione se a autenticação SMTP usa a mesma senha que POP/IMAP.
Usar somente no e-mail	Selecione se quiser que essa configuração seja utilizada somente pelo cliente de e-mail. Outros apps que enviam e-mail, incluindo apps que enviam conteúdo usando o cliente de e-mail nativo, não podem usar essa configuração.
Usar SSL	Selecione para usar somente uma camada de soquete segura para comunicações entre o dispositivo e o servidor.

Configuração do Exchange

Uma configuração do Exchange define o e-mail baseado em ActiveSync em dispositivos Android e iOS, além do e-mail baseado em Exchange Web Services (EWS) para dispositivos macOS.

A configuração do Exchange foi preterida pela Samsung no Android 9. Para dispositivos Samsung com Android 9 e versões posteriores, não há suporte à configuração do Exchange no modo Administrador do Dispositivo.

Configurações do Exchange

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Host do Exchange	Se você estiver usando Sentry para controlar o acesso ao email, insira o nome do host do servidor Sentry. Caso contrário, digite o endereço do servidor ActiveSync.*
Permitir movimentação	**Para iOS e Android:** Selecione se você não deseja impedir que o e-mail seja movido desta conta. **Para Windows Phone 8.1 e Windows 10:** não aplicável.

Habilitar S/MIME	Selecione para ativar o suporte da criptografia S/MIME. Depois, selecione os certificados de autenticação e criptografia. Requer armazenamento em cache de certificados. Verifique se o cache está ativado na Autoridade de certificação usada pela configuração do Certificado de identidade. **iOS 10.3 ou superior:** Selecione uma das opções a seguir para os campos **Assinatura S/MIME** e **Criptografia S/MIME**: • Desligar • Ligar • Seleção do usuário **iOS 12.0+:** • Permitir que o usuário substitua configurações de assinatura de S/MIME • Permitir que o usuário selecione a identidade de assinatura de S/MIME • Permitir que o usuário substitua configurações de criptografia de S/MIME • Permitir que o usuário selecione a identidade de criptografia de S/MIME **Ativar assinatura e criptografia S/MIME por mensagem** se necessário.

Sincronizar endereços de e-mail recentes	Selecione para sincronizar endereços de e-mail contatados recentemente entre o dispositivo e o servidor.
Usar somente no e-mail	Selecione se quiser que essa configuração seja utilizada somente pelo cliente de e-mail. Outros apps que enviam e-mail, incluindo apps que enviam conteúdo usando o cliente de e-mail nativo, não podem usar essa configuração.
Usar SSL	Selecione para usar somente uma camada de soquete segura para comunicações entre o dispositivo e o servidor.
Ativar OAuth para trocar carga útil	iOS 12.0+ e macOS 10.14+: Selecione para ativar a autenticação via OAuth. Se esta opção estiver habilitada, as seguintes configurações adicionais estarão disponíveis para apps de e-mail que suportam autenticação via OAuth: • URL de login do OAuth • URL de solicitação do token OAuth
Domínio	Insira o domínio para essa conta de e-mail, a menos que você queira que o usuário receba uma solicitação para isso.
Usuário	Insira uma variável que represente o endereço de e-mail dessa conta.*
Senha da conta	Insira a senha para essa conta, a menos que você queira que o usuário receba uma solicitação para isso.
Endereço de e-mail	Insira uma variável que represente o endereço de e-mail dessa conta.*

Dias anteriores de e-mail para sincronizar	Selecione o número de dias para que o e-mail seja sincronizado entre o dispositivo e o servidor.
VPN por aplicativo	**Pré-requisito:** configure o Tunnel ou qualquer configuração VPN por aplicativo antes de configurar a VPN por aplicativo na configuração do Exchange ActiveSync. No menu suspenso, selecione a configuração de VPN por aplicativo pré-configurada. **Aplicável a**: iOS 14+
Android e Windows	
Sincronizar calendário	**Para Android, Windows Phone 8.1 e Windows 10:** selecione para sincronizar itens de calendário entre o dispositivo e o servidor. **Para dispositivos Samsung:** esta configuração não é usada (está ATIVADA por padrão). **Para aplicativo Android Email+:** esta configuração é usada.
Sincronizar contatos	**Para Android, Windows Phone 8.1 e Windows 10:** selecione para sincronizar contatos entre o dispositivo e o servidor. **Para dispositivos Samsung:** esta configuração não é usada (está ATIVADA por padrão). **Para aplicativo Android Email+:** esta configuração é usada.

Sincronizar e-mail	**Para Android, Windows Phone 8.1 e Windows 10:** selecione para sincronizar o e-mail entre o dispositivo e o servidor. **Para dispositivos Samsung:** esta configuração não é usada (está ATIVADA por padrão). **Para aplicativo Android Email+:** esta configuração não é usada (está ATIVADA por padrão).
Sincronizar tarefas	**Para Android, Windows Phone 8.1 e Windows 10:** selecione para sincronizar tarefas entre o dispositivo e o servidor. **Para dispositivos Samsung:** esta configuração não é usada (está ATIVADA por padrão). **Para aplicativo Android Email+:** não aplicável.
iOS 13.0+	
• Sincronizar calendário • Sincronizar contatos • Sincronizar e-mail • Sincronizar notas • Lembretes de sincronização	Especifique a sincronização individual de itens do Outlook Exchange, como Calendário, Contatos, E-mail, Notas e Lembretes. Para cada item, selecione ou desmarque as opções **Ativar** e **Permitir substituição do usuário**. A sincronização deve ser ativada pelo menos para um desses itens. Se você desativar a sincronização de uma das opções, mas permitir a substituição do usuário, o usuário ainda poderá ativá-la.

Certificado de identidade	Selecione um certificado de identidade na lista se quiser que o dispositivo se autentique no servidor usando um certificado. Os certificados são exibidos nesta lista somente se eles já tiverem sido configurados usando uma configuração de certificado de identidade.
Android	
Usar somente autenticação baseada em certificado	Use o certificado de identidade selecionado como a única maneira de autenticação do servidor Exchange.
Aceitar todos os Certificados SSL	Selecione para permitir que os usuários de dispositivo configurem os dispositivos Android para aceitar todos os certificados SSL. Esta configuração se aplica ao Android Email+ e ao Samsung Knox Email. • Cuidado ao ativar essa configuração, pois os usuários do dispositivo podem expor, sem saber, seu dispositivo a ataques. • Esta opção precisa ser habilitada se o certificado do Sentry for um certificado desconhecido ou autoassinado.
Prioridade do aplicativo do Exchange	Selecione o cliente de e-mail a ser configurado por padrão em dispositivos Android: Android Email+ e Samsung Email. O aplicativo Email+ é adicionado ao App Catalog para todos os locatários que têm a prioridade do aplicativo do Exchange ativada.

iOS 10+	
Regras de serviço de comunicação	Escolha um aplicativo padrão para usar a fim de fazer chamadas de áudio para contatos do sistema CardDAV.
Apenas Windows10+	
Configurar Outlook	Selecione essa opção para configurar o Microsoft Outlook em um dispositivo. Haverá suporte para essa opção somente se o Bridge estiver ativado.

*Digite $ para ver uma lista de variáveis suportadas, se disponível, para esse campo.

Configuração de fonte

A configuração da fonte permite fornecer arquivos de fonte TrueType ou OpenType adicionais nos dispositivos iOS 7. A tabela a seguir descreve as configurações de fonte:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Fazer upload de fontes	Arraste o arquivo de fonte até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo do seu sistema de arquivos. Os arquivos de fonte devem ser arquivos .otf ou .ttf.

Para obter mais informações, consulte Como criar uma configuração

Configuração do calendário assinado

Uma configuração de calendário assinado define o acesso a um calendário da web público.

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
URL	Insira o URL para acessar o calendário.*
Usuário	Insira o nome de usuário a ser usado para acesso.*
Senha	Insira a senha para o acesso.
Usar SSL	Selecione para usar somente uma camada de soquete segura para comunicações entre o dispositivo e o servidor.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Para obter mais informações, consulte Como criar uma configuração

Criar uma configuração de Web Clip

Um Web Clip é um atalho a um site ou página da web para um dispositivo iOS. Use uma configuração de Web Clip para criar web clips padrões nos dispositivos. Você pode adicionar ao seu dispositivo iOS um ícone de web clip que inicie um site específico. Os Web Clips ajudam você a encontrar e usar marcadores rapidamente nas telas iniciais de seus dispositivos. Você também pode controlar alguns parâmetros da experiência de visualização do Mobile Safari para o site.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Clique em **Configurações**.
3. Clique em **+Adicionar**.
4. Procure e selecione a configuração Web Clip.
5. Defina as configurações nessa página. Consulte a tabela no tópico **Definições de Configuração de Web Clip** para obter orientação sobre os valores.
6. Clique em **Avançar** para configurar as definições de distribuição.
7. Selecione **Personalizado** e, em seguida, selecione **Dispositivos/Grupos de dispositivos**.
8. Clique em **Concluído**.

Definições de Configuração de Web Clip

A tabela a seguir lista as definições de configuração de Web Clip:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Rótulo	Insira o texto que deseja exibir abaixo do atalho na tela do dispositivo.*
URL	Insira o URL que o web clip acessará.*
Removível	Marque a caixa de seleção para permitir que o usuário do dispositivo exclua o web clip.
Ícone	Arraste o arquivo de ícone até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo do seu sistema de arquivos.
Ícone pré-composto	Selecione para eliminar os efeitos especiais adicionados pelas versões mais recentes do Safari.
Tela inteira	Selecione para exibir o Web Clip no modo de tela cheia ao invés de conteúdo no navegador.
Ignorar escopo do manifesto	Selecione para permitir a navegação para um site externo sem exibir o navegador Safari. Esta opção não tem efeito quando Tela Inteira não está selecionada.
Identificador do pacote de aplicativo de destino	O identificador de pacote de aplicativo que especifica qual aplicativo abre a URL. **Exemplo**: com.google.chrome.ios

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Tópicos relacionados:

- Entrada segura multiusuário para iOS
- Como criar uma configuração

Instalação do Office 365

Licença: Silver

Aplicável a: Windows 10+

Configurar a Instalação do Office 365

A instalação do Office 365 é uma configuração que pode ser aplicada aos dispositivos selecionados para instalar ou desinstalar o Office 365. Você pode definir as configurações no formato xml usando a ferramenta de implantação do Microsoft Office e, em seguida, carregar o arquivo. Após carregar os arquivos, você poderá enviar por push as opções de configuração para os dispositivos selecionados.

Procedimento

1. Na aba **Configuração**, clique em **+Adicionar**.
2. Selecione **Instalação do Office 365**. A página **Instalação do Office 365** é exibida.
3. No campo **Nome**, digite um nome apropriado para a configuração.
4. Clique no link +**Adicionar descrição** para adicionar uma descrição para a configuração. Este campo

é opcional.

5. Na seção **Configuração**, atualize os seguintes campos:

Nome do campo	Descrição
Arquivo de configuração para instalação do Office 365	Clique no botão **Escolher arquivo** para procurar e selecionar o arquivo de configuração no formato XML que inclui as configurações definidas para a Instalação do Office 365. Exemplo: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> Certifique-se de que o arquivo de configuração esteja no formato xml e a marca de seleção verde seja exibida após adicionar o arquivo de configurações.

Arquivo de configuração para desinstalar o Office 365	Clique no botão **Escolher arquivo** para procurar e selecionar o arquivo no arquivo de configuração no formato XML que inclui as configurações definidas para desinstalar o Office 365. Exemplo: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> Certifique-se de que o arquivo de configuração esteja no formato xml e a marca de seleção verde seja exibida após adicionar o arquivo de configurações.

6. Clique em **Avançar**.

7. Selecione uma das opções a seguir para distribuir as configurações para os dispositivos.

Opção	Descrição
Ativar essa configuração	Selecionar a caixa de seleção permite esta configuração para os dispositivos selecionados. Desmarcar a caixa de seleção, exclui a configuração, se já aplicada nos dispositivos.
Todos os dispositivos	Distribui as configurações para todos os dispositivos.
Nenhum dispositivo	Retém as configurações a serem distribuídas para o(s) dispositivo(s).
Personalizada	Distribui as configurações para um grupo definido de dispositivos. Marque a caixa de seleção ao lado do tipo de dispositivo para o qual deseja distribuir as configurações. Como alternativa, você pode procurar grupos de dispositivos digitando o nome do grupo no campo **Pesquisar grupos de dispositivos**. Se desejar criar um novo grupo de dispositivos, clique no link **Criar novo grupo de dispositivos** na parte inferior da página. Consulte Grupos de dispositivos para obter mais informações. Quando você seleciona a categoria do dispositivo, pode observar os detalhes (**NOME**, **NÚMERO DE TELEFONE** e **TIPO DE DISPOSITIVO**) na lista de usuários do dispositivo para a categoria selecionada na seção **Resumo da distribuição**.

8. Clique em **Concluído** para enviar por push a configuração para os dispositivos selecionados.

Configurações de GPO do Windows

Licença: Bridge

Aplicável para: Windows Desktop

Definição das Configurações de GPO do Windows

O Objeto de Política de Grupo (GPO) é uma coleção de definições que estabelecem as permissões sobre o que os dispositivos estão ou não habilitados a fazer. É um pré-requisito ter uma configuração do Bridge para gerenciar as configurações de GPO. Consulte Ivanti Bridge para mais detalhes.

Entre em contato com o administrador do site se os metadados de GPO não estiverem carregados no banco de dados. A configuração de GPO é implementada nos dispositivos por scripts de PowerShell pelo Bridge. Com as configurações de GPO você pode configurar e enviar configurações específicas para os dispositivos.

Procedimento

1. Na aba **Configuração**, clique em **+Adicionar**.
2. Selecionar a configuração **Configurações de GPO do Windows**. A página **Configurações de GPO do Windows**será exibida.
3. No campo **Nome**, digite um nome apropriado para as Configurações de GPO do Windows.
4. Clique no link +**Adicionar descrição** para adicionar uma descrição para a configuração. Esse campo é opcional.
5. Na seção **Configuração**, clique em +**Adicionar**. Uma janela **Adicione Objeto de Política de Grupo (GPO) do Windows** será exibida.
6. Pesquise e selecione um GPO clicando no componente relevante da árvore hierárquica de GPO no painel esquerdo. A árvore hierárquica de GPO representa o caminho das configurações de política. Alternativamente, você pode pesquisar por uma configuração de GPO específica digitando o nome das configurações de GPO no campo Pesquisa.
   Após selecionar uma configuração de GPO, você pode visualizar os detalhes da configuração de GPO selecionada no painel à direita.

7. No campo **Status da configuração**, estão disponíveis as seguintes opções:

Opção	Descrição
Não configurado	Remove configurações de GPO existentes.
Ativado	Ativa as configurações de GPO.
Desativado	Desativa as configurações de GPO.

8. No campo **Valor da Configuração**, digite um nome apropriado para o GPO.

Este campo é editável apenas quando a opção **Habilitado** está selecionada em **Status da configuração**.

Para adicionar valores de configurações adicionais, clique no ícone **+**. Algumas configurações de GPO podem não precisar de nenhum Valor de configuração adicional. Alguns podem exigir que dados adicionais sejam especificados em Valor da configuração, na forma de valor de texto. Em tais configurações, selecione qualquer valor nos valores suspensos disponíveis.

9. Clique em **Salvar e Fechar** para salvar o GPO e fechar a janela. Se desejar adicionar outro GPO, clique em **Salvar e Adicionar outro** para salvar e continuar com a janela de GPO aberta.
   A configuração de GPO adicionada será exibida na seção **Configuração**.

   É possível editar ou excluir uma configuração de GPO clicando nos ícones relevantes na coluna **Ações**.

Opção	Descrição
Ativar essa configuração	Selecionar a caixa de seleção permite esta configuração para os dispositivos selecionados. Desmarcar a caixa de seleção, exclui a configuração, se já aplicada nos dispositivos.
Todos os dispositivos	Distribui as configurações para todos os dispositivos.
Nenhum dispositivo	Retém as configurações a serem distribuídas para o(s) dispositivo(s).
Personalizada	Distribui as configurações para um grupo definido de dispositivos. Marque a caixa de seleção ao lado do tipo de dispositivo para o qual deseja distribuir as configurações. Como alternativa, você pode procurar grupos de dispositivos digitando o nome do grupo no campo **Pesquisar grupos de dispositivos**. Se desejar criar um novo grupo de dispositivos, clique no link **Criar novo grupo de dispositivos** na parte inferior da página. Consulte Grupos de dispositivos para obter mais informações.

	Quando você seleciona a categoria do dispositivo, pode observar os detalhes (**nome**, **número de telefone** e **tipo de dispositivo**) na lista de usuários do dispositivo para a categoria selecionada na seção **Resumo da distribuição**.

10. Clique em **Concluído** para enviar a configuração de GPO para os dispositivos selecionados.

Configuração da criptografia BitLocker

Licença: Bridge

Aplicável para: Windows Desktop

Esta seção contém os seguintes tópicos:

- Configuração da criptografia BitLocker
- Visualização das configurações do BitLocker

Configuração da criptografia BitLocker

A criptografia BitLocker é um recurso que impinge a criptografia em discos rígidos e unidades removíveis dos dispositivos para proteção dos dados. A configuração do Bridge é obrigatória para o gerenciamento da criptografia BitLocker. Consulte Bridge para mais detalhes. A configuração da criptografia BitLocker ajuda a configurar as definições de criptografia nos dispositivos.

Procedimento

1. Na aba **Configuração**, clique em **+Adicionar**.
2. Selecione a configuração **Criptografia BitLocker**. A página **Criptografia BitLocker** é exibida.
3. No campo **Nome**, insira um nome apropriado para a criptografia BitLocker.
4. Clique no link **+Adicionar descrição** para adicionar uma descrição para a configuração. Esse campo

é opcional.

5. Na seção Configuração, configure as definições a seguir:

Configuração	Descrição
Método e tipo de criptografia	Selecione o tipo do algoritmo de criptografia com base no tamanho da chave de criptografia. As seguintes opções estão disponíveis: • **AES-CBL de 128 bits** • **AES-CBL de 256 bits**
Criptografar todas as unidades de hardware	Clique no botão de alternar para **ATIVAR** ou **DESATIVAR** a configuração de criptografia de todas as unidades de hardware. Se alguma unidade de hardware já estiver criptografada em um dispositivo, a edição dessa configuração não será aplicada, pois o processo de criptografia não pode ser revertido por meio de edição.
Selecionar unidades	Selecione as unidades que precisam ser criptografadas. Exemplo: **C:** Clique em **+Adicionar** para adicionar mais unidades. Esse campo não será exibido se você tiver ativado a configuração **Criptografar todas as unidades de hardware**.

Configuração	Descrição
Criptografia baseada em hardware para tipos de unidade	Trusted Platform Module (TPM) é um chip na placa-mãe do computador que auxilia na criptografia resistente à adulteração. Ao usar a criptografia BitLocker ou criptografia do dispositivo em um computador com TPM, parte da chave é armazenada no TPM. É possível escolher as seguintes opções de configuração de criptografia baseada em hardware na lista suspensa: • **Exigir TPM na inicialização** • **Exigir PIN de inicialização com TPM** • **Não usar TPM** A opção TPM é aplicável somente a unidades do SO e o TPM versão 1.2 ou mais recente. Se você aplicar uma configuração de criptografia baseada em hardware a um dispositivo, não será mais possível editar essa configuração no dispositivo. Se um dispositivo já estiver configurado com uma configuração BitLocker, não será possível aplicar uma segunda configuração BitLocker com uma opção de TPM diferente.

Configuração	Descrição
Selecione as seguintes opções de configuração (opcional): • **Negar acesso de gravação às unidades fixas não protegidas pelo BitLocker** • **Negar acesso de gravação às unidades removíveis não protegidas pelo BitLocker**	
Ação de dispositivo pré-criptografado	Selecione qualquer uma das seguintes opções para definir como lidar com uma unidade que não está totalmente descriptografada ou que já tem um protetor de chave. • **Interromper criptografia -** interrompe a criptografia se alguma das unidades selecionadas já estiver criptografada. • **Descriptografar a unidade selecionada que não tenha uma senha de recuperação armazenada no Ivanti Neurons for MDM -** selecione essa opção para limitar a aplicação apenas às unidades que não tenham uma senha de recuperação no Ivanti Neurons for MDM.

Configuração	Descrição
Opções de recuperação	A opção de recuperação é usada quando o usuário esquece a senha. É possível recuperar a senha na página de detalhes do dispositivo. é possível configurar as seguintes opções de recuperação: • **Desativar recuperação** • **Usar senha e armazenar no AD** • **Usar senha e armazenar no AD e no MobileIron**
Intervalo de reinicialização	Depois de enviar a configuração por push ao dispositivo, ele solicita uma reinicialização. A criptografia inicia após a reinicialização. Para configurar o intervalo de reinicialização da lista suspensa, selecione uma duração de tempo que o dispositivo deve levar para reinicializar. O intervalo mínimo de reinicialização é 1 minuto e o intervalo máximo de reinicialização é 120 minutos (2 horas).
Mensagem de reinicialização	Insira a mensagem de reinicialização a ser exibida no dispositivo. Se aplicável, a senha ou o PIN de inicialização também é exibido ao usuário. O usuário pode anotá-lo para inseri-lo quando solicitado após a reinicialização.

6. Clique em **Avançar**.

7. Selecione uma das opções a seguir para distribuir as configurações para os dispositivos.

Configuração	Descrição
Ativar essa configuração	Selecionar a caixa de seleção permite esta configuração para os dispositivos selecionados. Desmarcar a caixa de seleção, exclui a configuração, se já aplicada nos dispositivos.
Todos os dispositivos	Distribui as configurações para todos os dispositivos.
Nenhum dispositivo	Retém as configurações a serem distribuídas para o(s) dispositivo(s).
Personalizada	Distribui as configurações para um grupo definido de dispositivos. Marque a caixa de seleção ao lado do tipo de dispositivo para o qual deseja distribuir as configurações. Como alternativa, você pode procurar grupos de dispositivos digitando o nome do grupo no campo **Pesquisar grupos de dispositivos**. Se desejar criar um novo grupo de dispositivos, clique no link **Criar novo grupo de dispositivos** na parte inferior da página. Consulte Grupos de dispositivos para obter mais informações. Quando você seleciona a categoria do dispositivo, pode observar os detalhes (**NOME**, **NÚMERO DE TELEFONE** e **TIPO DE DISPOSITIVO**) na lista de usuários do dispositivo para a categoria selecionada na seção **Resumo da distribuição**.

8. Clique em **Concluído** para enviar por push a configuração para os dispositivos selecionados.

Visualização das configurações do BitLocker

É possível visualizar as configurações do BitLocker definidas na página de detalhes do Dispositivo (**Dispositivos>Dispositivos>[Nome do dispositivo]**) sob a seção **Configurações do Bitlocker**. Por padrão, os detalhes estão ocultos.

Você pode visualizar os seguintes detalhes clicando no ícone de visualização (em formato de olho) ao lado de cada campo:

Configuração	Descrição
Senha de recuperação	Quando esta opção é selecionada, a senha de recuperação é gerada pelo Windows e transmitida ao Ivanti Neurons for MDM após o envio da configuração do BitLocker. Se o dispositivo passar pelo modo de recuperação, o usuário será solicitado a inserir essa senha. A mesma senha de recuperação deve ser utilizada se várias unidades foram criptografadas. A senha de recuperação será publicada somente se a opção de recuperação **Usar senha e armazenar no AD e no MobileIron** estiver selecionada.
PIN	Exibe o PIN de inicialização de 6 dígitos. O PIN será exibido somente se a opção **Exigir PIN de inicialização com TPM** estiver selecionada na configuração do BitLocker.
Senha de inicialização	A senha de inicialização definida para o dispositivo. A senha de inicialização será exibida somente se a opção **Não usar TPM** estiver selecionada na configuração do BitLocker.
Versão do TPM	Exibe a versão do TPM configurado.

Alguns campos podem exibir **N/A** com base nas definições presentes na configuração do BitLocker.

- O status da criptografia é exibido no status de criptografia do dispositivo na página de detalhes do dispositivo.
- A mesma senha ou PIN de inicialização será usada para todas as unidades do dispositivo no qual o BitLocker deve ser aplicado.
- Se você criar uma configuração para criptografar uma segunda unidade de um dispositivo que já tenha uma unidade criptografada e uma senha de recuperação salva, a senha antiga será substituída. Então, recomendamos que a opção Senha de recuperação seja usada somente para uma unidade no dispositivo.

Configuração do acesso à rede corporativa

Esta seção contém os seguintes tópicos:

Configuração do AirPlay

Licença: Silver

A configuração do AirPlay define o acesso para alternar dispositivos para a exibição de mídia. A tabela a seguir lista as configurações do AirPlay:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Lista de permissão	Insira a ID do dispositivo de cada destino do AirPlay permitido. Se você não listar um ID, os destinos do AirPlay não estarão restritos. **Aplicável a**: iOS 7.0+ e macOS 10.10+ (Supervisionado).
Configurações do dispositivo	Insira o ID do dispositivo (macOS) ou o nome do dispositivo (iOS) e a senha para cada destino conhecido do AirPlay.

Para obter mais informações, consulte Como criar uma configuração

Configuração do AirPrint

Licença: Silver

Uma configuração do AirPrint define a impressão sem fio. A tabela a seguir lista as configurações do AirPrint:

Ajustes	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Configurações do AirPrint	**Endereço IP:** insira o endereço IP da impressora AirPrint. **Caminho de recursos:** insira o caminho de recursos associado à impressora AirPrint. Ele corresponde ao parâmetro rp do registro _ ipps.tcp Bonjour. Exemplos: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. O caminho de recursos faz distinção entre letras maiúsculas e minúsculas. **Porta:** Insira a porta de escuta do destino do AirPrint. Se ela não for especificada, o AirPrint usará a porta padrão. Para mais detalhes sobre as portas padrão da Apple, acesse https://support.apple.com/en-us/HT202944 **Forçar TLS**: permite ativar a proteção da conexão pelo Transport Layer Security (TLS). Por padrão, essa configuração está desativada.

Após a instalação da configuração do **AirPrint** no Mac OS, os detalhes da impressora são enviados por meio da configuração do **AirPrint** para o dispositivo. Os usuários podem ver os detalhes da impressora preenchidos automaticamente clicando em **Preferências do sistema> Impressoras e scanners> +**. Na tela **Adicionar**, o usuário deve selecionar **Padrão** e selecionar o perfil de impressão necessário. Isso adiciona a impressora necessária a **Impressoras e scanners**.

Para obter mais informações, consulte Como criar uma configuração

Configuração VPN Sempre Ativa

Licença:

- **Gold para Android Enterprise**
- **Silver para iOS**

A configuração VPN Sempre Ativa garante que os usuários sejam conectados automaticamente à VPN (quando disponível) sem precisar realizar nenhuma ação. Este recurso exige o Android 7.0 ou superior ou iOS 8 ou superior, bem como um provedor de VPN compatível com o Protocolo IKEv2.

Configurações de VPN Sempre Ativa para Android

A configuração VPN Sempre Ativa é enviada aos dispositivos Android Enterprise com Android 7.0 +. No dispositivo gerenciado com Perfil de trabalho (Android 8.0 ou superior), a configuração da VPN é aplicada no Perfil de trabalho.

Quando um dispositivo é implantado no modo **COSU** tendo **AMA** como o tipo de registro de dispositivo, e se um app com a configuração **Sempre ativo** for enviado ao dispositivo, então a configuração **Sempre ativo** também será enviada ao dispositivo.

Para habilitar essa configuração, selecione um aplicativo no App Catalog ou insira um nome de pacote.

Configurações de VPN Sempre Ativa para iOS

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Utilize a mesma configuração de túnel para Celular e Wi-Fi	Selecione para definir um único par de identificações de servidor para conexões VPN, independentemente de a conexão ser estabelecida por celular ou rede Wi-Fi.
Servidor	Insira o nome do host ou endereço IP do servidor VPN.
Identificador local	Identificador do cliente IKEv2 em um dos formatos a seguir: • FQDN • UserFQDN • Endereço • ASN1DN
Identificador remoto	Identificador remoto em um dos formatos a seguir: • FQDN • UserFQDN • Endereço • ASN1DN
Ativar EAP	Selecione para ativar a autenticação estendida.

Autenticação da máquina	Disponível apenas se a opção Ativar EAP não estiver selecionada. Selecione uma das opções a seguir: • Certificado • Segredo compartilhado
Autenticação EAP	Disponível apenas se a opção Ativar EAP estiver selecionada. Selecione uma das opções a seguir: • Certificado • Nome de usuário/senha
Segredo compartilhado	Disponível apenas se Segredo Compartilhado estiver selecionado para Autenticação da Máquina. Insira o segredo compartilhado da conexão.
Credencial	Disponível apenas se Certificado foi selecionado para a Autenticação da Máquina. Selecione o certificado a ser utilizado. Esse certificado será enviado para autenticação do cliente IKE. Se a autenticação estendida for utilizada, esse certificado pode ser utilizado para EAP-TLS.
Conta	Disponível apenas se Nome de Usuário/Senha estiver selecionado para Autenticação EAP. Insira o ID da conta para o servidor VPN.
Senha	Disponível apenas se Nome de Usuário/Senha estiver selecionado para Autenticação EAP. Insira a senha para o servidor VPN.

Intervalo de detecção de par morto	Selecione uma das opções a seguir: • Nenhum (Desativar) • Baixo (keepalive enviado a cada hora) • Médio (keepalive enviado a cada 30 minutos) • Alto (keepalive enviado a cada 10 minutos)
Algoritmo de criptografia	Selecione uma das opções a seguir: • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
Algoritmo de integridade	Selecione uma das opções a seguir: • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
Grupo Diffie-Hellman	Selecione o grupo de troca de chaves do D-H.

Vida útil em minutos	Insira a vida útil do SA (intervalo de rechaveamento) em minutos. Valores válidos são 10 a 1440.
Correio de Voz	Selecione Permitir tráfego via túnel para tornar o correio de voz isento da opção VPN Sempre Ativa. Selecione Ignorar tráfego para que não seja isento.
AirPrint	Selecione Permitir tráfego via túnel para tornar o tráfego Airprint isento da opção VPN Sempre Ativa. Selecione Ignorar tráfego para que não seja isento.
Serviços de celular	Selecione Permitir tráfego via túnel para tornar o tráfego de serviços celulares isento da opção VPN Sempre Ativa. Selecione Ignorar tráfego para que não seja isento.
Permitir tráfego de folha de web interna fora do túnel VPN	Selecione para permitir tráfego de folhas de web internas fora do túnel VPN.
Permitir tráfego de todos os apps de rede interna fora do túnel VPN	Selecione para permitir tráfego de todos os apps de rede interna fora do túnel VPN para realizar o manuseio da rede interna.
Aplicativos de Rede Interna Identificadores de Pacote	Liste os IDs de pacote para aplicativos de rede cativos cujo tráfego será permitido fora do túnel VPN para realizar o manuseio da rede cativa. Apps de rede interna podem precisar de direitos adicionais para funcionarem em um ambiente interno.

Para obter mais informações, consulte Como criar uma configuração

Permissões padrão de tempo de execução do aplicativo

Aplicável a: Apps desenvolvidos para API Android 23 ou superior e que executam Android 6.0 ou superior em dispositivos com Android Enterprise.

Os administradores podem configurar permissões de tempo de execução para os apps implantados em dispositivos empresariais Android. Os apps desenvolvidos para a API 23 (ou mais recente) e com o Android 6.0 ou mais recente podem solicitar permissões aos usuários em tempo de execução. A configuração Permissões padrão de tempo de execução do aplicativo define o padrão dessas permissões de tempo de execução do aplicativo. Ivanti Neurons for MDM cria esta configuração por padrão. Você pode editar esta configuração padrão do sistema ou criar uma nova configuração baseada nos seus requisitos.

As permissões específicas do aplicativo têm precedência sobre a configuração geral de permissões de aplicativo. Os apps internos estão sujeitos às permissões globais. A configuração de permissões por aplicativo para os apps internos não é suportada.

Configuração de permissões globais de tempo de execução

Os administradores podem editar as permissões padrão de tempo de execução do aplicativo e a distribuição dessa configuração da seguinte forma:

ProcedureProcedimento

1. Vá até **Configurações**.
2. Execute uma das seguintes ações:
    - Para editar as configurações padrão do sistema clique em **Permissões padrão de tempo de execução do aplicativo** e clique em **Editar**.
    - Para adicionar uma nova configuração, clique em **Adicionar > Permissões padrão de tempo de execução do aplicativo**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Definição de configuração, defina uma das seguintes permissões padrão de tempo de execução:

- Prompt de usuário (opção padrão)
- Concessão automática
- Negação automática (usar com cautela)

6. Clique em **Avançar**.
7. Selecione a opção **Habilitar essa configuração**.

> Se você desmarcar essa opção, a configuração não será aplicada a nenhum dispositivo. Ela será removida de todos os dispositivos aos quais foi aplicada anteriormente.

8. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizada
9. Clique em **Concluído** .

Configuração de permissões de tempo de execução específicas do aplicativo

Os administradores podem definir as permissões de tempo de execução de um aplicativo individual, como segue:

Procedimento

1. Acesse **Apps**.
2. Clique no nome do aplicativo.
3. Clique em **Configurações do aplicativo > Android Enterprise**.
4. Clique em **Adicionar** ou clique no nome da configuração para editar uma configuração existente.
5. Defina as opções de configuração, como nome, descrição e restrições.
6. Na seção Permissões de tempo de execução, clique em **Gerenciar permissões**.

7. Selecione as permissões na janela exibida e clique em **Selecionar**.
   Somente as permissões perigosas apropriadas ao aplicativo específico estão listadas para seleção. A lista completa de permissões perigosas (como ler seus contatos, localizar contas no dispositivo, gravar registro de chamadas e assim por diante) está em https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.

   - As permissões são aplicadas somente quando o aplicativo solicita permissões.
   - As permissões não são aplicadas se os usuários já tiverem aceitado ou negado permissões anteriormente.

8. Na seção Permissões de tempo de execução, selecione uma das permissões padrão de tempo de execução a seguir:

   - Padrão/global (opção padrão)
   - Concessão automática
   - Negação automática (usar com cautela)

9. Na seção Distribuir essa configuração de aplicativo, selecione uma das opções de distribuição a seguir:

   - Todos com o aplicativo
   - Ninguém
   - Personalizada

10. Clique em **Salvar**.

Educação

Licença: Gold

Aplicável para: iOS 9.3+ supervisionado

Configura a carga útil de Educação da Apple e o aplicativo Classroom para líderes e membros. A tabela a seguir lista as configurações de Educação:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Tipo de configuração	Selecione um dos tipos a seguir: • Líder • Membro
Ativar essa configuração	• Selecione essa opção para aplicar essa configuração nos dispositivos selecionados. • Desmarque essa opção para remover essa configuração de todos os dispositivos, caso tenha sido aplicada anteriormente.
Distribuir	Selecione uma das opções de distribuição a seguir: • Todos os dispositivos • Nenhum dispositivo • Personalizada

Para obter mais informações, consulte Como criar uma configuração

Configuração do proxy global

Licença: Silver

A configuração do proxy global configura os dispositivos para direcionar o tráfego HTTP para um servidor proxy. A tabela a seguir lista as configurações de Proxy global:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Tipo	Selecione **Manual** ou **Automático**. Se você selecionar **Manual**, precisará do nome do host e porta do servidor proxy e, opcionalmente, um nome de usuário e senha no servidor proxy. Se você selecionar **Automático**, poderá inserir um URL de configuração automática do proxy (PAC).
Nome do host e porta	Se você selecionou **Manual**, insira o nome do host e o número da porta do servidor proxy.
Usuário	(Opcional) Nome de usuário para acessar o servidor proxy.*
Senha	(Opcional) Senha para acessar o servidor proxy.
URL do PAC	(Opcional) Se você selecionou **Automático**, você pode inserir a URL do arquivo PAC que define a configuração do proxy. Se você deixar essa configuração em branco, o dispositivo usará o protocolo de descoberta automática do proxy da web (WPAD) para descobrir proxies.
Permitir conexão direta se o PAC estiver inacessível	(iOS 7 e posterior) Selecione para permitir uma conexão direta se o dispositivo estiver inacessível para acessar o arquivo do PAC por qualquer motivo.
Permite ignorar o proxy para acessar redes internas	(iOS 7 e posterior) Selecione para permitir que o proxy seja ignorado e exibir a página de login para uma rede interna.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Para obter mais informações, consulte Como criar uma configuração

Configuração LDAP

Uma configuração LDAP configura o acesso para um diretório corporativo. A tabela a seguir lista as configurações LDAP:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome do host	Insira o nome do host para o servidor LDAP.*
Usuário	Digite o nome de usuário para acessar a conta LDAP.*
Senha	Insira a senha para acessar a conta LDAP.
Usar SSL	Selecione se você deseja usar SSL para a conexão ao servidor LDAP.
Configurações de pesquisa	Insira pelo menos uma entrada para a conta. Cada entrada representa um nó na árvore LDAP em que a pesquisa é iniciada. Clique no botão + para adicionar uma nova entrada e edite a entrada. Uma entrada consiste nos seguintes valores: Descrição: Explica o propósito da configuração da pesquisa. Escopo: **Selecione Base, Subárvore** ou **Um nível** para indicar o escopo da pesquisa. **Base** indica somente um nível de nó, **Subárvore** indica o nó e todas as ramificações, **Um nível** indica o nó e um nível de ramificação. Base de pesquisa: O caminho conceitual para a observação especificada (por exemplo, ou=people, o=mycorp).

VPN por aplicativo	**Pré-requisito**: configure o Tunnel ou qualquer configuração VPN por aplicativo antes de realizar a configuração de VPN por aplicativo em LDAP. No menu suspenso, selecione a configuração de VPN por aplicativo pré-configurada. **Aplicável a**: iOS 14+
iOS 10+	
Regras de serviço de comunicação	Escolha um aplicativo padrão para usar a fim de fazer chamadas de áudio para contatos do sistema LDAP.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Para obter mais informações, consulte Como criar uma configuração

Configuração de servidor macOS

A configuração de servidor macOS define uma conta de servidor macOS com os parâmetros e tipos de conta configurados. Essa configuração permite que o usuário ative o Compartilhamento de arquivos no servidor.

Aplicável para: iOS 10+

Configuração de servidor macOS

Procedimento

1. Acesse **Configurações > +Adicionar**.
2. Selecione a configuração **Servidor macOS** para exibir a página **Criar configuração de servidor macOS**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Insira o **Nome do host** para especificar o endereço do servidor.
6. Insira o **Nome do usuário** para especificar o nome de login do usuário.
7. (Opcional) Insira a **Senha** do usuário.
8. (Opcional) Insira a **Descrição** da conta.
9. (Opcional) Em Contas configuradas, insira o número da **porta** a ser utilizada ao contatar o servidor para a conta de dicionário de documentos. Se não for especificado nenhum número de porta, será utilizado o número de porta padrão.
10. Clique em **Avançar**.
11. Selecione uma distribuição para essa configuração.

Tunnel

Cria uma configuração da VPN por aplicativo para usar com o aplicativo Tunnel versão 2.1+. Selecione o perfil do Sentry e defina as configurações para começar a fazer o tunneling dos dados do aplicativo pelo Sentry.

Documentação mais recente

Para as instruções mais recentes do Tunnel, acesse a documentação dos produtos em **> Apps** e selecione o documento adequado para sua versão do Tunnel.

Como configurar o AppTunnel

O AppTunnel protege os dados do aplicativo ao fornecer segurança da sessão conforme o aplicativo entre cada contêiner de aplicativos e a rede corporativa.

Esta seção contém os seguintes tópicos:

- Como configurar o Sentry para usar o AppTunnel com certificados
- Como carregar certificados do Sentry
- Como configurar apps para usar o AppTunnel
- Sobre o nome de serviço AppTunnel

Como configurar o Sentry para usar o AppTunnel com certificados

Pré-requisitos

- O AppTunnel depende da versão mais recente suportada do Sentry. Conclua a instalação do Sentry antes de iniciar as tarefas de configuração do AppTunnel.
- Caso pretenda usar uma identidade SCEP:
  - Adicione uma autoridade de certificação local ou externa. É necessário instalar o Connector.
  - Adicione uma Configuração do certificado de identidade do aplicativo. Essa é a distribuição dinâmica que será usada para configurar o AppTunnel.

Você pode configurar o ActiveSync e/ou o App Tunnel usando certificados X.509 para autenticação para usar os servidores Sentry atribuídos a um perfil.

Procedimento

1. Acesse **Administrador** > **Sentry**.
2. Clique em **+ Adicionar perfil do Sentry**.
3. Clique em **ActiveSync e/ou AppTunnel com certificados**.

4. Clique em **Avançar**.

5. Use as diretrizes da tabela a seguir para preencher a página **Configurações globais**.

Tabela: Configurações globais para Admin > Sentry	
Configuração	**O que fazer**
Nome	Insira um nome que identifique esse perfil.
Descrição	Insira uma descrição que esclareça o objetivo deste perfil.
Nome do host externo e porta	Insira o nome de porta e host externo para o Sentry.
Modo de autenticação do Dispositivo	
Usar apenas um certificado para a autenticação de dois fatores	Selecione para usar apenas um certificado para a autenticação. Se você ainda não tem um certificado carregado, pode carregá-lo na área exibida abaixo da opção selecionada.
Selecionar certificado	Para carregar um certificado de grupo necessário para autenticação do dispositivo: a. Clique em **Adicionar**. A janela **Adicionar certificado** é exibida. b. Digite o nome do fabricante no campo **Nome do certificado**. c. Digite a senha que protege o arquivo PKCS12. d. Clique em **Escolher arquivo** para carregar o certificado do grupo. Verifique se o formato do arquivo está em .p7b, .p12, .pfx, .pem, .der, .crt ou .cer.

Ativar lista de certificados revogados (CRL)	Selecione para validar os certificados apresentados pelo dispositivo em relação à Lista de revogação de certificados (CRL) publicada pela CA.
Comportamento padrão dos dispositivos não gerenciados	
Permitir que os dispositivos não gerenciados recebam e-mail e dados	Selecione se não desejar bloquear o acesso de dados para dispositivos não gerenciados pelo Ivanti Neurons for MDM.

6. Clique em **Avançar**.
7. Na página **Configuração do servidor Sentry**, configure os seguintes campos.

Tabela: Configuração do servidor Sentry para Administrador > Sentry	
Configuração	**O que fazer**
Protocolo de escuta	Selecione qualquer uma das opções de protocolo a seguir: • **Somente HTTPS** • **Somente HTTP** • **HTTPS e HTTP**
Porta Https	Digite o número da porta Https. Esse campo não será exibido se o protocolo de escuta estiver selecionado como Somente HTTP.
Porta Http	Digite o número da porta Http. Esse campo não será exibido se o protocolo de escuta estiver selecionado como Somente HTTPS.
Certificado/chave do servidor TLS Sentry	
Usar certificado autoassinado do Sentry	Selecione para usar um certificado autoassinado criado pelo serviço Ivanti Neurons for MDM e enviado ao Sentry como parte deste perfil. Este certificado é usado para comunicação entre o Sentry e os dispositivos móveis.

Adicionar	Para carregar seu próprio certificado necessário para autenticação: a. Clique em **Adicionar**. A janela **Adicionar certificado** é exibida. Você poderá ver essa opção somente quando desmarcar a opção **Usar certificado autoassinado do Sentry**. b. Digite o nome do fabricante no campo **Nome do certificado**. c. Digite a senha que protege o arquivo PKCS12. d. Clique em **Escolher arquivo** para carregar o certificado. Verifique se o formato do arquivo está em .p7b, .p12, .pfx, .pem, .der, .crt ou .cer. e. Clique em **Adicionar**. Todos os certificados de servidor TLS carregados (incluindo os certificados carregados da página principal do Sentry e de outros perfis) são exibidos na seção Certificado/Chave do servidor TLS Sentry. Para selecionar o certificado TLS necessário para autenticação, clique no botão de opção ao lado do certificado.
Protocolos	Selecione os protocolos de entrada e saída necessários.

Conjuntos de codificação	As codificações são utilizadas na comunicação criptografada pelo SSL com o Sentry. Geralmente, são preferidas as codificações fortes. Codificações fracas podem ser necessárias para dispositivos antigos. As codificações fortes são selecionadas por padrão. Selecione as codificações adicionais que deseja utilizar. Pelo menos uma codificação deve ser selecionada.

8. Clique em **Avançar**.
9. Adicione pelo menos um dos serviços exibidos.
10. Clique em **Salvar**.

Depois de registrar o Sentry, ele será exibido na página Sentry da seção Servidores Sentry não configurados. Para atribuir um perfil ao Sentry, clique em **Atribuir** na coluna **Ações**.

Como carregar certificados do Sentry

Ivanti Neurons for MDM carrega os certificados do servidor TLS e de grupo ao criar um perfil do Sentry. Você também pode carregar esses certificados da página **Sentry** na seção **Certificados do Sentry**.

O Ivanti Neurons valida os certificados Sentry no carregamento, retornando os seguintes tipos de informações dependendo das condições encontradas nos certificados:

Condição	Tipo de informação
O certificado de folha não contém uma cadeia para nenhuma autoridade de certificação ou não há nenhuma autoridade de certificação no arquivo carregado.	Erro
Não há autoridade de certificação raiz disponível.	Perigo
A autoridade de certificação raiz não assinou a autoridade de certificação intermediária para o certificado de folha.	Perigo

Ivanti Neurons for MDM também valida de acordo com as regras nesse artigo.

Procedimento

1. Na seção **Certificados do servidor TLS**, clique em **Adicionar**. A janela **Adicionar certificado** é exibida.
2. Digite o nome do fabricante no campo **Nome do certificado**.
3. Digite a senha que protege o arquivo PKCS12.
4. Clique em **Escolher arquivo** para carregar o certificado do grupo. Verifique se o formato do arquivo está em .p7b, .p12, .pfx, .pem, .der, .crt ou .cer.
5. Clique em **Adicionar**. O certificado carregado é exibido na tabela.
6. Para excluir o certificado do servidor TLS, clique no ícone Excluir na coluna **Ações**.

Se o certificado do servidor TLS for usado em qualquer perfil do Sentry, você não poderá excluir o certificado. Será exibida uma mensagem de erro se a ação de exclusão for executada.

Adicionar certificados de grupo

Procedimento

1. Na seção **Certificados de grupo**, clique em **Adicionar**. A janela **Adicionar certificado** é exibida.
2. Digite o nome do fabricante no campo **Nome do certificado**.
3. Digite a senha que protege o arquivo PKCS12.
4. Clique em **Escolher arquivo** para carregar o certificado do grupo. Verifique se o formato do arquivo está em .p7b, .p12, .pfx, .pem, .der, .crt ou .cer.
5. Clique em **Adicionar**.

Para excluir o certificado de grupo carregado, clique no ícone Excluir na coluna **Ações**.

Como configurar apps para usar o AppTunnel

Para obter as instruções mais recentes do Sentry, acesse Documentação do produto e clique em Sentry. Selecione o documento apropriado para sua versão do Sentry.

Sobre o nome de serviço AppTunnel

Um serviço AppTunnel define o serviço de backend ao qual um aplicativo AppConnect é vinculado.

Para obter as instruções mais recentes, visite a Documentação do produto e selecione os documentos adequados para suas versões do Sentry e do AppConnect.

Configuração VPN por aplicativo

Licença: Silver

Aplicável para: dispositivos iOS

Uma configuração VPN por aplicativo define as configurações para o acesso à rede privada virtual dos apps específicos a seguir:

- Configurações VPN por aplicativo
- Psec (Cisco)
- Cisco AnyConnect
- SSL Juniper
- VPN NetMotion
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- SSL personalizado
- GlobalProtect da Palo Alto Networks

> Configuração VPN por aplicativo é dependente da Configuração do aplicativo. Configuração VPN por aplicativo é criada durante a Configuração do aplicativo. Quando Configuração VPN por aplicativo é excluída ou não distribuída, a Configuração do aplicativo apresenta problema desconectando o Aplicativo da rede.

Configurações VPN por aplicativo

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Tipo de conexão	Selecione o tipo de VPN para configurar. As configurações restantes dependem dessa seleção.
Habilitar VPN sob demanda	Selecione para usar essa configuração para domínios e nomes do host que estabelecem uma VPN sob demanda.

Ativar regras do iOS (Aplicável se a opção Habilitar VPN sob demanda estiver selecionada)	Para iOS e macOS, você pode configurar: • Regras da rede que permitem ou impedem conexões e permitem ou ignoram, as redes que são avaliadas como verdadeiras. • As regras de conexão permitem quando necessário, ou nunca permitem, conexões com as redes que são avaliadas como verdadeiras. Para as regras da rede, você pode especificar os seguintes tipos de parâmetros: • Associação de domínio de DNS • Associação de endereço do servidor de DNS • Associação de SSID • Investigação da sequência da URL • Associação do tipo de interface Para as regras de conexão, você pode especificar os seguintes tipos de parâmetros: • Associação de domínio de DNS • Associação de endereço do servidor de DNS • Associação de SSID • Investigação da sequência da URL • Associação do tipo de interface • Domínios • Servidor de DNS

	• Investigação da URL
Aplicativo associado sob demanda ativado	Selecione para habilitar VPN por aplicativo sob demanda.
Domínios	
Safari Domínios (iOS)	Uma matriz cujas entradas devem especificar cada domínio que dispare a conexão de VPN no Safari. Cada entrada está no formato www.apple.com.
iOS 14.0 ou posterior e macOS 11.0 ou posterior	
Domínios associados	Especifique um ou mais domínios associados. As conexões com servidores dentro de um desses domínios são associadas à VPN por aplicativo.
Domínios excluídos	Especifique um ou mais domínios excluídos. As conexões com servidores dentro de um desses domínios são excluídas da VPN por aplicativo.
iOS 13 ou posterior e macOS 10.15 ou posterior	
Domínios de e-mail	Clique em **+Adicionar** para inserir um ou mais domínios que acionarão essa conexão VPN em E-mail. Cada entrada está no formato www.apple.com.
Domínios de contatos	Clique em **+Adicionar** para inserir um ou mais domínios que acionarão essa conexão VPN em Contatos. Cada entrada está no formato www.apple.com.

Domínios de calendário	Clique em **+Adicionar** para inserir um ou mais domínios que acionarão essa conexão VPN em Calendário. Cada entrada está no formato www.apple.com.
iOS 9 ou mais recente	
Tipo do fornecedor (iOS 9+)	Selecione um dos seguintes fornecedores de túnel: • proxy do aplicativo - tráfego de túneis na camada do aplicativo. Consulte Documentação da Apple para obter uma visão geral do fornecedor de proxy do aplicativo. • túnel do pacote - tráfego de túneis na camada do IP. Consulte Documentação da Apple para obter uma visão geral do fornecedor de túnel do pacote.

IPsec (Cisco)

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação da máquina	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Incluir PIN do usuário	Selecione para solicitar um PIN ao usuário.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Cisco AnyConnect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Agrupar	Insira o grupo que será utilizado para autenticar a conexão.
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SSL Juniper

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Realm	Insira o realm de autenticação que será utilizado para autenticar a conexão.
Função	Insira a função de autenticação que será utilizada para autenticar a conexão.
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	**Certificado** é o método de autenticação de usuário a ser usado. O campo a seguir está disponível: **Credencial**: Selecione o certificado de identidade que será utilizado. Os certificados fornecidos pelo usuário têm suporte apenas em dispositivos iOS.

Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy. Selecione as seguintes opções: • Ativar VPN sob demanda – Adicione nomes de host ou domínios que estabelecem uma VPN sob demanda. • Ativar regras do iOS. • Aplicativo associado sob demanda ativado.
Domínios do Safari	Clique **+Adicionar** para adicionar domínios do Safari.
Tipo do fornecedor (iOS 9.0+)	**túnel do pacote** é selecionado como o tipo de provedor de túnel padrão. Consulte Documentação da Apple para obter uma visão geral do fornecedor de túnel do pacote.

F5 SSL

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SonicWALL Mobile Connect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Domínio ou grupo de login	Insira o grupo de login ou domínio que será utilizado para autenticar a conexão.
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Aruba VIA

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SSL personalizado

Configuração	O que fazer
Identificador	Insira o identificador para esse SSL VPN personalizado no formato DNS reverso (como, com.minhaempresa.meuservidor).
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Dados personalizados	Insira os pares de valores principais que definem os dados personalizados para esse VPN.
Autenticação do usuário	É suportada somente a autenticação do certificado.

Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.
(iOS 9.0+) Incluir ProviderType no dicionário principal e no subdicionário de VPN	Opte por incluir o tipo de provedor durante a geração de um plist (arquivo de configuração predefinido).

GlobalProtect da Palo Alto Networks

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta do usuário que será utilizada para autenticar a conexão.
Dados personalizados	Insira os pares de valores principais que definem os dados personalizados para esse VPN.
Autenticação do usuário	O certificado é o método de autenticação do usuário. Selecione um certificado de identidade para usar no campo **Credencial**.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático**, estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Distribuir configuração

A partir da versão 91 do Ivanti Neurons for MDM, os administradores globais poderão autorizar os administradores de espaço a editar a Configuração VPN por Aplicativo nas seções Todos os Aplicativos e na opção de distribuição personalizada. Na configuração de VPN por aplicativo, você pode, opcionalmente, selecionar a opção "Permitir que esta configuração esteja disponível em todos os espaços".

As alterações de distribuição são aplicáveis somente ao espaço específico. Todos os outros espaços continuam herdando as configurações de distribuição de espaço padrão.

Procedimento

1. Especifique as definições de configuração nos campos usando as informações da tabela anterior.
2. Clique em **Avançar**.
3. Selecione a opção **Habilitar essa configuração**.
4. Selecione uma das opções de distribuição a seguir:
    - **Todos os dispositivos**. Selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.
    - **Nenhum dispositivo** (padrão)
    - **Personalizado** Selecione uma das opções a seguir:
        - **Não se aplica a outros espaços**.
        - **Aplicável a dispositivos em outros espaços**.
            - Marque a caixa de seleção **Permitir que o administrador de espaço edite a distribuição** para permitir que os administradores de espaço delegados editem a distribuição do espaço específico.

Para obter mais informações, consulte Como criar uma configuração

Configuração do logon único

O Ivanti Neurons for MDM permite Logon único (SSO) extensível com as configurações SSO extensível e SSO extensível Kerberos. A implementação requer uma extensão de aplicativo (como Microsoft Authenticator) do provedor de identidade. Com uma implementação SSO extensível, os usuários precisam se autenticar apenas uma vez ao acessar os recursos corporativos. Os usuários não precisam de autenticação nos logins subsequentes. Para obter informações de configuração relativas ao provedor de identidade pretendido, consulte "Configuração de provedor de identidade" na página 1244.

Esta seção contém os seguintes tópicos:

- Configurações da conta de logon único
- Configurações da conta de logon único extensível
- Configurações da conta Kerberos de logon único extensível

Configurações da conta de logon único

Aplicável a: iOS 7.0 até a versão mais recente compatível com o Ivanti Neurons for MDM.

Use as opções a seguir para configurar o SSO corporativo baseado em Kerberos para qualquer aplicativo gerenciado e para o navegador Apple Safari em dispositivos iOS.

Esta configuração requer Tunnel e Sentry. Para obter mais informações, consulte a seção "Configuração de logon único com Kerberos" no *Guia do Tunnel para iOS*.

Configuração	Descrição
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome de usuário	Insira o nome da entidade de segurança Kerberos.
Nome do realm do Kerberos	Insira no nome do realm Kerberos.
Certificado	**Para iOS 8 com licença Gold:** selecione o certificado a ser usado para renovar a credencial Kerberos.
Associações dos prefixos da URL	Lista de prefixos de URLs que devem corresponder para usar essa conta para autenticação Kerberos com HTTP.
Apps permitidos para SSO	Adicione apps do App Catalog para permiti-los para SSO. Por exemplo, digite "Safari" para adicionar o Apple Safari. Se nenhum aplicativo for permitido para SSO usando uma configuração desse tipo, todos os apps compatíveis com o SSO do iOS poderão usar o SSO, incluindo os apps iOS integrados.

Configurações da conta de logon único extensível

Aplicável a:

- iOS 13.0 até a versão mais recente com suporte do Ivanti Neurons for MDM.
- macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Use as opções a seguir para configurar o perfil de SSO extensível com o tipo de extensão genérica e habilitar o SSO para sites e aplicativos nativos com vários métodos de autenticação.

O SSO extensível não funciona quando a configuração é transferida no canal do usuário para dispositivos macOS 10.15.x.

Configuração	Descrição
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Escolher o tipo de SSO	Selecione um dos seguintes tipos de SSO: • **Credenciais** ◦ Insira um ou mais nomes de **Host** e nomes de domínio que possam ser autenticados pela extensão de aplicativo. A correspondência de nomes de host ou de domínio não diferencia letras maiúsculas de minúsculas, e todos os nomes de host/domínio de todos os conteúdos de SSO extensível instalados devem ser exclusivos. Hosts que começam com "." são sufixos curinga e corresponderão a todos os subdomínios, caso contrário, o host deve ser uma correspondência exata. ◦ Insira o nome do **Realm**. Esse valor deve ter a capitalização correta. • **Redirecionar** ◦ Informe um ou mais prefixos de **URL** de provedores de identidade em que a extensão de aplicativo executa SSO. Os URLs devem começar com http:// ou https://, a correspondência de esquema e nome do host não diferencia letras maiúsculas de minúsculas, não são permitidos parâmetros de consulta e fragmentos de URL, e os URLs de todos os conteúdos de SSO extensível instalados devem ser exclusivos.
Identificador de extensão	Insira o identificador do pacote da extensão de aplicativo que executa SSO para os URLs especificados.
Identificador de equipe	O identificador de equipe da extensão de aplicativo. Essa chave é obrigatória no macOS e ignorada em outros locais.

Configuração	Descrição
Dados personalizados	Insira um ou mais dados personalizados como pares de chave-valor.
Método de autenticação (Aplicável apenas a macOS 13+)	• Senha • Chave de enclave segura do usuário
Token de registro	Insira o token. Este campo é habilitado quando você seleciona um dos Métodos de Autenticação.

Configurações da conta Kerberos de logon único extensível

Aplicável a:

- iOS 13.0 até a versão mais recente com suporte do Ivanti Neurons for MDM.
- macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Use as opções a seguir para configurar uma extensão de aplicativo que executa SSO com extensão Kerberos.

O SSO extensível Kerberos não funciona quando a configuração é transferida no canal do usuário para dispositivos macOS 10.15.x.

Configuração	Descrição
Configurações básicas	
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome de usuário	Insira o nome da entidade de segurança Kerberos.
Realm	Insira no nome do realm Kerberos.
Certificado	Selecione o certificado a ser usado para renovar a credencial Kerberos.
Prefixos da URL	Lista de prefixos de URLs que devem corresponder para usar essa conta para autenticação Kerberos com HTTP.
Configurações avançadas	
Permitir login automático	Se for falso, as senhas não podem ser salvas no chaveiro. Por padrão, essa opção está habilitada.
Atrasar configuração do usuário	Se for verdadeiro, não solicita que o usuário configure a extensão do Kerberos até que o administrador a habilite com a ferramenta app-sso ou quando for recebido um desafio do Kerberos. Esta opção é aplicável ao macOS 11 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Exigir presença do usuário	Se for verdadeiro, exige que o usuário entre com o Touch ID, Face ID ou a senha para acessar a entrada do chaveiro.
Monitorar cache de credenciais	Se for falso, a credencial é solicitada no próximo desafio do Kerberos correspondente ou na alteração de estado da rede. Se a credencial estiver vencida ou ausente, será criada uma nova. Esta opção é aplicável ao macOS 11 até a versão mais recente com suporte do Ivanti Neurons for MDM. Por padrão, essa opção está habilitada.
Nome do cache	Insira o nome do Serviço genérico de segurança (GSS) do cache Kerberos a ser usado. Esta opção foi preterida.

Configuração	Descrição
Mapeamento do Realm de domínio	Insira o nome do realm como chave. O valor é uma matriz de sufixos DNS que mapeiam para o realm. Clique em **+ Adicionar** para adicionar um ou mais pares de chave-valor.
Realm padrão	Esta propriedade especifica o realm padrão se houver mais de uma configuração de extensão do Kerberos.
Usar a descoberta automática de sites	Se for falso, a extensão do Kerberos não usa o LDAP e o DNS automaticamente para determinar o nome de site do AD. Por padrão, essa opção está habilitada.
Código de local	Insira o nome do site do Active Directory que deve ser usado pela extensão do Kerberos.
Tempo de replicação	Insira o tempo, em segundos, necessário para replicar as alterações no domínio do Active Directory. A extensão do Kerberos usará isso ao verificar a idade da senha após uma alteração. Esta opção é aplicável ao macOS 11 até a versão mais recente com suporte do Ivanti Neurons for MDM. Esta opção foi preterida.
ACL de ID de pacote de credenciais	Clique em **+ Adicionar** para adicionar uma lista de IDs de pacote autorizados a acessar o sistema Ticket Granting Ticket (TGT) para fins de autenticação.
Inclui aplicativos gerenciados na ACL de ID do pacote	Se for verdadeiro, a extensão do Kerberos permitirá que apenas aplicativos gerenciados acessem e usem a credencial. É um acréscimo à ACL de ID do pacote de credenciais, se especificada. Esta opção é aplicável ao iOS 14 ou a versões mais recentes com suporte do Ivanti Neurons for MDM.
Inclui apps Kerberos na ACL de ID em pacote	Se for verdadeiro, a extensão do Kerberos permitirá que os utilitários Kerberos padrão, incluindo Visualizador de tíquete e klist, acessem e usem a credencial. Disponível no macOS 12 e posterior.
Rótulo de nome de usuário personalizado	Digite o rótulo de nome de usuário personalizado usado na extensão Kerberos em vez de "Nome de usuário". Por exemplo, "ID da empresa". Essa opção é aplicável ao macOS 11 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Configuração	Descrição
Texto de ajuda	Insira o texto a ser exibido para o usuário na parte inferior da janela de login do Kerberos. Pode ser usado para exibir informações de ajuda ou texto de isenção de responsabilidade. Esta opção é aplicável ao iOS 14 e macOS 11 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Modo de uso de credencial	Essa configuração afeta a forma como a credencial da extensão do Kerberos é usada por outros processos. Selecione uma das opções a seguir: • Sempre (padrão) – a credencial da extensão sempre será usada se o nome principal do serviço (SPN) corresponder à matriz de Hosts de extensão do Kerberos. A credencial não será usada se o aplicativo chamador não estiver em credentialBundleIDACL. • Quando não especificada – A credencial só será usada se não houver outra credencial especificada pelo chamador, e se o SPN corresponder à matriz de Hosts de extensão do Kerberos. A credencial não será usada se o aplicativo chamador não estiver em credentialBundleIDACL. • Padrão Kerberos – São seguidos os processos padrão do Kerberos para a seleção de credenciais, que geralmente utilizam a credencial padrão do Kerberos. Isso equivale a desativar esse recurso. (Opcional) Selecione **Exigir TLS para LDAP**.
Centros de distribuição de chaves preferenciais	Adicionar Centros de distribuição de chaves preferenciais. Clique em **+Adicionar** para adicionar um KDC preferencial.
	Permitir fallback de autenticação SSO da plataforma - se Verdadeiro, e se Usar TGT SSO da Plataforma for verdadeiro, permite que o usuário faça login manualmente. Disponível em macOS 13 e posteriores
	Executar apenas Kerberos - se verdadeiro, a extensão Kerberos trata apenas de solicitações Kerberos. Disponível em macOS 13 e posteriores.
	Usar TGT SSO da plataforma - se verdadeiro, esta configuração usa um TGT de SSO da plataforma em vez de solicitar um novo. Disponível em macOS 13 e posteriores.
Configurações da senha	

Configuração	Descrição
Permitir alteração de senha	Se for falso, desativa as alterações de senha. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM. Por padrão, essa opção está habilitada.
URL de alteração de senha	Insira a URL a ser aberto no navegador da Web padrão do usuário quando o usuário iniciar uma alteração de senha. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Permitir complexidade de senha	Se verdadeiro, as senhas devem atender à definição de "complexa" do Active Directory. Essa opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Comprimento mínimo da senha	Informe a quantidade mínima de caracteres exigida para as senhas no domínio. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Notificação de expiração de senha	Insira o número de dias antes da expiração da senha em que uma notificação de expiração da senha será enviada ao usuário. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM. O tempo padrão é 15 dias.
Anular expiração de senha	Informe o número de dias que as senhas podem ser usadas neste domínio. Para a maioria dos domínios, pode ser calculado automaticamente. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM. (Esta opção agora está obsoleta)
Texto de senha obrigatória	Insira a versão em texto dos requisitos de senha do domínio. Para uso somente se pwReqComplexity ou pwReqLength não forem especificados. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Configuração	Descrição
Contagem do histórico de senha	Informe o número de senhas anteriores que não podem ser reutilizadas neste domínio. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Idade mínima da senha	Informe a idade mínima (em dias) que as senhas devem ter para que possam ser alteradas neste domínio. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.
Permitir sincronização de senha local	Se for falso, desativa a sincronização da senha. Esta ação não funcionará se o usuário estiver conectado com uma conta móvel. Esta opção é aplicável ao macOS 10.15 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Para obter mais informações, consulte Como criar uma configuração

Entrada segura multiusuário para iOS

O clipe da web multiusuário permite que os usuários efetuem login e logout em dispositivos iOS registrados no Ivanti Neurons for MDM. Quando um usuário faz login pela primeira vez, os perfis, os aplicativos e as configurações associados a esse usuário são transmitidos para o dispositivo. Ao terminar seu trabalho, o usuário pode abrir o clipe da Web e selecionar a função "logout", que atribui o dispositivo ao Usuário ninguém e remove os perfis, aplicativos e configurações associados ao usuário que fez login originalmente, desde que os aplicativos e as configurações não estejam sendo distribuídos ao Usuário ninguém. Depois do logout, o clipe da Web é redefinido para que o próximo usuário possa fazer login e receber configurações, políticas e aplicativos personalizados. Não é necessário que a supervisão do dispositivo use o recurso de login seguro multiusuário. Na base de conhecimento do Suporte, consulte o artigo Ivanti Neurons for MDM: login seguro multiusuário para iOS, para obter uma descrição mais detalhada desse recurso.

Aplicável a: dispositivos iOS (não aplicável a dispositivos registrados pelo usuário)

Esta seção contém os seguintes tópicos:

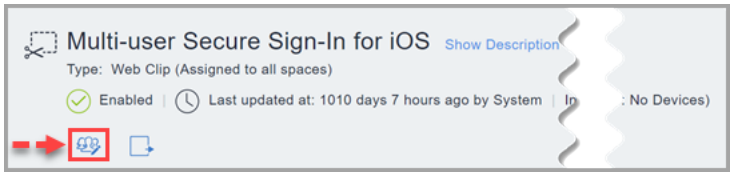
Credenciais compatíveis

O nome de usuário e a senha devem ser usados para o login no clipe da Web seguro multiusuários. Registro baseado em PIN e registros baseados em IdP SAML 2.0 não são compatíveis com o clipe da Web seguro multiusuários.

Procedimento

1. Vá até **Configurações**.
2. Clique em **Entrada segura multiusuário para iOS**. Se houver múltiplas páginas de configurações, pode ser necessário usar a funcionalidade de busca para encontrar a configuração específica. Essa configuração não é acessada pelo botão **+Adicionar**.

3. Clique em **Editar distribuição**ou no ícone associado para distribuir o clipe da web ao grupo de dispositivos apropriado.



   Se você desejar distribuir o clipe da Web para um Grupo de usuários, pode criar um Grupo de dispositivos dinâmico vinculado a um Grupo de usuários.

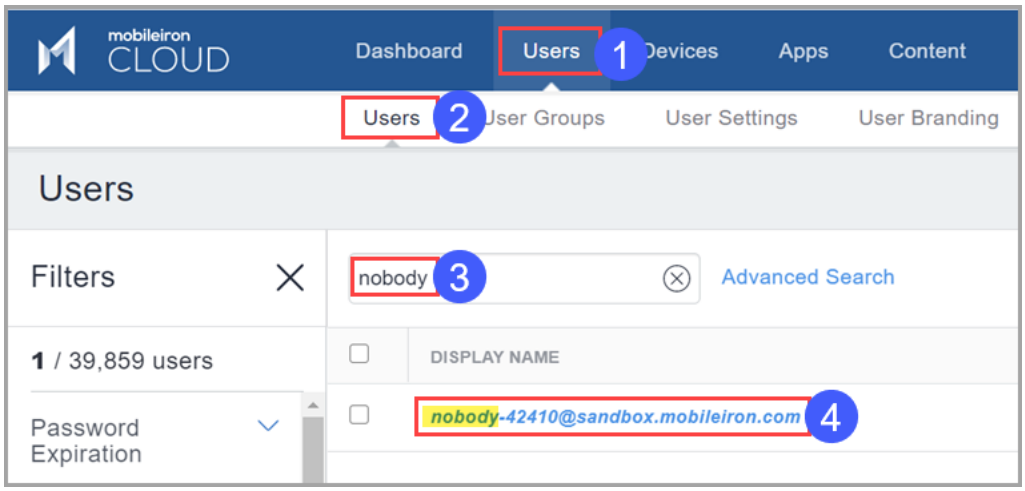
4. Selecione uma das opções de distribuição a seguir, lembrando que você sempre deve distribuir o clipe da Web para o Usuário ninguém ou para o Grupo de dispositivos ao qual o Usuário ninguém está associado. Isso não acontece por padrão, por isso certifique-se de fazer a distribuição para o Usuário ninguém.

   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizada

5. Clique em **Salvar**.

Explicação sobre o Usuário *ninguém*

Quando ocorre o logout de um dispositivo por meio do clipe da web, o dispositivo permanece registrado no Ivanti Neurons for MDM para um usuário especial chamado Usuário Ninguém. Se você desejar remover aplicativos e configurações do dispositivo quando um usuário fizer logout, certifique-se de que tais aplicativos e configurações não estejam distribuídos para o Usuário ninguém. Se você desejar que determinadas configurações, como Wi-Fi, permaneçam no dispositivo quando o usuário fizer logout do clipe da Web de login seguro, também é necessário distribuir essas configurações para o Usuário ninguém.



Isso significa que você deve prestar atenção aos Grupos de usuários e Grupos de dispositivos para os quais distribui aplicativos e configurações. Se você estiver distribuindo um aplicativo para Todos e desejar que ele seja removido quando o usuário fizer logout do dispositivo, é recomendável criar um Grupo de usuários que não inclua o Usuário ninguém. Os atributos personalizados facilitam muito a criação de um grupo de usuários que sejam "multiusuários" e de outro Grupo de usuários formado apenas pelo Usuário ninguém. Você pode criar um Atributo de usuário em Administrador > Sistema > Atributos com o nome "Proprietário multiusuário" e depois atribuir o valor "Sim" ou "Verdadeiro" ao Usuário "ninguém". Em seguida, você pode criar Grupos de usuários e Grupos de dispositivos com base no valor do atributo.

Iniciar sessão para um dispositivo

Um usuário pode iniciar a sessão para um dispositivo iOS e atribuir esse dispositivo a ele mesmo. Após fazer o login, todos os aplicativos, políticas, configurações e certificados relevantes serão enviados ao dispositivo.

Cancelar sessão de um dispositivo

Um usuário pode cancelar sua sessão do dispositivo iOS após o uso. Após cancelar a sessão, os aplicativos, políticas, configurações e certificados relevantes serão removidos do dispositivo, deixando-o no estado em que estava antes do início da sessão do usuário. Então, o dispositivo será disponibilizado para o início de sessão de outro usuário.

Para obter mais informações, consulte Atribuição de marca ao registro de vários usuários

Configurações de APN de Android

As Configurações de APN do Android permitem definir as configurações do nome do ponto de acesso (APN) necessárias em dispositivos em uma rede pública. Esta configuração é aplicável apenas aos Dispositivos gerenciados de trabalho do Android Enterprise e Dispositivos gerenciado com o Work Profile em dispositivo de propriedade da empresa (no Android 9.0 ou em versões mais recentes com suporte).

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione **Configurações de APN de Android**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Definição da configuração, configure as seguintes opções:

Configuração	Descrição
Nome de entrada	Insira o nome das configurações do ponto de acesso.
Nome do ponto de acesso	Digite o nome do ponto de acesso.
Tipo do ponto de acesso	Selecione o tipo de ponto de acesso entre as opções a seguir: • **Padrão** • **DUN** • **IMS** • **Emergência** • **MMS** • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
Tipo de MVNO	Selecione o tipo de operado de rede virtual móvel entre as seguintes opções: • **Nenhum** • **SPN** • **IMSI** • **GID** • **ICCID**

Configuração	Descrição
Bearer	Selecione o tipo de serviço de portador usado para transmissão de dados entre as seguintes opções: • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA** • **IDEN** • **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**

Configuração	Descrição
Protocolo APN	Selecione o protocolo APN necessário para o APN. As opções disponíveis são as seguintes: • **Nenhum** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Protocolo Ponto a Ponto) • **NÃO ESTRUTURADO**
Protocolo de roaming de APN	Selecione o protocolo de roaming APN necessário para o APN. As opções disponíveis são as seguintes: • **Nenhum** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Point-to-Point Protocol, protocolo ponto a ponto) • **NÃO ESTRUTURADO**
Ativar/desativar APN	Ative a configuração do APN.
ID da operadora	Insira o valor numérico do ID da operadora.

Configuração	Descrição
Tipo de autenticação	Selecione o tipo de protocolo de autenticação entre as seguintes opções: • **Nenhum** • **PAP** (Password Authentication Protocol, protocolo de autenticação de senha) • **CHAP** (Challenge Handshake Authentication Protocol, protocolo de autenticação de handshake de desafio) • **PAP ou CHAP**
Nome de usuário	Insira o nome de usuário de login.
Senha	Insira a senha de login.
Confirmar senha	Insira novamente a senha para confirmação.
Número da porta	Insira o número da porta (valor numérico entre 1 e 65.535).
Endereço proxy	Insira o endereço proxy.
Código do país para dispositivos móveis	Insira o código do país para dispositivos móveis.
Código de rede móvel	Insira o código de rede móvel.

Configuração	Descrição
Endereço proxy MMS	Insira o endereço proxy MMS.
Número da porta MMS	Insira o número da porta MMS (valor numérico entre 1 e 65.535).
Endereço do Servidor MMS (mmsc)	Insira o endereço do servidor MMS.

6. Clique em **Avançar**.
7. Selecione uma das opções de distribuição a seguir:
   - **Todos os dispositivos**
   - **Nenhum dispositivo** (padrão)
   - **Personalizada**
8. Clique em **Concluído**.

Se houver uma configuração de APN existente com determinados valores para o dispositivo, não será possível adicionar outra configuração de APN com os mesmos valores nos seguintes campos:

- Código do país para dispositivos móveis
- Código de rede móvel
- Nome do Ponto de Acesso
- Endereço proxy
- Número da porta
- Endereço proxy MMS
- Número da porta MMS
- Endereço do servidor MMS
- Ativar/desativar APN

- Tipo de MVNO
- Protocolo de APN
- Protocolo de roaming de APN

A configuração de APN de Android tem precedência sobre as configurações de APN, se já estiverem configuradas no dispositivo manualmente ou pela operadora de rede.

Configuração VPN

Aplicável a:

- Android
- Windows
- iOS
- macOS

Uma configuração VPN define as configurações para o acesso à rede privada virtual.

Procedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Selecione a configuração **VPN**.
3. Insira um **Nome** para a configuração.
4. Insira uma descrição.
5. Defina as configurações de VPN segundo as descrições a seguir.
6. (Somente iOS 9.0+) Na seção Domínios de correspondência, clique em **+Adicionar** para inserir um ou mais domínios de correspondência (exemplo: company.com). A conexão de proxy é usada quando o domínio é um dos domínios especificados.
7. Clique em **Avançar**.
8. (Apenas macOS) Na página Distribuir, selecione uma das seguintes opções de distribuição:
    - Canal do dispositivo – A configuração vale para todos os usuários em um dispositivo, que é a opção comum.
    - Canal do usuário – A configuração vale apenas para o usuário registrado atualmente em um dispositivo.
9. Selecione as demais opções de distribuição desta configuração.
10. Clique em **Concluído**.

Configurações VPN

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração. Dispositivos com Windows Phone 8.1 não oferecem suporte para a alteração do nome. Exclua a configuração e crie uma nova configuração se precisar alterar o nome de um perfil de VPN em dispositivos com Windows Phone 8.1.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Tipo de conexão	Selecione o tipo de VPN para configurar. As configurações restantes dependem dessa seleção.

Os protocolos e suas configurações são listados da seguinte forma:

- L2TP (não compatível com Ivanti Go)
- PPTP (não compatível com Ivanti Go)
- IPsec (Cisco) (não compatível com Ivanti Go)
- Cisco AnyConnect (não compatível com Ivanti Go)
- Juniper SSL (não compatível com Ivanti Go)
- NetMotion VPN (não compatível com Ivanti Go)
- Pulse Secure (compatível com Ivanti Go)

- F5 SSL (não compatível com Ivanti Go)
- SonicWALL Mobile Connect (não compatível com Ivanti Go)
- Aruba VIA (não compatível com Ivanti Go)
- SSL personalizado (não compatível com Ivanti Go)
- Palo Alto Networks GlobalProtect (compatível com Ivanti Go)
- KEv2 (somente Windows) (não compatível com Ivanti Go)
- IKEv2 (não compatível com Ivanti Go)

L2TP

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	Selecione o método de autenticação que será utilizado: **Senha** ou **RSA SecurID**.
Segredo compartilhado	Insira a senha secreta compartilhada, caso ela seja necessária para iniciar a conexão.
Enviar todo o tráfego	Selecione essa opção para usar essa conexão para todo o tráfego de rede. Essa opção ajuda a proteger os dados de serem comprometidos, principalmente em redes públicas.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

PPTP

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	Selecione o método de autenticação que será utilizado: **Senha** ou **RSA SecurID**.
Nível de criptografia	Selecione um nível de criptografia de dados para a conexão: **Nenhum, Automático** ou **Máximo (128 bits)**.
Enviar todo o tráfego	Selecione essa opção para usar essa conexão para todo o tráfego de rede. Essa opção ajuda a proteger os dados de serem comprometidos, principalmente em redes públicas.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

IPsec (Cisco)

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação da máquina	Selecione o método de autenticação que será utilizado: **Nome do grupo/secreto compartilhado** ou **Certificado**.
Nome do grupo	Autenticação do Nome do grupo/secreto compartilhado. Especifique o nome do grupo para ser utilizado. Se for utilizada uma autenticação híbrida, a sequência deverá terminar com â€œ[hybrid]â€ .
Segredo compartilhado	Autenticação do Nome do grupo/secreto compartilhado. Insira a senha secreta compartilhada.
Usar autenticação híbrida	Autenticação do Nome do grupo/secreto compartilhado. Selecione para especificar uma autenticação híbrida, por exemplo, o servidor fornece um certificado e o cliente fornece uma chave pré-compartilhada.
Solicitar senha	Autenticação do Nome do grupo/secreto compartilhado. Especifique se o usuário deve fornecer uma senha ao conectar.

Credencial	*Autenticação do certificado* Selecione o certificado de identidade que será utilizado.
Incluir PIN do usuário	*Autenticação do certificado* Selecione para solicitar um PIN ao usuário.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Cisco AnyConnect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Agrupar	Insira o grupo que será utilizado para autenticar a conexão.
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar **Certificado**, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SSL Juniper

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Realm	Insira o realm de autenticação que será utilizado para autenticar a conexão.

Função	Insira a função de autenticação que será utilizada para autenticar a conexão.
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar **Certificado**, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

VPN NetMotion

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar **Certificado**, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

F5 SSL

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta do usuário que será utilizada para autenticar a conexão.
Autenticação do usuário	Insira o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar **Certificado**, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione Manual ou Automático para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SonicWALL Mobile Connect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Domínio ou grupo de login	Insira o grupo de login ou domínio que será utilizado para autenticar a conexão.
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar Certificado, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Aruba VIA

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar **Certificado**, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione Manual ou Automático para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SSL personalizado

Configuração	O que fazer
Identificador	Insira o identificador para esse SSL VPN personalizado no formato DNS reverso (como, com.minhaempresa.meuservidor).
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*

Dados personalizados	Insira os pares de valores principais que definem os dados personalizados para esse VPN.
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar Certificado, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Palo Alto Networks GlobalProtect

Não aplicável para os dispositivos Windows Phone e Android.

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta do usuário que será utilizada para autenticar a conexão.

Dados personalizados	Insira os pares de valores principais que definem os dados personalizados para esse VPN.
Autenticação do usuário	Selecione o método de autenticação do usuário que será utilizado: **Senha** ou **Certificado**. Se você selecionar Certificado, o seguinte campo estará disponível: **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

IKEv2 (somente para Windows)

Configuração	O que fazer
Servidor	Insira o nome do host ou endereço IP do servidor VPN.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

IKEv2

Configuração	O que fazer
Servidor	Insira o nome do host ou endereço IP do servidor VPN.
Identificador local	Identificador do cliente IKEv2 em um dos formatos a seguir: • **FQDN** • **UserFQDN** • **Endereço** • **ASN1DN**
Identificador remoto	Identificador remoto em um dos formatos a seguir: • **FQDN** • **UserFQDN** • **Endereço** • **ASN1DN**
Autenticação da máquina	Disponível apenas se a opção **Ativar EAP** não estiver selecionada. Selecione uma das opções a seguir: • Certificado • Segredo compartilhado
Autenticação EAP	Disponível apenas se a opção **Ativar EAP** estiver selecionada. Selecione uma das opções a seguir: • Certificado • Nome de usuário/senha

Segredo compartilhado	Disponível apenas se Segredo Compartilhado estiver selecionado para Autenticação da Máquina. Insira o segredo compartilhado da conexão.
Credencial	Disponível apenas se Certificado foi selecionado para a Autenticação da Máquina. Selecione o certificado a ser utilizado. Esse certificado será enviado para autenticação do cliente IKE. Se a autenticação estendida for utilizada, esse certificado pode ser utilizado para EAP-TLS.
Ativar EAP	Selecione para ativar a autenticação estendida.
Conta	Disponível apenas se Nome de Usuário/Senha estiver selecionado para Autenticação EAP. Insira o ID da conta para o servidor VPN.
Senha	Disponível apenas se Nome de Usuário/Senha estiver selecionado para Autenticação EAP. Insira a senha para o servidor VPN.
Intervalo de detecção de par morto	Selecione uma das opções a seguir: • **Nenhum (Desativar)** • **Baixo (keepalive enviado a cada hora)** • **Médio (keepalive enviado a cada 30 minutos)** • **Alto (keepalive enviado a cada 10 minutos)**

Nome comum do emissor de certificado do servidor	(Opcional) - Nome comum de um emissor de certificado do servidor, faz com que o servidor IKE envie uma solicitação de certificado com base no emissor do certificado para o servidor.
Nome comum do certificado do servidor	(Opcional) - Nome comum de um certificado de servidor usado para validar o certificado enviado pelo servidor IKEv2.
Usar atributos de sub-redes IP4 e IP6	(Opcional) Selecione para usar atributos de sub-rede IP4 e IP6.
Habilitar protocolo multihoming e mobilidade IKEv2 (MOBIKE)	(Opcional) A configuração padrão é 0. O MOBIKE (A capacidade de suportar dispositivos móveis com hospedagem múltipla quando conectados tanto ao Wi-Fi quanto a links de celular com vários endereços IP) está ativado. Ele é ativado por padrão. Definir para 1 para desativar o MOBIKE.
Habilitar Sigilo avançado perfeito (PFS)	(Opcional) Quando definido para 1, ativa o PFS para conexões IKEv2. A configuração padrão é 0.
Habilitar redirecionamento IKEv2	(Opcional) A configuração padrão é 0. A conexão IKEv2 é redirecionada se uma solicitação de redirecionamento for recebida do servidor. Ele é ativado por padrão. Definir para 1 para desabilitar o redirecionamento IKEv2.
Habilitar manutenção de atividade de NAT	Ativa a manutenção de atividade da conversão de endereços de rede que impede a exclusão das entradas do NAT na ausência de qualquer tráfego quando há NAT entre pares IKE.

Intervalo de manutenção de atividade do NAT	Se a manutenção de atividade do NAT estiver ativada, ela representará o tempo em segundos que os pacotes de manutenção de atividade serão enviados para o dispositivo.
Algoritmo de criptografia	Selecione uma das opções a seguir: • **DES** • **3DES** • **AES-128** • **AES-256** (padrão) • **AES-128 GCM** • **AES-256 GCM**
Algoritmo de integridade	Selecione uma das opções a seguir: • **SHA2-256** (padrão) • **SHA2-384** • **SHA2-512**

Grupo Diffie-Hellman	Selecione uma das opções a seguir: • **1** • **2** (padrão) • **5** • **14** • **15** • **16** • **17** • **18**
Vida útil em minutos	Insira a vida útil do SA (intervalo de rechaveamento) em minutos. Valores válidos são 10 a 1440.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

*Digite $ para ver uma lista de variáveis suportadas, se disponível, para esse campo.

Para obter mais informações, consulte Como criar uma configuração

VPN sob demanda

Aplicável para: dispositivos iOS

Uma configuração VPN sob demanda configura o acesso para um servidor VPN com base em domínios, nomes do host etc.

Configurações de VPN sob demanda

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Tipo de conexão	Selecione o tipo de VPN para configurar. As configurações restantes dependem dessa seleção.

Habilitar VPN sob demanda	Selecione para usar essa configuração para domínios e nomes do host que estabelecem uma VPN sob demanda.

Ativar regras do iOS (Aplicável se a opção Habilitar VPN sob demanda estiver selecionada)	Para iOS e macOS, você pode configurar: • Regras da rede que permitem ou impedem conexões e permitem ou ignoram, as redes que são avaliadas como verdadeiras. • As regras de conexão permitem quando necessário, ou nunca permitem, conexões com as redes que são avaliadas como verdadeiras. Para as regras da rede, você pode especificar os seguintes tipos de parâmetros: • Associação de domínio de DNS • Associação de endereço do servidor de DNS • Associação de SSID • Investigação da sequência da URL • Associação do tipo de interface Para as regras de conexão, você pode especificar os seguintes tipos de parâmetros: • Associação de domínio de DNS • Associação de endereço do servidor de DNS • Associação de SSID • Investigação da sequência da URL • Associação do tipo de interface • Nome do domínio • Servidor de DNS

	• Investigação da URL
Tipo do fornecedor (iOS 9+)	Selecione um dos seguintes fornecedores de túnel: • proxy do aplicativo - tráfego de túneis na camada do aplicativo. Consulte Documentação da Apple para obter uma visão geral do fornecedor de proxy do aplicativo. • túnel do pacote - tráfego de túneis na camada do IP. Consulte Documentação da Apple para obter uma visão geral do fornecedor de túnel do pacote.

Os protocolos e suas configurações são listados da seguinte forma:

- IPsec (Cisco)
- Cisco AnyConnect
- SSL Juniper
- VPN NetMotion
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- SSL personalizado
- Palo Alto Networks GlobalProtect

IPsec (Cisco)

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação da máquina	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Incluir PIN do usuário	Selecione para solicitar um PIN ao usuário.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Cisco AnyConnect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Agrupar	Insira o grupo que será utilizado para autenticar a conexão.
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SSL Juniper

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Realm	Insira o realm de autenticação que será utilizado para autenticar a conexão.
Função	Insira a função de autenticação que será utilizada para autenticar a conexão.
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

VPN NetMotion

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	O certificado é o método de autenticação do usuário. **Credencial**: Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: **URL do servidor proxy**: Insira a URL qualificada para o proxy.

F5 SSL

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SonicWALL Mobile Connect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Domínio ou grupo de login	Insira o grupo de login ou domínio que será utilizado para autenticar a conexão.
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Aruba VIA

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

SSL personalizado

Configuração	O que fazer
Identificador	Insira o identificador para esse SSL VPN personalizado no formato DNS reverso (como, com.minhaempresa.meuservidor).
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta de usuário que será utilizada para autenticar a conexão.*
Dados personalizados	Insira os pares de valores principais que definem os dados personalizados para esse VPN.

Autenticação do usuário	É suportada somente a autenticação do certificado.
Credencial	Selecione o certificado de identidade que será utilizado.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Palo Alto Networks GlobalProtect

Configuração	O que fazer
Servidor	Insira o endereço IP ou nome do host para o servidor VPN.
Conta	Insira a conta do usuário que será utilizada para autenticar a conexão.
Dados personalizados	Insira os pares de valores principais que definem os dados personalizados para esse VPN.
Autenticação do usuário	O certificado é o método de autenticação do usuário. Selecione um certificado de identidade para usar no campo **Credencial**.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Se você selecionar Manual,** estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. **Se você selecionar Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Para obter mais informações, consulte Como criar uma configuração

Configuração Wi-Fi

Aplicável a:

- Android
- Windows
- iOS
- macOS

Esta seção contém os seguintes tópicos:

Configurações Wi-Fi

Uma configuração Wi-Fi configura o acesso para uma rede sem fio.

Usuários podem modificar algumas configurações do Wi-Fi no dispositivo. No entanto, o servidor MDM pode ou não receber informações sobre as alterações, o que depende do SO do dispositivo. Então, as configurações não serão enviadas por push novamente de forma automática ao dispositivo para substituir a configuração no dispositivo com a configuração do servidor.

ProcedureProcedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Selecione a configuração **Wi-Fi**.
3. Insira um **Nome** para a configuração.
4. Insira uma descrição.
5. Defina as configurações de Wi-Fi segundo as descrições a seguir.

6. Clique em **Avançar**.
7. (Apenas macOS) Na página Distribuir, selecione uma das seguintes opções de distribuição:
    - Canal do dispositivo – A configuração vale para todos os usuários em um dispositivo, que é a opção comum.
    - Canal do usuário – A configuração vale apenas para o usuário registrado atualmente em um dispositivo.
8. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizado.
9. Clique em **Concluído**.

A tabela a seguir lista as Configurações Wi-Fi:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Identificador de Conjunto de Serviços (SSID)	Insira o nome da rede sem fio a qual essas configurações se aplicam. Esse campo faz distinção entre letras maiúsculas e minúsculas.
Associação automática	Selecione se os dispositivos devem se associar automaticamente à rede Wi-Fi correspondente. Se essa opção não estiver selecionada, os usuários do dispositivo devem tocar no nome da rede no dispositivo para associar à rede.
Rede oculta	Selecione essa opção se o acesso à rede não for transmitido.

Configuração	O que fazer
Desativar detecção da rede cativa (iOS 10+)	Os administradores podem ativar ou desativar o modo de desvio cativo de Wi-Fi. Quando a Apple detecta a presença de um portal cativo, ela abre uma tela de login para solicitar acesso. Você pode desativar a detecção de portais cativos, solicitando que o usuário abra manualmente um navegador, que aciona o login do portal de uma rede cativa. Esta nova configuração é útil quando um portal ISE cativo evita que a tela de login seja exibida em uma janela de pop-up, o que faz com que os usuários acreditem que seus dispositivos não conectados estão conectados à Internet.
Configuração do proxy	Selecione **Manual** ou **Automático** para configurar um proxy. **Para Windows Phone 8.1, Automático** não se aplica. Se você selecionar **Manual**, estarão disponíveis os seguintes campos adicionais: • **Servidor e porta**: Insira o endereço da rede e o número da porta para o servidor proxy*. • **Autenticação**: Insira um nome de usuário válido, se necessário para conectar ao proxy*. • **Senha**: Insira uma senha válida, se necessário para conectar ao proxy. Para remover o nome de host adicionado, clique no ícone de "menos". Se você selecionar **Automático,** estarão disponíveis os seguintes campos adicionais: • **URL do servidor proxy**: Insira a URL qualificada para o proxy.
Tipo de segurança	Selecione o método de segurança necessário para acessar a rede: • Qualquer (Pessoal) • Qualquer (Corporativo) • WEP

Configuração	O que fazer
	• WEP Corporativo • WPA • WPA corporativo • WPA2 • WPA2 corporativo • WPA3 • WPA3 Enterprise WPA3/WPA3 corporativo aplica-se a iOS 13+. O Windows é compatível com WPA, WPA corporativo, WPA2 e WPA2 corporativo.

Configurações WEP, WPA/WPA2/WPA3, Qualquer (Pessoal)

Configuração	O que fazer
Senha	(Opcional) Insira a senha para acessar essa rede. Caso contrário, o usuário do dispositivo deverá fornecer uma senha obrigatória para acessar a rede.

Configurações WEP Enterprise, WPA/WPA2/WPA3 Enterprise, Qualquer (Corporativo)

Configuração	O que fazer
Protocolos	
Tipos de EAP aceitos	Selecione os tipos de EAP que podem ser utilizados para acessar essa rede: • TLS • TTLS – no campo Identidade interna, selecione um dos protocolos de autenticação, como Padrão do SO, PAP, CHAP, MSCHAP, MSCHAPv2 e EAP. • PEAP • LEAP (sem suporte para dispositivos registrados com AMAPI) • EAP-SIM • EAP-AKA • EAP-FAST (sem suporte para dispositivos registrados com AMAPI) O Windows Phone não é compatível com vários tipos de EAP, como LEAP, EAP-SIM, EAP-AKA e EAP-FAST. No entanto, o AMAPI é compatível no momento apenas com o EAP único.

Configuração	O que fazer
EAP-FAST	Selecione a opção EAP-FAST que define os métodos de autenticação: • **Usar PAC:** selecione para usar uma configuração automática de proxy (PAC). • **Provisionar PAC:** selecione para permitir que um PAC seja provisionado. Caso contrário, somente um PAC já fornecido no dispositivo poderá ser utilizado. Essa opção estará disponível somente se você selecionou Usar PAC. • **Fornecer PAC anonimamente:** Selecione para permitir o fornecimento de um PAC sem autenticar o servidor. Essa opção estará disponível somente se você selecionou Fornecer PAC. **Para Windows Phone 8.1**, selecione somente um método de autenticação.
Autenticação	
Nome de Usuário	Especifique o nome de usuário necessário para o acesso à rede. Se você deixar esse campo em branco, o usuário do dispositivo deverá fornecer um.*
Usar senha por conexão	Selecione para solicitar uma senha para cada conexão ao usuário do dispositivo. Quando o dispositivo acessar novamente a mesma rede, o usuário deverá reautenticar para ingressar na rede. Esta opção não compatível com dispositivos registrados no AMAPI.
Senha	(Opcional) Insira a senha para acessar essa rede. Caso contrário, o usuário do dispositivo deverá fornecer uma senha obrigatória para acessar a rede.
Certificado de identidade	(Opcional) Selecione o certificado que será utilizado para a credencial de identidade. A configuração Certificado de identidade define cada certificado de identidade disponível.

Configuração	O que fazer
Certificado de autenticação (disponível apenas para dispositivos Windows)	Selecione um dos três repositórios de certificados a seguir para escolher um certificado e conectar-se a uma rede Wi-Fi: • Máquina ou usuário: se esta opção estiver selecionada e o usuário não estiver logado, o certificado de autenticação será colhido no repositório da máquina. Se o usuário estiver logado, o certificado específico será colhido no repositório do usuário. • Máquina: se esta opção for selecionada, o certificado de autenticação será colhido no repositório da máquina. • Usuário: se esta opção for selecionada, o certificado de autenticação será colhido no repositório do usuário. Por padrão, a opção Usuário fica selecionada.
Identidade externa	(Opcional) Para TLS, TTLS, PEAP e EAP-FAST, selecione para permitir que os usuários do dispositivo ocultem sua identidade. O nome real do usuário é exibido somente dentro do túnel criptografado. Essa opção pode aumentar a segurança, pois um invasor não conseguirá ver o nome do usuário autenticado de forma clara.
Domínio	Suportado quando o tipo EAP é TLS e TTLS.
Confiar	
Certificados confiáveis (sem suporte para dispositivos registrados com AMAPI)	Marque ou desmarque a opção **Certificado CA do agente**.
Nomes de certificados do servidor confiáveis	Clique em **+ Adicionar** para inserir os nomes de um ou mais certificados de servidor confiáveis. (Opcional) Selecione **Permitir exceções de confiança** para permitir que decisões de confiança sejam tomadas pelo usuário em uma janela de diálogo.

iOS e macOS

Configuração	O que fazer
Todas as versões	
Tipo de rede	Selecione se essa rede deve ser tratada como: • padrão • hotspot herdado • Passpoint
Fallback PAC do proxy permitido	(Opcional) Permite que o dispositivo conecte diretamente ao destino se o arquivo do PAC estiver inacessível.
Modos de instalação (opcional)	Uma matriz de strings que contém o tipo de modo de conexão a ser anexado. • Sistema: o Wi-Fi é conectado antes que o usuário faça login no dispositivo. • Janela de login: o Wi-Fi fica disponível depois que o usuário faz login no dispositivo. Atualmente, os modos de configuração funcionam apenas quando os modos Sistema e Janela de Login estão ativados.
Configurações de Passpoint	As configurações nesta seção aparecem se você selecionou a opção de Passpoint para o tipo de rede.
Nome do domínio	Insira o nome de domínio a ser usado para a negociação de Passpoint.
Conectar a redes de Passpoint de parceiro de roaming	(Opcional) Selecione para permitir conexões a provedores de serviço de roaming.
Identificadores da organização do consórcio de roaming	(Opcional) Insira os identificadores atribuídos pelo IEEE para as entidades suportadas por esse perfil Wi-Fi.

Configuração	O que fazer
Nomes do realm do identificador de acesso à rede	(Opcional) Insira os nomes do realm do identificador de acesso à rede para serem utilizados na negociação do Passpoint.
Par de MCC e MNC	(Opcional) Insira os pares de Mobile Country Code (MCC)/Mobile Network Code (MNC) para serem utilizados na negociação do Passpoint. Cada sequência deve conter exatamente seis dígitos.
Nome de exibição do operador	(Opcional) Insira o nome do operador da rede para ser exibido.
Via rápida Cisco QoS	As definições nesta seção se aplicam à configuração de via rápida da Cisco. As configurações incluem adicionar apps na lista de permitidos para as marcações L2 e L3, e a possibilidade de adicionar na lista de permitidos o tráfego de áudio e vídeo de serviços de áudio/vídeo integrados, como o FaceTime e Chamada por Wi-Fi.
Restringir marcação de QoS	Se não selecionado, todos os apps usarão as marcações L2 e L3 quando a rede oferecer suporte à Via rápida Cisco QoS. Se selecionado, use as configurações que aparecem em **Escolher apps** para adicionar os apps a serem incluídos nas marcações L2 e L3. Os apps não selecionados não usarão as marcações L2 e L3.
Ativar marcação de QoS	Desativa a marcação L3 e usa apenas a marcação L2 para o tráfego enviado para a rede Wi-Fi. Quando não selecionado, o sistema trata o Wi-Fi como não associado à rede de Via rápida Cisco QoS.
Incluir na lista de permitidos as chamadas de áudio/vídeo da Apple	Especifica a possibilidade de adicionar na lista de permitidos o tráfego de áudio e vídeo de serviços de áudio/vídeo integrados, como o FaceTime e Chamada por Wi-Fi.
Escolher apps	Use para adicionar os apps que você deseja incluir nas marcações L2 e L3. Os apps não selecionados não usarão as marcações L2 e L3.
iOS 10+	

Configuração	O que fazer
Via rápida Cisco QoS	As definições nesta seção se aplicam à configuração de via rápida da Cisco. As configurações incluem adicionar apps na lista de permitidos para as marcações L2 e L3, e a possibilidade de adicionar na lista de permitidos o tráfego de áudio e vídeo de serviços de áudio/vídeo integrados, como o FaceTime e Chamada por Wi-Fi.
Restringir marcação de QoS	Se não selecionado, todos os apps usarão as marcações L2 e L3 quando a rede oferecer suporte à Via rápida Cisco QoS. Se selecionado, use as configurações que aparecem em **Escolher apps** para adicionar os apps a serem incluídos nas marcações L2 e L3. Os apps não selecionados não usarão as marcações L2 e L3.
Ativar marcação de QoS	Desativa a marcação L3 e usa apenas a marcação L2 para o tráfego enviado para a rede Wi-Fi. Quando não selecionado, o sistema trata o Wi-Fi como não associado à rede de Via rápida Cisco QoS.
Incluir na lista de permitidos as chamadas de áudio/vídeo da Apple	Especifica a possibilidade de adicionar na lista de permitidos o tráfego de áudio e vídeo de serviços de áudio/vídeo integrados, como o FaceTime e Chamada por Wi-Fi.
Escolher apps	Use para adicionar os apps que você deseja incluir nas marcações L2 e L3. Os apps não selecionados não usarão as marcações L2 e L3.
iOS 10.3 ou superior supervisionado	
Habilitar lista de Wi-Fi permitidos	Determina a quais redes Wi-Fi o dispositivo pode se conectar. Se existirem várias configurações Wi-Fi, as mais restritivas serão aplicadas.
iOS 14.0+	

Configuração	O que fazer
Desativar aleatorização do endereço MAC	No iOS 14.0, a Apple modificou o comportamento padrão de um dispositivo que reporta o endereço MAC do Wi-Fi para que ele reporte um endereço aleatório em novas conexões, em vez do endereço MAC do dispositivo. Como resultado, esse recurso pode causar comportamento inesperado para empresas que utilizam portais cativos ou filtram endereços MAC. Os administradores podem **desativar a randomização do endereço MAC** de uma rede Wi-Fi editando a configuração de Wi-Fi associada e habilitando esta opção (que, por padrão, é falsa). Isso fará com que a configuração do Wi-Fi seja reenviada a todos os dispositivos. Essa opção exibe um aviso de privacidade nas Configurações do dispositivo, informando que a rede reduziu as proteções de privacidade. O usuário do dispositivo ainda pode ativar ou desativar manualmente essa opção, acessando as configurações do dispositivo.
Android 11+	
Aleatorização do endereço MAC	• Desabilitado: o Wi-Fi é conectado antes que o usuário faça login no dispositivo. • Habilitado - Automático: o Wi-Fi fica disponível depois que o usuário faz login no dispositivo. • Habilitado - Não persistente • Habilitado - Persistente

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Para obter mais informações, consulte Como criar uma configuração.

Configuração de rede celular

Esta seção contém os seguintes tópicos:

Configuração APN

A configuração APN define o nome do ponto de acesso celular para o dispositivo. Para iOS 7, use Configuração do celular.

Configurações APN

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome do Ponto de Acesso	Insira o nome para o ponto de acesso correspondente. Geralmente, o nome é definido pelo serviço de fornecimento do operador.
Nome de usuário do ponto de acesso	Insira um nome de usuário autorizado para este ponto de acesso.*
Senha do ponto de acesso	Insira a senha correspondente ao nome de usuário inserido.
Servidor proxy e porta	Insira o endereço IP ou URL e o número da porta para o proxy APN.
HabilitarXLAT464	Marque a caixa de seleção para habilitar o nome do ponto de acesso (APN). Esta opção fornece serviços IPv4 em uma rede somente IPv6.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Para obter mais informações, consulte Como criar uma configuração.

Celular

Aplicável para: iOS 7.0+

Esta seção contém os seguintes tópicos:

- Configurações de celular para APN padrão
- Configurações de celular para APNs de dados
- Como controlar o acesso do celular enquanto ele estiver em roaming
- Como controlar o acesso do celular

Uma configuração de celular define o perfil de celular para um dispositivo. Defina as configurações da rede celular em dispositivos que executam iOS 7.0 ou posterior. Algumas empresas possuem contratos com suas operadoras de telefonia celular que fornecem o acesso a um Nome do Ponto de Acesso (APN) exclusivo para acesso à rede remoto ou planos especiais de tarifação. Consultar a operadora de telefonia celular para obter os parâmetros de configuração.

- Não pode ser instalado mais de um perfil de celular ao mesmo tempo.
- Um perfil de celular não pode ser instalado se já houver um perfil APN instalado.

É possível definir as configurações de celular para os seguintes tipos de APN na caixa suspensa **Tipos de APN configurados**:

- APNs padrão e de dados
- APNs padrão
- APNs de dados

Para todas as configurações, insira um nome que as identifique e uma descrição opcional.

Configurações de celular para APN padrão

Configurações de APN padrão	O que fazer
Nome do APN	Insira o nome para o ponto de acesso correspondente. Geralmente, o nome é definido pelo serviço de fornecimento do operador.
Tipo de autenticação APN	(Opcional) Selecione uma das opções a seguir: • CHAP (Challenge Handshake Authentication Protocol, protocolo de autenticação de handshake de desafio) • PAP (Password Authentication Protocol, protocolo de autenticação de senha)
Nome de Usuário	(Opcional) Insira um nome de usuário para ser utilizado na autenticação.
Senha	(Opcional) Insira uma senha para ser utilizada na autenticação.

Configurações de celular para APNs de dados

Configurações de APN de dados	O que fazer
Nome do APN	Insira o nome para o ponto de acesso correspondente. Geralmente, o nome é definido pelo serviço de fornecimento do operador.
Tipo de autenticação APN	(Opcional) Selecione uma das opções a seguir: • CHAP (Challenge Handshake Authentication Protocol, protocolo de autenticação de handshake de desafio) • PAP (Password Authentication Protocol, protocolo de autenticação de senha)
Nome de Usuário	(Opcional) Insira um nome de usuário para ser utilizado na autenticação.
Senha	(Opcional) Insira uma senha para ser utilizada na autenticação.
Servidor proxy	Especifique o servidor proxy.
Porta do servidor proxy	Especifique a porta do servidor proxy.
10.3+	
Máscara de protocolo permitida	Selecione IPv4, IPv6 ou Ambos.
Máscara de protocolo permitida em roaming nacional	Selecione IPv4, IPv6 ou Ambos.
Máscara de protocolo permitida em roaming	Selecione IPv4, IPv6 ou Ambos.

Como controlar o acesso do celular em roaming

Você pode limitar o acesso de alguns ou todos os apps gerenciados para os dados do celular enquanto o dispositivo estiver em roaming.

Procedimento

1. Acesse a aba **Políticas** no menu de navegação principal do Ivanti Neurons for MDM.
2. Clique em **+Adicionar**
3. Clique em **Configuração de uso da rede**.
   A página de configuração Criar uso da rede é exibida.
4. Marque a caixa de seleção **Proibir para todos os apps gerenciados** para impedir que apps gerenciados acessem dados de celular quando em roaming ou a qualquer momento.
5. Deixe a caixa de seleção desmarcada para poder especificar os aplicativos gerenciados por nome ou por ID do pacote que não receberão os dados do celular.
6. Use os menus suspensos no campo Apps para pesquisar por um aplicativo por nome ou por ID do pacote.

Como controlar o acesso do celular

Você pode limitar o acesso de alguns ou todos os apps gerenciados para os dados do celular a qualquer momento. Esses apps ainda podem ser usados de forma limitada, mas eles não têm acesso aos dados do celular.

Procedimento

1. Acesse a aba **Políticas** no menu de navegação principal do Ivanti Neurons for MDM.
2. Clique em **+Adicionar**
3. Clique em **Configuração de uso da rede**.
   A página de configuração Criar uso da rede é exibida.
4. Marque a caixa de seleção **Proibir para todos os apps gerenciados** para impedir que apps gerenciados acessem dados de celular a qualquer momento.
5. Como alternativa, deixe a caixa de seleção desmarcada para especificar os apps gerenciados que não receberão os dados do celular.

6. Use os menus suspensos no campo Apps para pesquisar por um aplicativo por nome ou por ID do pacote.

Para obter mais informações, consulte Como criar uma configuração.

Definição das configurações de telecomunicação para iOS

Uma definição das configurações de telecomunicação para iOS configura os valores padrão para restrições de roaming e ponto de acesso.

Definições das configurações de telecomunicação para iOS

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Permitir que os dispositivos usem serviços de voz enquanto estiverem em roaming	Selecione para habilitar o roaming de voz. A disponibilidade do roaming de voz depende do operador.
Permitir que os dispositivos usem serviços de dados enquanto estiverem em roaming	Selecione para habilitar o roaming de dados. Ativar o roaming de dados também ativa o roaming de voz no dispositivo.
Permitir que os usuários habilitem o ponto de acesso pessoal	Selecione para habilitar o recurso de ponto de acesso pessoal. A disponibilidade desse recurso depende do operador.

Para obter mais informações, consulte Como criar uma configuração.

Configuração de eSIM

A configuração de iSIM configura a rede celular nos dispositivos com o comando `RefreshCellularPlans`. Os administradores devem obter a URL da operadora eSIM antes de mapear a rede celular do dispositivo.

Aplicável para: iOS, iPadOS

Procedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **eSIM** no campo de pesquisa e, então, clique na configuração de **eSIM**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Clique em **iOS/iPadOS**.
5. Digite a URL da operadora.
6. Clique em **Avançar**.
7. Selecione a opção **Ativar esta configuração**.
8. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizado.
9. Clique em **Concluído**.

Outra configuração

Esta seção contém os seguintes tópicos:

Configuração Domínios Associados

Licença: Gold

A configuração Domínios Associados é um dicionário que mapeia os aplicativos a seus domínios associados. Domínios associados podem ser usados com recursos como AppSSO extensível, links universais e preenchimento automático de senha.

As configurações de Domínios Associados são as seguintes:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Identificador do aplicativo	(Obrigatório) O identificador de aplicativo ao qual associar os domínios.
Domínios associados	(Obrigatório) Os domínios a serem associados ao aplicativo. Cada string está na forma "serviço:domínio". Os domínios devem ser nomes de host totalmente qualificados, como www.exemplo.com.
Habilitar download direto	Se verdadeiro, os dados desse domínio devem ser baixados diretamente em vez de por meio de uma CDN. O valor de qualificação para esse domínio deve ser definido como service:domain?mode=managed ou o valor será ignorado. Disponível em macOS 11 e posteriores. **Padrão**: falso

Configuração de transferência de arquivo do Android

A configuração de transferência de arquivo está disponível no Catálogo de Aplicativos para dispositivos Android. Usando essa configuração, o administrador pode fornecer uma opção para que se transfiram, no dispositivo, arquivos a serem compartilhados entre diferentes aplicativos permitidos que estejam presentes no mesmo aparelho. Os outros aplicativos podem usar o arquivo para atualizar ou inicializar arquivos de aplicativo. Essa configuração é compatível com os modos de dispositivo totalmente gerenciado.

Por padrão, o limite máximo de tamanho para o arquivo é 50 MB. No caso de licenças independentes, mais opções de armazenamento estão disponíveis.

Procedimento

1. Acesse **Configuração** > **Configuração de transferência de arquivo**.
2. Insira um nome para configuração na caixa **Nome**.

   Definição da configuração

3. Na seção **Arquivo a transferir**, selecione os arquivos a serem transferidos usando a opção de Arrastar e soltar ou navegando pela opção Escolher arquivo.
4. Em **Baixar para o dispositivo**, selecione uma ou mais entre estas opções:

   - Permitir download via rede limitada - selecione para continuar baixando o arquivo mesmo em uma rede limitada
   - Exigir carregamento - selecione para garantir que o dispositivo esteja carregando durante o processo de transferência de arquivos
   - Exigir inatividade do dispositivo - selecione para manter o dispositivo inativo durante o processo de transferência de arquivos

   Compartilhar um arquivo com outros aplicativos

   Você pode usar as opções **Configuração de Aplicativos Gerenciados Android** ou **Intenção no Dispositivo**.

   Configuração de aplicativo gerenciado do Android (as etapas 5 e 6 são apenas para a opção Configuração de Aplicativo Gerenciado do Android) - use esta opção se o app de destino puder consumir URI de Conteúdo usando sua Configuração de Aplicativo Gerenciado.

5. Escolha um atributo personalizado existente, baseado em dispositivo, para compartilhar o arquivo com outros apps.
6. Fornecer acesso aos seguintes aplicativos e/ou nomes de pacote: você pode selecionar nomes de app no seletor Nomes de aplicativo e adicionar nomes de pacote nas caixas Nomes de Aplicativo / ID do Pacote.

   Nomes de aplicativo - você pode selecionar nomes de aplicativo no seletor Nomes de aplicativo

   IDs de pacote - você pode inserir os IDs de pacote nessa área

   Intenção no dispositivo (as etapas 7,8 e 9 são apenas para a opção Intenção no dispositivo) - as intenções são específicas do aplicativo. Para compartilhar um arquivo usando essa opção, consulte a documentação do aplicativo de destino e forneça as informações a seguir.
7. Selecione um aplicativo na lista **Fornecer acesso a um aplicativo específico**.
8. Forneça os valores **Intenções-Padrão** da lista.
9. Forneça os valores **Intenções-Extras** em CHAVE, TIPO e VALOR.
10. Clique em **Avançar**.
11. Selecione as opções de distribuição necessárias e clique em **Concluído**.

Você pode encontrar as informações de URI do conteúdo na guia Atributos de um dispositivo. Isso fornece as informações sobre o local de armazenamento do arquivo no dispositivo.

Configuração da Apple TV

Licença: Silver

Uma configuração Apple TV define o idioma e o local para a Apple TV.

As configurações da Apple TV são as seguintes:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Idioma	Insira o código de idioma com dois caracteres para especificar o idioma da IU.
Local	Insira a ID do local para especificar a combinação de país/idioma para a IU.

Para obter mais informações, consulte Como criar uma configuração.

Espelhamento do AirPlay

Licença: Gold

O AirPlay Mirroring é uma ferramenta que permite que você exiba a tela de qualquer dispositivo iOS em um monitor usando a Apple TV. A Apple TV e o dispositivo iOS devem estar conectados na mesma rede Wi-Fi. Este recurso requer os seguintes dispositivos:

- iOS 7 e dispositivos mais recentes - Supervisionados
- macOS 10.10 e dispositivos mais recentes – Supervisionados
- Versão Apple TV - Supervisionada
- AirPlay

A alternância para incluir a gestão de dispositivos não iOS não poderá ser revertida.

Esta seção contém os seguintes tópicos:

- Como configurar o Apple AirPlay
- Como configurar o AirPlay no dispositivo móvel
- Como configurar o monitor para funcionar com a Apple TV
- Como conectar seu dispositivo iOS à Apple TV

Como configurar o Apple AirPlay

Para obter mais informações sobre as configurações do AirPlay, consulte Configuração do AirPlay.

Procedimento

1. Vá até **Configurações**.
2. Clique em **+Adicionar**.
3. Clique em **AirPlay**.
4. Insira um Nome e uma Descrição para a configuração nos devidos campos.
5. Para todas as versões de iOS que recebem suporte, insira um Nome do dispositivo e a Senha.
6. Clique em + **Adicionar** para adicionar outro dispositivo, se necessário.

7. Também é possível adicionar IDs de dispositivos a uma lista de permissão para dispositivos iOS 7+ ou macOS 10.10+ supervisionados.
8. Clique em **Avançar**.
9. Escolha um nível de distribuição.
10. Clique em **Concluído**.

Como configurar o AirPlay no dispositivo móvel

Procedimento

1. Configure o Apple Configurator.
2. Acesse **Dispositivos > Dispositivos**.
3. Clique no nome de um dispositivo iOS para exibir a página Detalhes do dispositivo.
4. Clique no ícone .
5. Selecione **AirPlay Mirroring** para exibir a caixa de diálogo do AirPlay Mirroring.
6. Selecione um dispositivo Apple TV do menu suspenso.
7. Insira um tempo de verificação em segundos para especificar um limite de tempo para pesquisar pelo dispositivo que você selecionou.
8. Insira a senha do dispositivo Apple TV.
9. Clique em **Enviar Solicitação**.

Como configurar o monitor para funcionar com a Apple TV

Procedimento

1. Em um monitor conectado à Apple TV, vá para **Configurações > Perfil**.
2. Selecione **Apple Configurator do Ivanti Neurons for MDM**.
3. Clique em **Adicionar Perfil**.
4. Clique no ícone .

5. Selecione **AirPlay Mirroring** para exibir a caixa de diálogo do AirPlay Mirroring.
6. Selecione um dispositivo Apple TV do menu suspenso.
7. Insira um tempo de verificação em segundos para especificar um limite de tempo para pesquisar pelo dispositivo que você selecionou.
8. Insira a senha do dispositivo Apple TV.
9. Clique em **Enviar Solicitação**.

Como conectar seu dispositivo iOS à Apple TV

Procedimento

1. Conecte o dispositivo Apple TV a um monitor.
2. Ao usar a Apple TV remotamente, acesse **Configurações > Contas > Compartilhamento doméstico** para ativar o Compartilhamento doméstico.
3. **Conecte o dispositivo iOS** à mesma rede Wi-Fi em que se encontra o seu **dispositivo Apple TV**.
4. Abra o Aplicativo remoto no seu dispositivo **iOS**.
5. Ative o **Compartilhamento doméstico** por meio da tela **Configurações remotas**.

Configurações do navegador

Usando Configurações do navegador, é possível definir as configurações e as restrições para Google Chrome, Mozilla Firefox, Microsoft Edge e Internet Explorer em dispositivos Windows 10.

Este recurso exige o Bridge. Consulte "Ivanti Bridge" na página 429 para detalhes.

Tenha certeza de que os navegadores estão instalados no dispositivo antes de aplicar as configurações do navegador.

Para ajustar as configurações do navegador:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a definição **Configurações do navegador**.
3. Insira um nome para a configuração.
4. Insira uma descrição.

5. Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela a seguir.

Configuração	O que fazer
Navegadores	Selecione o tipo de navegador que é necessário configurar: • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**

Configurações do navegador	Configure as seguintes opções: **Permitir navegadores**: • **Permitir salvar senhas** • **Permitir modo de navegação segura** • **Permitir que plugins desatualizados permaneçam no navegador** **Chrome e Firefox**: • **Permitir exclusão do histórico do navegador** **Chrome e Internet Explorer**: • **Permitir impressão pelo navegador** • **URL da página de nova guia** **Somente Chrome**: • **Mostrar atalhos de apps na barra de favoritos** • **Mostrar botão Início** • **Permitir sincronização de dados com o Google** • **Continuar executando apps de segundo plano quando o Chrome for fechado** **Somente Firefox**: • **Permitir instalação de extensões** **Somente Internet Explorer**: • **Permitir o download de dados de sites**

Favoritos do navegador	Clique em **+Adicionar**. A janela **Adicionar favorito do navegador** é exibida. Configure os seguintes campos: • **Nome de exibição**: Digite o nome de exibição do favorito • **URL**: digite a URL do favorito do navegador. Clique em **Adicionar**. Os detalhes do favorito do navegador adicionado são exibidos na página. Na coluna **Ações**, clique no ícone Editar para editar a configuração. Para excluir o favorito do navegador, clique no ícone Excluir. **Nome da pasta de favoritos do navegador**: Digite o nome da pasta onde os favoritos do navegador devem ser relacionados. Também é possível adicionar um favorito do navegador no formato CSV. Para carregar em formato CSV: a. Clique em Carregar arquivo CSV. Navegue e escolha o arquivo CSV a ser carregado. b. Clique em **Upload**. Os detalhes no arquivo CSV devem ser adicionados no seguinte formato: • A primeira coluna (Nome de exibição) deve especificar o nome de exibição do favorito. Por exemplo: "compras". • A segunda coluna (URL) deve especificar a URL do favorito. Exemplo: "https://amazon.com".

Segurança do site	Configure as seguintes definições de segurança do site: **Todos os sites (Chrome e Firefox)** • **Bloquear cookies** • **Bloquear javascript** • **Bloquear plugins** • **Bloquear popups** Sites específicos (somente Chrome) **Sites bloqueados (Chrome e Edge)**: adicione o site que você deseja bloquear. Clique em **+Adicionar**. A janela **Adicionar site bloqueado** é exibida. Em **URL do site**, digite o URL do site que deve ser bloqueado. No campo **Acesso**, selecione **Bloquear** para inserir o site na lista de bloqueados. A opção padrão é **Permitir**. Clique em **Adicionar**.

Extensões do navegador	**Tipos de extensão permitidos (somente Chrome)**: selecione uma das seguintes opções: • **Extensão** • **Script do usuário** • **Temas** • **Aplicativo empacotado** • **Aplicativo hospedado** • **Aplicativo de plataforma** **Origens de extensão do navegador (somente Chrome)**: Clique em **+Adicionar** para adicionar origens de extensão do navegador. Após a adição das origens de extensão do navegador, você pode editá-las ou excluí-las clicando nas opções relevantes na coluna **Ações**. **Extensões de instalação forçada (somente Chrome)**: Clique em **+Adicionar** para adicionar extensões de instalação forçada. Após a adição das extensões de instalação forçada, você pode editá-las ou excluí-las clicando nas opções relevantes na coluna **Ações**.

6. Clique em **Avançar**.

7. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
8. Clique em **Concluído**.

Configuração do modo de aplicativo único para iOS

Licença: Silver

O modo de aplicativo único restringe os dispositivos com iOS ao uso do aplicativo especificado. Por exemplo, você pode querer configurar dispositivos que possam usar somente um aplicativo personalizado desenvolvido por sua empresa.

Procedimento

1. Acesse **Configurações > Adicionar > Modo de aplicativo único**.
2. Use as diretrizes a seguir para definir o aplicativo e as configurações relacionadas.

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Escolher aplicativo	Escolha o método a ser usado para selecionar o aplicativo: • **Em Catálogo de Aplicativos e aplicativos do sistema:** selecione para pesquisar o Catálogo de Aplicativos do Ivanti Neurons for MDM e os aplicativos do sistema (pré-instalados nos dispositivos Apple por padrão). • Insira o nome do aplicativo e selecione-o quando ele for exibido na lista de apps. • **Inserir ID do grupo:** selecione para inserir o identificador exclusivo do aplicativo do sistema que você deseja selecionar. Use esta opção se não conseguir localizar o aplicativo do sistema usando a opção **Do App Catalog e dos aplicativos do sistema**.
Desativar toque	Selecione para desabilitar a tela sensível ao toque.
Desabilitar rotação do dispositivo	Selecione para desabilitar o sensor de rotação do dispositivo.
Desabilitar botões de volume	Selecione para desabilitar os botões de volume do dispositivo.
Desabilitar interruptor da campainha	Selecione para desabilitar o interruptor da campainha do dispositivo.
Desabilitar botão suspender/reativar	Selecione para desabilitar o botão suspender/reativar do dispositivo (canto superior direito na borda do dispositivo).

Desabilitar bloqueio automático	Selecione para impedir que o dispositivo vá para o modo de suspensão após o período ocioso.
Ativar narração	Selecione para habilitar o leitor de tela VoiceOver (recurso de acessibilidade).
Ativar zoom	Selecione para habilitar o zoom (recurso de acessibilidade).
Habilitar inversão de cores	Selecione para habilitar o ajuste da inversão de cores (recurso de acessibilidade).
Ativar toque de assistência	Selecione para habilitar o AssistiveTouch (recurso de acessibilidade).
Habilitar seleção da fala	Selecione para habilitar a Seleção da fala (recurso de acessibilidade).
Habilitar áudio mono	Selecione para alternar de áudio estéreo para mono (recurso de acessibilidade).
Ajustes da narração	Selecione para permitir que os usuários do dispositivo façam ajustes no VoiceOver.
Ajustes do zoom	Selecione para permitir que os usuários do dispositivo façam ajustes no Zoom.
Ajustes da inversão de cores	Selecione para permitir que os usuários do dispositivo invertam as cores.
Ajustes do toque de assistência	Selecione para permitir que os usuários façam ajustes no AssistiveTouch.

3. Clique em **Avançar**.
4. Na tela **Distribuição**, selecione os grupos de dispositivos que receberão essa configuração.
5. Clique em **Concluído**.

Se você configurou o discador do telefone como o aplicativo a ser usado, o botão Início funcionará assim que o dispositivo entrar no modo de aplicativo único.

Configuração de um perfil de MDM para iOS

A configuração de MDM para iOS define os limites de acesso do Ivanti Neurons for MDM. Existem dois tipos de configurações de MDM com iOS:

- **MDM para iOS - provisionado em massa:** para dispositivos adquiridos pela empresa e provisionados como parte de uma distribuição em massa.
- **MDM para iOS - provisionado individualmente:** para dispositivos provisionados um a um. Não aplicável a dispositivos supervisionados e registrados pelo usuário.

Somente um de cada tipo é fornecido e permitido em todos os Espaços.

Editar uma configuração de MDM para iOS

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá até **Configurações**.
3. Selecione a configuração de MDM para iOS que você deseja editar.
4. Clique no ícone de lápis (editar) para editar a configuração.
5. Use as diretrizes a seguir para fazer alterações:

Configuração	O que fazer
Direitos de Acesso do MDM	
Permitir a remoção de bloqueio e senha do dispositivo	Desmarque para evitar a execução de uma configuração de conformidade de senha.
Permitir apagamento do dispositivo	Desmarque para impedir que uma ação de apagamento seja aplicada ao dispositivo.
Permitir a consulta de informações de rede (números de telefone/SIM, endereços MAC)	Desmarque para impedir o dispositivo de fornecer informações de rede. Se esta opção estiver desmarcada, a exibição da lista de dispositivos e a exibição dos detalhes do dispositivo exibirão N/A para as informações da rede que não forem mais informadas. Além disso, a política de roaming não será imposta aos dispositivos afetados.
Senha de remoção de perfil	
Senha para remover o perfil	Especifique uma senha. O usuário será solicitado a inserir a senha ao excluir um perfil do dispositivo.

Configuração	O que fazer
ADICIONAR aplicativo necessário (iOS 15+)	
Adicionar por consulta	Digite o nome o aplicativo, procure-o na App Store e selecione o aplicativo necessário. Apenas um aplicativo pode ser adicionado por vez. Selecionar um aplicativo desativa os outros apps.
Adicionar manualmente	Insira o ID do iTunes do aplicativo.

6. Clique em **Concluído**.

   Suas alterações se aplicam apenas aos dispositivos provisionados após você fazer a alteração.

Configuração de um perfil de MDM para macOS

A configuração de MDM para macOS define os limites de acesso do Ivanti Neurons for MDM. As configurações de MDM para macOS são oferecidas individualmente para dispositivos provisionados um a um.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá até **Configurações**.
3. Selecione a configuração de MDM para macOS que você deseja editar.
4. Clique no ícone de lápis (editar) para editar a configuração.

5. Use as diretrizes a seguir para fazer alterações:

Configuração	O que fazer
Permitir a remoção de bloqueio e senha do dispositivo	Desmarque para evitar a execução de uma configuração de conformidade de senha.
Permitir apagamento do dispositivo	Desmarque para impedir que uma ação de apagamento seja aplicada ao dispositivo.
Permitir a consulta de informações de rede (números de telefone/SIM, endereços MAC)	Desmarque para impedir o dispositivo de fornecer informações de rede. Se esta opção estiver desmarcada, a exibição da lista de dispositivos e a exibição dos detalhes do dispositivo exibirão N/A para as informações da rede que não forem mais informadas. Além disso, a política de roaming não será imposta aos dispositivos afetados.
Senha de remoção de perfil	
Senha para remover o perfil	Especifique uma senha. O usuário será solicitado a inserir a senha ao excluir um perfil do dispositivo.

6. Clique em **Concluído**.

   Suas alterações se aplicam apenas aos dispositivos provisionados após você fazer a alteração.

Cache de conteúdo

Licença: Gold

Aplicável a: macOS 10.13.4 ou a versões mais recentes com suporte.

Configure o serviço de cache de conteúdo para habilitar cópias locais do software da App Store e habilitar clientes conectados para downloads mais rápidos de software e aplicativos.

Configuração de cache de conteúdo

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **cache** no campo de pesquisa e, em seguida, clique na configuração de **Cache de conteúdo**.
4. Digite um nome e descreva a configuração.
5. Insira as definições da configuração de cache de conteúdo.
6. Clique em **Avançar**.
7. Selecione a opção **Habilitar essa configuração**.
8. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
9. Clique em **Concluído** .

Definições da configuração de cache de conteúdo

Use as definições na tabela a seguir para configurar o cache de conteúdo. Para obter mais informações sobre essas definições, consulte a Documentação da Apple.

Configuração	Descrição
Permitir que o sistema remova o conteúdo do cache automaticamente (Disponível para macOS 10.15 ou versões mais recentes com suporte.	Permitir que o sistema limpe o conteúdo do cache automaticamente quando precisar de espaço em disco para outros aplicativos (ou seja, quando o espaço livre em disco ficar baixo no computador). Por padrão, essa opção está habilitada.
Permitir cache de conteúdo	Armazena em cache os dados do iCloud do usuário. Os clientes podem demorar algum tempo (horas ou dias) para reagir às alterações nessa definição; ela não tem um efeito imediato. Por padrão, essa opção está habilitada.
Permitir cache compartilhado	Armazena em cache o conteúdo não iCloud, como atualizações de apps e software. Os clientes podem demorar algum tempo (horas ou dias) para reagir às alterações nessa definição; ela não tem um efeito imediato. Por padrão, essa opção está habilitada.
Permitir a ativação automática do cache de conteúdo	Ativa automaticamente o cache de conteúdo quando possível e evita que ele seja desativado.
Permitir habilitação automática de cache tethered (Disponível para macOS 10.15.4 ou versões mais recentes com suporte	Ativa automaticamente o compartilhamento de conexão com a Internet quando possível e evita desativar o compartilhamento de conexão com a Internet.
Desativar o cache tethered	Desativa o cache conectado. A opção Desativa o cache conectado substitui a opção Permitir habilitação automática de cache conectado.

Configuração	Descrição
Limite de cache	O número máximo de bytes de espaço em disco que será utilizado para o cache do conteúdo. Um valor de 0 significa espaço em disco ilimitado. Valor padrão: 0
Caminho de dados	O caminho para o diretório usado para armazenar o conteúdo em cache. Armazenar em cache essa definição manualmente não move automaticamente o conteúdo em cache do local antigo para o novo. Para mover o conteúdo automaticamente, use o painel Cache de conteúdo das preferências de Compartilhamento. O valor deve ser (ou terminar em) /Library/Application Support/Apple/AssetCache/Data.
Permitir alertas na tela (Disponível para macOS 10.15 ou versões mais recentes com suporte.	O Cache de conteúdo exibe condições excepcionais (alertas) como notificações do sistema no canto superior da tela.
Manter o dispositivo ativado (Disponível para macOS 10.15 ou versões mais recentes com suporte.	Impede que o computador entre em suspensão enquanto o Cache de conteúdo estiver ativo (Preferências do sistema > Compartilhamento > Cache de conteúdo está ativo).
Escutar intervalos	Uma matriz de dicionários que descreve um intervalo de endereços IP de clientes para servir.
Primeiro endereço IP	Primeiro endereço IP dos clientes nos Intervalos de escuta.
Último endereço IP	Último endereço IP dos clientes nos Intervalos de escuta.
Tipo de endereço IP	Selecione uma das opções a seguir: • IPv4 (padrão) • IPv6

Configuração	Descrição
Permitir somente faixas de escuta	O cache de conteúdo fornece conteúdo apenas aos clientes nos Intervalos de escuta.
Permitir escuta com pares e pais	O cache de conteúdo fornece conteúdo apenas aos clientes na união dos Intervalos de escuta, Intervalos de escuta de par e Pais. Por padrão, essa opção está habilitada.
Permitir apenas subredes locais	O cache de conteúdo oferece conteúdo apenas aos clientes na mesma rede local imediata. Nenhum conteúdo é oferecido a clientes de outras redes que possam ser alcançadas pelo cache de conteúdo. Se essa opção estiver ativada, os Intervalos de escuta serão ignorados. Por padrão, essa opção está habilitada.
Registrar identidade do cliente	O Cache de conteúdo registra o endereço IP e número de porta dos clientes que solicitam o conteúdo.
Política de seleção de pais	Selecione uma das opções de política a seguir: • Primeiro disponível • Hash de caminho de URL • Round-robin (padrão) • Aleatório • Sticky-Disponível
Pais	Uma matriz de endereços IP locais de outros caches de conteúdo que esse cache deve baixar ou para o qual carregar, em vez de baixar ou carregar diretamente para a Apple. Clique em **+ Adicionar** para adicionar um ou mais endereços IP.
Permitir apenas subredes locais de pares	O cache de conteúdo faz par apenas com outros caches de conteúdo na mesma rede local imediata e não com outros caches de conteúdo que usam o mesmo endereço IP público que o dispositivo. Por padrão, essa opção está habilitada.

Configuração	Descrição
Porta	O número de porta TCP na qual o cache de conteúdo aceita solicitações para uploads e downloads. Defina a porta para 0 para selecionar uma porta disponível aleatória. Valor padrão: 0
Intervalos públicos	Uma matriz de dicionários que descreve um intervalo de endereços IP públicos que os servidores do Ivanti Neurons for MDM devem usar para corresponder clientes a caches de conteúdo.
Primeiro endereço IP	Primeiro endereço IP dos servidores nos Intervalos públicos.
Último endereço IP	Último endereço IP dos servidores nos Intervalos públicos.
Tipo de endereço IP	Selecione uma das opções a seguir: • IPv4 (padrão) • IPv6

Para obter mais informações, consulte Como criar uma configuração.

Criação de um atalho do Android

Atalhos estão disponíveis apenas em Modo de quiosque usando um navegador permitido. O navegador deve ser permitido na configuração de Quiosque e

Bloqueio. Os atalhos serão exibidos no ativador de quiosque do Ivanti Neurons for MDM.

Procedimento

1. Vá até **Configurações**. **>** **+Adicionar**
2. Clique em **Atalho do Android** para exibir a página **Criar Configuração de Atalho do Android**.
3. Insira um nome para a configuração no campo **Nome**.
4. Insira a descrição da configuração no campo **Descrição**.
5. Insira um rótulo exclusivo para o atalho no campo **Rótulo**.
6. Insira o URL referente ao destino do atalho no campo **URL**.
7. Opcionalmente, arraste e solte um arquivo no campo do ícone ou clique em **Escolher arquivo** para navegar até o arquivo e escolher um ícone para o atalho.
8. Clique em **Avançar**.

Configurações de nome de dispositivo

Licença: Silver

Uma configuração padrão de nome de dispositivo permite criar uma nova configuração que é enviada ao dispositivo no nível de registro ou pós-registro e permite a nomeação do dispositivo. O administrador pode definir nomes padronizados apenas para **dispositivos iOS 8 supervisionados**. Você pode utilizar as variáveis a seguir para elaborar o nome do dispositivo:

- Número de série do dispositivo
- IMEI do dispositivo
- Modelo do dispositivo
- Ivanti Neurons for MDM Nome de usuário (somente usuários locais)
- Unidade Organizacional (OU) LDAP
- Nome Comum (CN) LDAP

Por exemplo, você iria inserir ${deviceSN}-${userOU} para nomes de dispositivos que começam com o número de série do dispositivo e termina com a organização do usuário conforme definida no LDAP.

Configurações de nome de dispositivo padrão (para iOS)

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nome do dispositivo	Insira o formato para o nome de dispositivo padrão, incluindo os atributos de dispositivo e LDAP disponíveis.* Se o nome resultante do dispositivo exceder 63 caracteres, ele será diminuído para garantir que seja exibido corretamente no dispositivo.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.

Digite $ para ver uma lista de variáveis suportadas, se disponíveis, para esse campo.

Configurações de nome do dispositivo (Android)

O nome do dispositivo Android pode ser recuperado pelo Go app. Quando o administrador gera o relatório Detalhes do Dispositivo, é mostrado o nome real do dispositivo em vez do modelo do dispositivo ou o nome do fabricante. Caso o usuário altere o nome do dispositivo, o novo nome será mostrado na próxima vez que o relatório for gerado. O respectivo nome do dispositivo pode ser visualizado em **Dispositivos** > **Configurações** > **Nome do dispositivo**.

Ethernet (macOS)

Licença: Gold

Aplicável a: macOS 10.13+ ou a versões mais recentes com suporte.

O administrador pode configurar a interface Ethernet em variações. As seguintes cargas úteis estão disponíveis para configurar a Ethernet:

- Ethernet global
- Primeira Ethernet ativa
- Primeira Ethernet
- Segunda Ethernet ativa
- Segunda Ethernet
- Terceira Ethernet ativa
- Terceira Ethernet

As diferentes cargas úteis para configurar a Ethernet são fallback padrão Global, Primeira, Primeira ativa, Segunda, Segunda ativa, Terceira e Terceira interface Ethernet ativa. A Apple tem um problema conhecido com a instalação da primeira, primeira interface ativa, segunda, segunda ativa, terceira e terceira interface Ethernet ativa.

Configuração de Ethernet

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.
3. Digite **Ethernet** no campo de pesquisa e, então, clique na configuração de **Ethernet**.
4. Digite um nome e descreva a configuração.
5. Escolha a configuração da lista suspensa.

6. Insira os ajustes de configuração de Ethernet.
7. Clique em **Avançar**.
8. Selecione a opção **Habilitar essa configuração**.
9. Selecione uma das seguintes opções de canal para aplicar a configuração:
    - Canal do dispositivo (mais comum)
    - Canal do usuário (usuário atualmente registrado)
10. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
11. Clique em **Concluído** .

Ajustes de configuração de Ethernet

Use as definições na tabela a seguir para configurar a Ethernet. Para obter mais informações sobre essas definições, consulte a Documentação da Apple.

Configuração	Descrição
Protocolos	
Tipos de EAP aceitos	Selecione os tipos de EAP que podem ser utilizados para acessar essa rede: • Transport Layer Security (TLS): o TLS é um protocolo que estabelece uma sessão criptografada entre dois computadores na Internet. Ele verifica a identidade do servidor e evita que hackers interceptem quaisquer dados. • TTLS: no campo **Identidade interna**, selecione um dos protocolos de autenticação, como Padrão do SO, PAP, CHAP, MSCHAP, MSCHAPv2 e EAP. • PEAP • LEAP • EAP-SIM: no campo **Número EAP SIM de RANDs**, selecione o número de rands na lista suspensa. • EAP-AKA • EAP-FAST: selecione a opção EAP-FAST que define os métodos de autenticação: ◦ **Usar PAC**: selecione para usar uma configuração automática de proxy (PAC). ◦ **Fornecer PAC**: selecione para permitir o fornecimento de um PAC. Caso contrário, somente um PAC já fornecido no dispositivo poderá ser utilizado. Essa opção estará disponível somente se você selecionou Usar PAC. ◦ **Fornecer PAC anonimamente**: selecione para permitir o fornecimento de um PAC sem autenticar o servidor. Essa opção estará disponível somente se você selecionou Fornecer PAC.

Configuração	Descrição
Autenticação	**Nome de usuário**: especifique o nome de usuário necessário para o acesso à rede. Se você deixar esse campo em branco, o usuário do dispositivo deverá fornecer um. • Usar senha por conexão: selecione para solicitar uma senha para cada conexão ao usuário do dispositivo. Quando o dispositivo acessar novamente a mesma rede, o usuário deverá reautenticar para ingressar na rede. Toda vez que a conexão é iniciada, a senha é solicitada. • Solicitar senha de uso único quando conectado à rede: a senha é solicitada apenas uma vez quando a configuração é enviada ao dispositivo. A senha não será solicitada a cada conexão e desconexão da rede. **Senha**: (opcional) Insira a senha para acessar essa rede. Caso contrário, o usuário do dispositivo deverá fornecer uma senha obrigatória para acessar a rede. **Identidade externa**: (opcional) Para TTLS, PEAP e EAP-FAST, selecione para permitir que os usuários do dispositivo ocultem sua identidade. O nome real do usuário é exibido somente dentro do túnel criptografado. Essa opção pode aumentar a segurança, pois um invasor não conseguirá ver o nome do usuário autenticado de forma clara. **Identidade de origem de credenciais do modo de sistema**: o modo de sistema é usado para autenticação do computador. A autenticação usando o modo de sistema ocorre antes de um usuário efetuar login no computador. O modo de sistema é normalmente configurado para fornecer autenticação com o certificado X.509 do computador (EAP-TLS) emitido por uma autoridade de certificação local.
Confiar	**Certificados confiáveis: Certificado CA do agente MobileIron** **Nomes de certificados do servidor confiáveis**: adicione o nome do certificado • **Permitir exceções de confiança**: permite decisões de confiança (via diálogo) tomadas pelo usuário • **Exigir certificado do TLS** **Versão TLS máxima permitida com autenticação EAP** **Versão TLS mínima permitida com autenticação EAP** **Certificados confiáveis TLS: Certificado CA do agente MobileIron**

Para obter mais informações, consulte Como criar uma configuração.

Configuração de integração do servidor EMA

A configuração da Integração do servidor EMA permite que os dispositivos Windows 10 sejam vinculados ao servidor Intel EMA configurado. Para vincular dispositivos ao servidor Intel EMA configurado, forneça o diretório de instalação do agente EMA original e carregue o arquivo .msh do agente EMA no novo servidor EMA.

Este recurso exige o Bridge. Consulte Bridge para detalhes.

Procedimento

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Integração do servidor EMA**.
3. Insira o nome da configuração.
4. Na seção Definição da configuração, clique em **Escolher arquivo** para selecionar o arquivo .msh do agente EMA.

   O arquivo msh é um arquivo de política do agente que pode ser baixado do servidor EMA.

5. No campo **diretório da Instalação do agente EMA** original, insira o local em que o arquivo EmaAgent.exe original está instalado.
6. Clique em **Avançar**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
8. Clique em **Concluído**.

Configuração da imagem de fundo do dispositivo

Licença: Silver

A configuração da imagem de fundo do dispositivo define uma imagem padrão para a tela inicial e a tela de bloqueio de dispositivos Android 7.0 no modo Proprietário do Dispositivo ou de dispositivos COPE (com exceção de dispositivos Android 11 em modo EPO). Os usuários do dispositivo podem alterar a imagem de fundo distribuída no dispositivo (Configurações > Imagens de fundo e brilho).

Configurações da imagem de fundo do Android

Para definir uma imagem de fundo padrão para dispositivos Android:

1. Vá até **Configurações**.
2. Clique em **+ Adicionar**.
3. Clique em **Imagens de fundo de dispositivos**.
4. Clique no ícone do Android para visualizar a seção Configuração da instalação do Android e definir as seguintes configurações

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Fazer upload de imagem de fundo do Android	
Use a mesma imagem para Tela inicial e tela de bloqueio	Selecione para fazer o upload de uma única imagem para ambas as telas.
Tela inicial	Arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecioná-lo.
Tela de bloqueio	Arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecioná-lo.

5. Clique em **Avançar**
6. Selecione uma das opções de distribuição a seguir:
   - **Todos os dispositivos**
   - **Nenhum dispositivo** (padrão)
   - **Personalizada**
7. Clique em **Concluído**.

> A imagem carregada deve estar no formato .jpg ou .png.

Configurações da imagem de fundo do iOS

Você pode definir uma imagem de papel de parede padrão para dispositivos iOS.

> Esta configuração é aplicável apenas a dispositivos supervisionados.

1. Vá até **Configurações**.
2. Clique em **+ Adicionar**.
3. Clique em **Imagens de fundo de dispositivos**.
4. Clique no ícone do iOS para visualizar a seção Configuração da instalação do iOS e definir as seguintes configurações

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Fazer upload de imagem de fundo do iPhone	
Use a mesma imagem para Tela inicial e tela de bloqueio	Selecione para fazer o upload de uma única imagem para iPhone.
Tela inicial	Arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecioná-lo.
Tela de bloqueio	Arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecioná-lo.
Fazer upload de imagem de fundo do iPad	
Use a mesma imagem para Tela inicial e tela de bloqueio	Selecione para fazer o upload de uma única imagem para iPad.
Tela inicial	Arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecioná-lo.
Tela de bloqueio	Arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecioná-lo.

5. Clique em **Avançar**.

6. Selecione uma das opções a seguir:
    - **Todos os dispositivos**
    - **Nenhum dispositivo** (padrão)
    - **Personalizada**
7. Clique em **Concluído**.

> As imagens enviadas devem ter 1.164 (A) x 640 (L) e no formato .jpg ou .png.

Configurações de papel de parede do macOS

Para definir uma imagem de papel de parede padrão para dispositivos macOS:

1. Vá até **Configurações**.
2. Clique em **+ Adicionar**.
3. Clique em **Imagens de fundo de dispositivos**.
4. Clique no ícone do macOS para visualizar a seção Configuração da instalação do macOS.
5. Insira o caminho para a imagem de desktop.
6. Clique em **Avançar**.
7. Selecione uma das opções a seguir:
    - **Todos os dispositivos**
    - **Nenhum dispositivo** (padrão)
    - **Personalizada**
8. Clique em **Concluído**

> Você pode alterar os papéis de parede com base na restrição. Se a configuração de restrições **Permitir modificação do papel de parede** do macOS estiver ativada, então será possível modificar o papel de parede.

Para obter mais informações, consulte Como criar uma configuração.

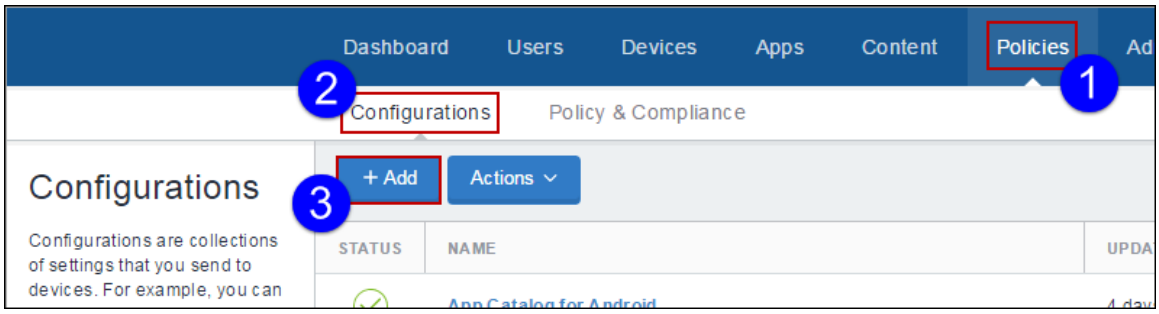
Configuração da mensagem da tela de bloqueio

Exibe uma mensagem e informações do rótulo do ativo nas telas de login e de bloqueio. Para dispositivos supervisionados usando iOS 9.3 ou versões mais recentes com suporte.

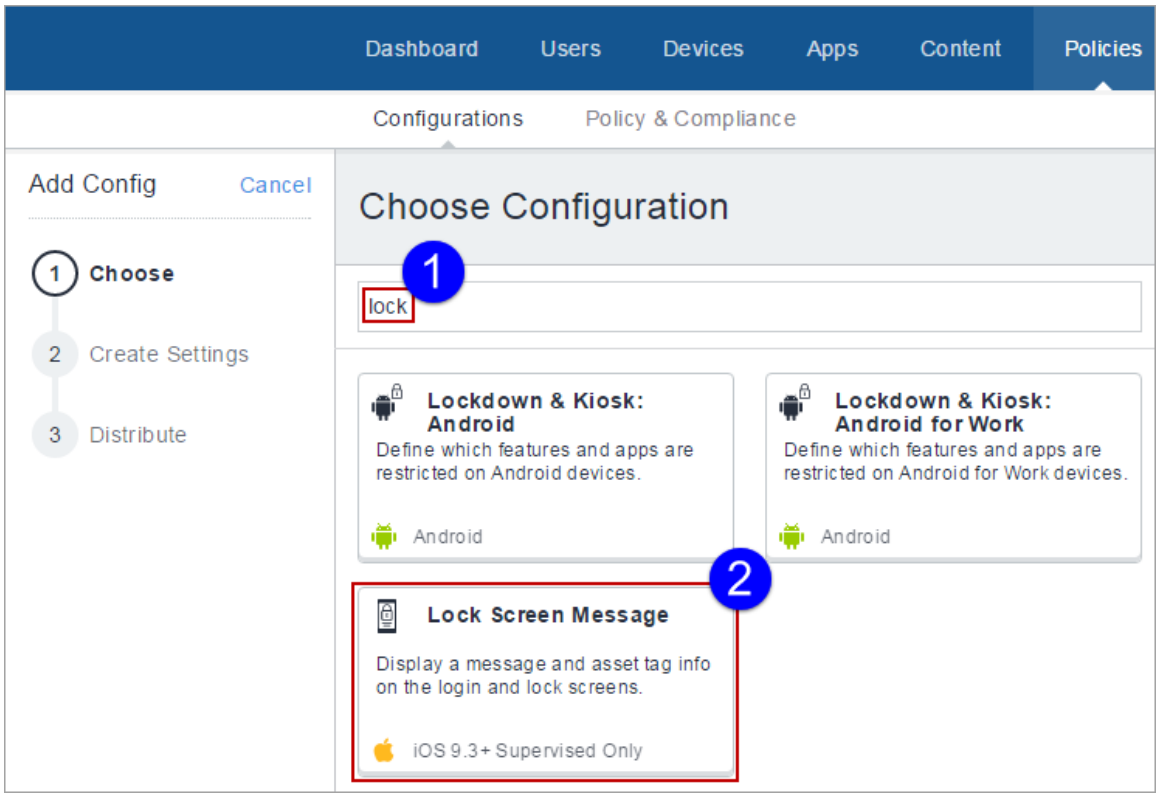
Criação da configuração da mensagem da tela de bloqueio

Procedimento

1. Selecione **Configurações**.
2. Clique em **+ Adicionar**.



3. Digite **bloqueio** no campo de busca e clique na configuração **Mensagem da tela de bloqueio**:



A página de detalhes Configuração da mensagem da tela de bloqueio é exibida.

4. Defina as configurações nessa página. Consulte a tabela na seção Definições de configuração da mensagem da tela de bloqueio para obter informações sobre os valores.

5. Clique em **Próximo** para definir as configurações de distribuição e clique em **Concluído**.

Definições de configuração da mensagem da tela de bloqueio

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Nota de rodapé da tela de bloqueio	Esse texto será exibido na janela de login e na tela de bloqueio.
Informações do rótulo do ativo	Esse texto será exibido na parte inferior da janela de login e da tela de bloqueio.

Para obter mais informações, consulte Como criar uma configuração.

Criar configuração de proteção de tela

A configuração de proteção de tela permite adicionar opções como senha, tempo ocioso, caminho e nome do módulo.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Clique em **Configurações**.
3. Clique em **+Adicionar**.
4. Digite tela no campo de pesquisa e clique em **Proteção de Tela**:

   A página de detalhes Criar Configuração de Proteção de Tela é exibida.
5. Defina as configurações nessa página. Consulte a tabela no tópico **Definições de configuração do protetor de tela** para obter orientação sobre os valores.
6. Clique em **Próximo** para definir as configurações de distribuição e clique em **Concluído**.

Definições de configuração do protetor de tela

Configuração	O que fazer
Nome (obrigatório)	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Caixa de seleção Solicitar senha	Marque a caixa de seleção para solicitar a senha ao usuário do dispositivo quando o protetor de tela for desbloqueado ou interrompido. (Disponível em macOS 10.13 e posteriores).
Atraso ao solicitar senha	Especifique a duração do atraso em segundos.
Tempo ocioso da janela de login	Especifique o tempo ocioso, em segundos, após o qual o protetor de tela deve aparecer.
Caminho para o módulo de proteção de tela	Especifique o caminho do módulo de proteção de tela.
Nome do módulo de proteção de tela (obrigatório)	Digite o nome do protetor de tela.

Para obter mais informações, consulte Como criar uma configuração.

Configurar proteção de tela do usuário

A configuração de proteção de tela do usuário permite adicionar opções como senha, tempo ocioso, caminho e nome do módulo.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Clique em **Configurações**.

3. Clique em **+Adicionar**.
4. Digite tela no campo de pesquisa e clique em **Proteção de Tela do Usuário**:

   A página de detalhes Criar Configuração de Proteção de Tela do Usuário é exibida.
5. Defina as configurações nessa página. Consulte a tabela no tópico **Definições de configuração do protetor de tela do usuário** para orientar-se quanto aos valores.
6. Clique em **Próximo** para definir as configurações de distribuição e clique em **Concluído**.

Definições de configuração do protetor de tela do usuário

Configuração	O que fazer
Nome (obrigatório)	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Tempo ocioso	Especifique o tempo ocioso, em segundos, após o qual o protetor de tela deve aparecer.
Caminho para o módulo de proteção de tela	Especifique o caminho do módulo de proteção de tela.
Nome do módulo de proteção de tela (obrigatório)	Digite o nome do protetor de tela.

Para obter mais informações, consulte Como criar uma configuração.

Configuração Extensões do sistema macOS

A configuração Extensões do sistema permite a instalação de tipos de extensão como Extensões de driver, Extensões de rede e Extensões de segurança de endpoint, sem acesso no nível de kernel.

Aplicável para: macOS 10.15+

Procedure Procedimento

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **extensões** no campo de pesquisa e, em seguida, clique na configuração **Extensões do sistema**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Em **Extensões do sistema permitidas**, **+Adicionar** os **Identificadores de equipe permitidos** e **Extensões do sistema permitidos**.
5. Em **Tipos de extensão do sistema permitidos**, **+Adicionar** os **Identificadores de equipe permitidos** e **Allowed System Types (Tipos de sistema permitidos)**.
6. Selecione a opção **Permitir substituições de usuários**.
7. Clique em **Avançar**.
8. Selecione a opção **Ativar esta configuração**.
9. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizado.
10. Clique em **Concluído**.

No macOS 12, `RemovableSystemExtensions` permite que o aplicativo desative sua extensão do sistema sem a aprovação do administrador durante a desinstalação do aplicativo.

Somente MAM

Ivanti Neurons for MDM permite que você especifique dispositivos iOS e Android como apenas MAM e oferece Gerenciamento de aplicativos móveis (MAM) para esses dispositivos. Uma implementação apenas MAM permite que você distribua e gerencie aplicativos sem precisar gerenciar o próprio aplicativo. A implementação apenas MAM é realizada pelo AppStation, que é o cliente do Ivanti Neurons for MDM para implementações apenas MAM. Para informações sobre como configurar e implementar apenas MAM, consulte o seguinte:

Para dispositivos Android, consulte a documentação do produto do AppStation para Android.

Para dispositivos iOS, consulte a documentação do produto do AppStation para iOS.

Se você já possui uma implementação apenas MAM usando o Go, você pode continuar com a implementação. No entanto, a Ivanti recomenda o uso do AppStation para novas implementações somente MAM.

Configuração do Google Play gerenciado

Os administradores podem definir a configuração de atualização automática que a Google Play Store usa para atualizar apps no dispositivo Android Enterprise.

Para ajustar as configurações de atualização automática:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Google Play gerenciado**.
3. Insira um nome para a configuração.
4. Insira uma descrição.

5. Na seção Definição da configuração, selecione uma opção para atualizar os apps do Google Play.

Configuração	O que fazer
Usuário definido	O usuário do dispositivo pode definir a configuração da janela de atualização automática de aplicativos para definir quando os aplicativos devem ser atualizados. a. No campo **Horário de início**, selecione o horário para atualizar o aplicativo. b. No campo **Duração**, selecione a duração (em horas) de acordo com a qual a atualização deve ser realizada. O intervalo mínimo e máximo é entre 1 hora a 24 horas. Os aplicativos podem ser atualizados a qualquer momento entre a hora de início e a duração selecionada. Por exemplo, se o "Horário de início" estiver definido como 18h e a "Duração" estiver definida para 12h, os aplicativos podem ser atualizados a qualquer momento das 18h às 6h.
Nenhum	A Google Play Store nunca atualiza automaticamente os apps no dispositivo.
Somente Wi-Fi	A Google Play Store atualiza automaticamente os apps no dispositivo, mas usando apenas conexões Wi-Fi, e não celular.
Sempre	A Google Play Store atualiza automaticamente os apps no dispositivo em conexões Wi-Fi ou celular.

6. Clique em **Avançar**.

7. Selecione uma das opções de distribuição a seguir:
    - Todos os dispositivos
    - Nenhum dispositivo (padrão)
    - Personalizar
8. Clique em **Concluído**.

Configurações da impressora

O Ivanti Neurons for MDM permite que você crie perfis de impressora e os adicione a dispositivos. Este recurso exige o Bridge. Consulte Bridge para detalhes.

Quando o perfil da impressora é enviado ao dispositivo, a impressora deverá estar ativa, caso contrário, o dispositivo não poderá encontrá-la.

Para definir as Configurações da impressora para um dispositivo Windows:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Configurações da impressora**.
3. Insira um nome para a configuração.

4. Selecione a opção **Windows**.

5. Na seção **Configuração**, configure as definições a seguir:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Configurações da impressora Windows	
Impressora compartilhada	Se a opção **Impressora compartilhada** for selecionada, a impressora será compartilhada com outros dispositivos. Configure os seguintes campos: **Nome**: insira o nome da configuração da impressora. **Descrição**: insira uma descrição da impressora. **Servidor de impressão**: insira o endereço IP do servidor da impressora. **Nome da impressora compartilhada**: insira o nome da impressora.
Impressora conectada à rede	Quando a opção **Conectado à rede** é selecionada, a impressora pode ser acessada apenas por dispositivos dentro da rede conectada. Configure os seguintes campos: **Nome**: insira o nome da configuração da impressora **Descrição**: insira uma descrição da impressora.

Configuração	O que fazer
	Nome da impressora: insira o nome da impressora na rede. **Endereço de host da impressora**: insira o endereço IP do host da impressora. **Número de porta da impressora**: selecione o número de porta da impressora de rede. **Nome do driver da impressora**: insira o nome do driver da impressora. **URL do driver da impressora**: insira o URL do driver da impressora.

6. Clique em **Avançar**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
8. Clique em **Concluído**.

Para definir as Configurações da impressora para um dispositivo macOS:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Configurações da impressora**.
3. Insira um nome para a configuração.
4. Selecione a opção **macOS**.

5. Na seção **Criar configuração de impressora**, configure as definições a seguir:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Definição da configuração	Atualize os campos a seguir para configurar a impressora para dispositivos macOS: • Permitir impressoras locais • Nome de exibição da impressora padrão • Nome da fonte do rodapé • Tamanho da fonte do rodapé • Lista de impressoras do usuário • + Adicionar impressora

6. Clique em **Avançar**
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
8. Clique em **Concluído**.

Configuração remover bloatware

A configuração Remover Bloatware permite selecionar a lista de aplicativos instalados em dispositivos que precisam ser removidos à força. Uma configuração Bridge é um pré-requisito para essa configuração. Consulte Bridge para mais detalhes.

Para executar ou desinstalar apps:

1. Na aba **Configuração**, clique em **+Adicionar**.
2. Selecione a configuração **Remover bloatware**. A página de configuração **Remover bloatware** é exibida.
3. No campo **Nome**, digite um nome apropriado para a configuração.
4. Clique no link +**Adicionar descrição** para adicionar uma descrição para a configuração. Este campo é opcional.
5. Na seção **Definição de configuração**, selecione os apps que devem ser removidos ou desinstalados. Você também pode pesquisar por um aplicativo no campo Pesquisar usando o nome do aplicativo exibido na lista Aplicativos da área de trabalho.

Antes de criar a configuração **Remover Bloatware**, você deve buscar aplicativos acessando **Apps > Apps do desktop > Buscar Apps**. Caso contrário, nenhum aplicativo estará disponível para pesquisa ou escolha ao criar a configuração **Remover Bloatware**.

É possível remover os tipos de arquivo .appx,.appxbundles,.xap e .msi, mas não o tipo de arquivo .exe.

6. Nas opções Avançadas, configure as seguintes opções:

Opção	Descrição
Execute esta configuração a cada	Defina a duração do intervalo (em minutos) após o qual a configuração deve ser executada.
Execute no login	Selecione a caixa de seleção para executar a configuração no login.
Suprima reinício forçado após a desinstalação	Selecione a caixa de seleção para evitar o reinício forçado após a desinstalação do aplicativo.

Configurações de restrições do telefone Samsung

Configurações

As configurações de restrições do telefone Samsung permitem que você defina restrições e exceções de chamada nos dispositivos Samsung. Estas restrições limitam os números de telefone que os usuários podem chamar ou receber ligações.

Aplicável a: Todos os dispositivos Samsung com SDK KNOX 2.0 ou superior.

Para configurar as restrições do telefone Samsung:

1. Na aba **Configuração**, clique em **+Adicionar**.
2. Selecione **Configurações de restrições do telefone Samsung**. A página **Configuração das Restrições do telefone Samsung**é exibida.
3. No campo **Nome**, digite um nome apropriado para a configuração.
4. Clique no link +**Adicionar descrição** para adicionar uma descrição para a configuração. Este campo

é opcional.

5. Na seção **Definição da configuração**, configure as seguintes opções:

Opção	Descrição
Chamadas de entrada	
Números bloqueados	Clique no ícone Adicionar para adicionar números e expressões regulares de Java para definir restrições em chamadas de entrada.
Números permitidos	Clique no ícone Adicionar para adicionar números e expressões regulares de Java para definir os números permitidos dentro de um conjunto maior de números bloqueados para chamadas de entrada. Esta opção não terá nenhum efeito se não houver nenhum número bloqueado.
Chamadas de saída	
Números bloqueados	Clique no ícone Adicionar para adicionar números e expressões regulares de Java para definir restrições em chamadas de saída.
Números permitidos	Clique no ícone Adicionar para adicionar números e expressões regulares de Java para definir os números permitidos dentro de um conjunto maior de números bloqueados para chamadas de saída. Esta opção não terá nenhum efeito se não houver nenhum número bloqueado.

6. Clique em **Concluído** para enviar por push a configuração para os dispositivos selecionados.

> Quando o dispositivo é desativado, todas as restrições de chamada são removidas do dispositivo.

Para obter mais informações, consulte Como criar uma configuração.

Configuração do modo de Single-App

Configurações

Licença: Silver

O modo de aplicativo único restringe os dispositivos com iOS ao uso do aplicativo especificado. Por exemplo, você pode querer configurar dispositivos que possam usar somente um aplicativo personalizado desenvolvido por sua empresa.

Configuração do modo de Single-App

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Escolher aplicativo	Escolha o método a ser usado para selecionar o aplicativo: • **Em Catálogo de Aplicativos e aplicativos do sistema:** selecione para pesquisar o Catálogo de Aplicativos do Ivanti Neurons for MDM e os aplicativos do sistema (pré-instalados nos dispositivos Apple por padrão). • Insira o nome do aplicativo e selecione-o quando ele for exibido na lista de apps. • **Inserir ID do grupo:** selecione para inserir o identificador exclusivo do aplicativo do sistema que você deseja selecionar. Use esta opção se não conseguir localizar o aplicativo do sistema usando a opção **Do App Catalog e dos aplicativos do sistema**.
Desativar toque	Selecione para desabilitar a tela sensível ao toque.
Desabilitar rotação do dispositivo	Selecione para desabilitar o sensor de rotação do dispositivo.
Desabilitar botões de volume	Selecione para desabilitar os botões de volume do dispositivo.
Desabilitar interruptor da campainha	Selecione para desabilitar o interruptor da campainha do dispositivo.
Desabilitar botão suspender/reativar	Selecione para desabilitar o botão suspender/reativar do dispositivo (canto superior direito na borda do dispositivo).
Desabilitar bloqueio automático	Selecione para impedir que o dispositivo vá para o modo de suspensão após o período ocioso.
Ativar narração	Selecione para habilitar o leitor de tela VoiceOver (recurso de acessibilidade).

Ativar zoom	Selecione para habilitar o zoom (recurso de acessibilidade).
Habilitar inversão de cores	Selecione para habilitar o ajuste da inversão de cores (recurso de acessibilidade).
Ativar toque de assistência	Selecione para habilitar o AssistiveTouch (recurso de acessibilidade).
Habilitar seleção da fala	Selecione para habilitar a Seleção da fala (recurso de acessibilidade).
Habilitar áudio mono	Selecione para alternar de áudio estéreo para mono (recurso de acessibilidade).
Ajustes da narração	Selecione para permitir que os usuários do dispositivo façam ajustes no VoiceOver.
Ajustes do zoom	Selecione para permitir que os usuários do dispositivo façam ajustes no Zoom.
Ajustes da inversão de cores	Selecione para permitir que os usuários do dispositivo invertam as cores.
Ajustes do toque de assistência	Selecione para permitir que os usuários façam ajustes no AssistiveTouch.

Para obter mais informações, consulte Como criar uma configuração.

Menu Iniciar e barra de tarefas

Você pode definir o layout do menu Iniciar de seus usuários para determinar aplicativos seguros de usar e remover aplicativos desnecessários. As versões 10 e 11 do Windows oferecem suporte a recursos diferentes, pois os layouts do menu Iniciar são diferentes.

Para definir a configuração do menu Iniciar e da barra de tarefas:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração **Menu Iniciar e Barra de tarefas do Windows**.
3. Insira um nome para a configuração.
4. Selecione a versão específica do Windows.

   Dispositivos Windows 10:

5. Na seção **Configuração**, configure as definições a seguir:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Selecione o dispositivo referencial	Selecione o dispositivo Windows 10 que tenha os apps provisionados no menu Iniciar e na barra de tarefas.

6. Clique em **Obter layout do menu Iniciar do dispositivo** e configure as seguintes opções.

7.

Configuração	O que fazer
Layout do menu Iniciar e da barra de tarefas	Selecione qualquer uma das seguintes opções para ocultar a lista de apps. • **Nenhum** • **Ocultar lista de todos os apps** • **Ocultar lista de todos os apps e desativar "Mostrar lista de apps no menu Iniciar" no aplicativo Configurações** • **Ocultar lista de todos os apps, remover o botão todos os apps e desativar "Mostrar lista de apps no menu Iniciar" no aplicativo Configurações**
Layout do menu Iniciar	
Personalizar menu Iniciar	Clique em **Sim** para personalizar o menu Iniciar e os parâmetros de layout.
Barra de tarefas	
Personalizar barra de tarefas	Clique em **Sim** para personalizar a Barra de tarefas
Remover os atalhos fixados existentes na barra de tarefas antes de adicionar os personalizados	Clique em **Sim** para remover o atalho fixado da barra de tarefas antes de adicionar a barra de tarefas personalizada.
Tipo de aplicativo	Especifica o tipo de aplicativo.
Aplicativo	Especifica o ID do aplicativo.
Restaurar	Clique no link **Restaurar** para restaurar a barra de tarefas a partir da barra de tarefas do dispositivo de referência original.

	Clique e arraste o ícone de seta na linha para mover a posição (para cima ou para baixo) da linha específica. Clique no ícone Excluir para excluir a linha. Clique no botão **Adicionar Novo** para adicionar uma nova linha.

Dispositivos Windows 11

8. Na seção **Configuração**, configure as definições a seguir:

Configuração	O que fazer
Nome	Insira um nome que identifique essa configuração.
Descrição	Insira uma descrição que esclareça o propósito dessa configuração.
Selecione o dispositivo referencial	Selecione o dispositivo Windows 11 que tenha os aplicativos configurados na seção AFIXADOS do menu Iniciar.

9. Clique em **Obter layout do menu Iniciar do dispositivo**.

   Depois de buscar as configurações do dispositivo referencial, todos os aplicativos configurados na seção FIXADOS do menu Iniciar serão exibidos para o administrador revisar.

10. Clique em **Salvar** e distribua a configuração para todos os dispositivos e grupos de usuários aplicáveis.

Devido a um problema do fornecedor, quando a configuração não for distribuída, os aplicativos fixados permanecerão conforme configurados originalmente. No entanto, quando uma nova configuração for distribuída, o layout anterior será substituído e o novo layout será aplicado.

Configuração de atualização do sistema

Os administradores podem limitar os usuários no dispositivo que podem gerenciar atualizações em dispositivos Android 6.0 ou em versões mais recentes com suporte. Esse recurso é aplicável apenas aos dispositivos Android corporativo.

Para configurar:

1. Acesse **Configuração> +Adicionar**.
2. Selecione a configuração **Atualização do sistema**.
3. Insira um nome para a configuração.

4. Insira uma descrição.

5. Na seção Definição da configuração, configure as seguintes opções:

Configuração	Descrição
Automático	Aplique silenciosamente a atualização do sistema sempre que um novo firmware estiver disponível.
Adiar	Adia a instalação das atualizações do sistema por 30 dias. Após o período de 30 dias, o sistema solicita que o usuário do dispositivo instale a atualização.
Em janela (Hora Local)	Agende um período para aplicar silenciosamente a atualização do sistema. Selecione a **Hora de início** e a **Hora de término**.
Período de congelamento	Congela a atualização do sistema por um período específico. Essa opção aplica-se apenas a dispositivos Android 9.0+. Clique em **Adicionar período de congelamento**. Selecione a **Hora de início** e a **Hora de término** para o período de congelamento. O período de congelamento não pode ser de mais de 90 dias, e você pode adicionar vários períodos de congelamento. O próximo período de congelamento pode ser selecionado apenas após 60 dias da data de término anterior. Para excluir um período de congelamento, clique no ícone Excluir.
Configuração do firmware Zebra	Selecione **Configurar Zebra OTA** para fazer o upgrade ou para atualizar o firmware operacional dos dispositivos Zebra (executando no Android 8.0 ou em versões mais recentes com suporte). Isso é aplicável apenas aos modos Propriedade do dispositivo.

Configuração	Descrição
	Para configurar as atualizações do Zebra OTA, você deve ativar o serviço OTA do Ivanti Neurons for MDM em **Administrador > Gerenciamento de firmware > Zebra OTA**, e os dispositivos Zebra devem estar presentes no Ivanti Neurons for MDM. Você deve inserir suas credenciais Zebra no pop-up. Para recriar suas credenciais, entre em contato diretamente com a Zebra. Quando essa opção está selecionada, a lista dos dispositivos Zebra registrados é exibida. Para selecionar e aplicar o firmware para o modelo do dispositivo: a. Na coluna **Ação** do dispositivo Zebra, execute uma das seguintes ações: • **Nenhum**: nenhuma ação será executada para o modelo do dispositivo. • **Atualização completa**. Na janela **Selecionar o firmware de destino Zebra**, selecione a versão completa do firmware a ser aplicada ao modelo do dispositivo. Durante o processo de **Atualização Completa**, somente a porta 443 é necessária. No campo **Localizar**, você pode digitar os caracteres de um ID criado para procurar atualizações com base nesse ID. Os IDs criados são classificados e exibidos em ordem decrescente (mais recente no topo). A opção **Atualização de PatchNÃO** estará disponível para dispositivos Android 11 e superiores.

Configuração	Descrição

Configuração	Descrição
Configuração do Samsung E-FOTA	Selecione **Configurar Samsung E-FOTA** para fazer o upgrade ou atualizar o firmware operacional dos dispositivos Samsung (no Knox versão 2.7.1 e superior). Isso é aplicável apenas ao modo Dispositivo gerenciado com perfil de trabalho em dispositivo de propriedade da empresa. Se não houver dispositivos compatíveis com o Samsung E-FOTA, uma mensagem será exibida na página com essas informações. Para configurar as atualizações do Samsung e-FOTA, você deve ativar a Licença Samsung e-FOTA em **Admin > Gerenciamento de firmware > Samsung E-FOTA**. Quando esta opção é selecionada, a lista de dispositivos Samsung registrados é exibida. Para selecionar e aplicar o firmware para o modelo do dispositivo: a. Na coluna **Ação** do dispositivo Samsung, execute uma das seguintes ações: • **Mais recente**: A versão mais recente do firmware é aplicada. Essa opção está selecionada por padrão. • **Forçar**: na janela Selecionar firmware de destino do Samsung, selecione a versão específica do firmware a ser aplicada de forma forçada (sem intervenção do usuário) ao modelo do dispositivo. Quando essa ação é executada, o download do firmware começa em quinze minutos. • **Destino**: na janela Selecionar o firmware de destino do Samsung, selecione a versão completa do firmware a ser aplicada ao modelo do dispositivo. Ao executar as ações "Forçar" ou "Destino", se não houver firmware listado para o dispositivo, uma mensagem com essas informações será exibida na página.

Configuração	Descrição
	b. **Ativar depuração do FW** (opcional): quando a opção **Ativar depuração do FW** está ativada e a configuração é aplicada, o dispositivo é atualizado em um firmware fictício. O firmware fictício do firmware do dispositivo Samsung permite que o administrador teste o comportamento da configuração de atualização do sistema nos dispositivos, sem modificar nada no dispositivo. Para atualizar para a atualização real do firmware, em vez do firmware fictício, o administrador deve garantir que a opção **Ativar depuração do FW** esteja desativada antes de aplicar a configuração c. Clique em **Aplicar**.

6. Clique em **Avançar**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
8. Clique em **Concluído**.

Configuração Samsung E-FOTA (descomissionado)

A configuração Samsung E-FOTA foi encerrada em julho de 2022. Portanto, tal configuração não estará disponível para novos dispositivos. Os dispositivos com configuração existente poderão apenas desativá-la.

Gerenciamento de atualização do Windows 10

Como administrador, você pode usar o Gerenciamento de Atualizações do Windows 10 para ver e aprovar as atualizações relatadas pelos dispositivos Windows 10 que você deseja atualizar. Ao usar este recurso você pode evitar que atualizações desnecessárias ou não testadas sejam instaladas em dispositivos.

O recurso Gerenciamento de Atualizações requer que os dispositivos sejam configurados com a configuração **Atualizações de software** com a opção **Exigir aprovação de atualização** ativada. É apenas ao aplicar esta configuração aos dispositivos que os dispositivos reportam atualizações para instalação e esperam pela aprovação.

Como gerenciar atualizações

1. Acesse **Administrador > Atualizações do Windows**. Os seguintes detalhes das atualizações são exibidos na página.

   Data de criação: A data em que o certificado foi transferido.
   Título: Descreve o tipo de atualização juntamente com o número do artigo da base de conhecimento.

   > Ao clicar na atualização, a descrição é exibida.

   Classificação: especifica o tipo de atualização. Exemplo: Atualizações de segurança.

   Distribuição: a distribuição realizada para a atualização. Por exemplo, ele exibe **Todos** quando a atualização é distribuída a todos os dispositivos.

   > Se a atualização for distribuída para um número específico de grupos, ela exibirá a contagem da distribuição. Por exemplo, ele exibe 3 se a distribuição for realizada apenas a três grupos.

   Além disso, é possível ver se a atualização foi ou não distribuída aos dispositivos pertinentes. As colunas a seguir possuem números que indicam a quantidade de dispositivos presentes nas diferentes categorias de atualização:

   - Dispositivos elegíveis
   - Dispositivos instalados

- Dispositivos com falha
- Dispositivos pendentes de reinicialização

  Ao clicar em qualquer um desses números, você será direcionado para a visualização filtrada na página Dispositivos para saber o status das atualizações e realizar as ações necessárias.

2. Reveja as atualizações e selecione a atualização que você gostaria de distribuir aos dispositivos clicando na caixa de seleção para a atualização.
3. Em **Ações**, clique em **Definir distribuição**.
4. Na janela **Distribuir atualizações do Windows**, selecione qualquer uma das seguintes opções de distribuição:

   Todos os dispositivos: Distribui as atualizações para todos os dispositivos.

   Nenhum dispositivo: Retém as atualizações a serem distribuídas aos dispositivos
   Personalizado: Distribui as atualizações para os grupos de dispositivos especificados.
5. Clique em **Salvar**.

Como pesquisar e filtrar atualizações

Você pode pesquisar e filtrar atualizações com base nos seguintes critérios:

- ID de artigo da base de conhecimento
- Distribuição configurada

Filtragem com base no ID de artigo da base de conhecimento:

1. Na página **Gerenciamento de Atualizações do Windows 10**, digite o ID da base de conhecimento no campo de pesquisa rápida (somente o número no campo Pesquisar).
   Exemplo: Para KB4056892, digite 4056892. A atualização que corresponde ao critério de pesquisa é exibida na página.

   Você pode procurar mais informações sobre a atualização ao clicar em **Suporte** e no link **Mais informações**. A opção **Suporte** direciona você para a página da Web da Microsoft que fornece informações de suporte do produto em relação à atualização e a opção **Mais informações** o direciona para a página da Web da Microsoft que exibe mais informações sobre a atualização, tal como o artigo da base de conhecimento.

Filtragem com base na distribuição:

Na página **Gerenciamento de atualização do Windows 10**, selecione qualquer uma das seguintes opções de filtro com base na distribuição configurada:

- **Todas**: Exibe todas as atualizações.
- **Configurado**: Exibe a lista de atualizações que são distribuídas a dispositivos.
- **Não configurado**: Exibe a lista de atualizações para as quais a distribuição não está especificada.

> Os filtros Configurado e Não configurado baseiam-se distribuição realizada, e a distribuição também pode ser **Nenhum**.

Como visualizar atualizações de um dispositivo

Para visualizar informações de atualizações detalhadas específicas a um dispositivo:

1. Acesse **Dispositivos > Dispositivos**.
2. Clique no nome de um dispositivo para visualizar a página de detalhes.
3. Acesse a aba **Atualizações**. As atualizações para o dispositivo que estão pendentes (atualização aprovada pelo administrador mas não reportada como instalada no dispositivo), com falha e instaladas são exibidas.

> Você também pode ver notificações sobre novas atualizações do Windows disponíveis na página Notificações, no Painel. A notificação inclui a data de criação da notificação, o número de notificações disponíveis e seu propósito. A notificação de atualização do Windows também é exibida no canto superior direito do portal do administrador.

Programação de aplicativo do Windows

Os apps para desktops Windows podem ser grandes, adicionando carga extra e estendida sobre redes e servidores durante os principais tempos de uso para a empresa. O recurso de programação de aplicativo do Windows permite que você programe um horário para instalar apps, especialmente apps grandes, em dispositivos no período que você escolher.

Para configurar a programação de aplicativo:

1. Acesse **Apps > Catálogo de aplicativos**.
2. Clique em **Adicionar**, selecione um aplicativo do Windows e siga as próximas etapas no assistente **Adicionar Aplicativo**.
3. Na etapa 5 (Configurar), clique em **Instalar definições de configuração de aplicativo** para ver a página **Definição da configuração**.
4. Marque a caixa de seleção **Agendar instalação**.

   A caixa de seleção **Programar instalação** é exibida apenas quando a instalação Silenciosa está ativada.

5. Selecione um **Horário de início** e um **Horário de término** para agendar o horário para instalar aplicativos.
6. Selecione uma **Data de início** e uma **Data de término** para agendar a data de instalação dos aplicativos.

   Você também pode selecionar uma das duas ações a seguir, que devem ser executadas se a data agendada for perdida: **Instalar durante o próximo check-in** ou **Não instalar**.

7. Selecione uma opção de distribuição em Configuração do Aplicativo: **Todos com o aplicativo**, **Ninguém** ou **Personalizado**.

8. Clique em **Concluído**.

> Aplicativos que precisam ser programados não devem ser adicionados ao Apps@Work. A programação de aplicativo não se aplica para apps da Store, já que não há suporte para instalações silenciosas de apps da Store.

Configuração da BIOS do Windows

Os administradores podem definir as configurações da BIOS do Windows em dispositivos Lenovo. Pelo menos um dispositivo Lenovo que suporta as configurações da BIOS deve estar inscrito para definir essa configuração.

Para configurar:

1. Acesse **Configuração> +Adicionar**.
2. Selecione a configuração **BIOS do Windows**.
3. Insira um nome para a configuração.
4. Insira uma descrição.
5. Na seção Escolher modelo do dispositivo, selecione o modelo do dispositivo na lista suspensa.

6. Na seção Definição da configuração, configure as seguintes opções:

> A lista de configurações varia conforme o que está disponível para o modelo específico do dispositivo inscrito.

Configuração	O que fazer
Controle de AMT	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Gerenciamento térmico adaptativo CA	Selecione qualquer uma das opções a seguir: • **Equilibrado** • **Desempenho maximizado**
Gerenciamento térmico adaptativo bateria	Selecione qualquer uma das opções a seguir: • **Equilibrado** • **Desempenho maximizado**
USB sempre ativado	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
BIOSPasswordAtBootDeviceList	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Senha da BIOS na reinicialização	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Senha da BIOS na inicialização autônoma	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Atualização da BIOS por usuários finais	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso por Bluetooth	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Lista de dispositivos de inicialização opção F12	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Dispositivo de exibição de inicialização	Selecione qualquer uma das opções a seguir: • **DisplayPort** • **Monitor acoplado** • **HDMI** • **LCD**
Modo de inicialização	Selecione qualquer uma das opções a seguir: • **Diagnóstico** • **Rápido**
Bloqueio da ordem de inicialização	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
BootTimeExtension	Selecione qualquer uma das opções a seguir: • **1** • **10** • **2** • **3** • **5** • **Desativar**

Violação da tampa inferior detectada	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Gerenciamento de energia da CPU	Selecione qualquer uma das opções a seguir: • **Automático** • **Desativar**
Ativação do módulo Computrace	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Prevenção de execução de dados	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso a Ethernet LAN	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
ROM de opção de Ethernet LAN	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Autenticação de senha por impressão digital	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Autenticação por impressão digital antes da área de trabalho	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso ao leitor de impressão digital	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Prioridade do leitor de impressão digital	Selecione qualquer uma das opções a seguir: • **Externo** • **Interno apenas**
Modo de segurança de impressão digital	Selecione qualquer uma das opções a seguir: • **Alto** • **Normal**
Troca das teclas Fn Ctrl	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

FnKeyAsPrimary	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
FnSticky	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Pilha de rede IPv4	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Pilha de rede IPv6	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso à câmera integrada	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
InternalStorageTamper	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Bipe do teclado	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Configuração de bloqueio da BIOS	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso ao slot de cartão de memória	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso ao microfone	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Comprimento mínimo da senha	Selecione qualquer uma das opções a seguir: • **4** • **5** • **6** • **7** • **8** • **9** • **10** • **11** • **12** • **Desativar**
NFFControl	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso a NFC	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Ligar por conexão CA	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

PasswordBeep	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Erro de contagem de senha excedida	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Presença física para remover TPM	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Presença física para fornecer TPM	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Tecnologia de início rápido	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
SecureBoot	Selecione **Ativar**

Prevenção de retrocesso segura	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Chip de segurança	Selecione qualquer uma das opções a seguir: • **Ativo** • **Desativar** • **Ativar** • **Inativo**
Acesso ao slot de cartão inteligente	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
SpeedStep	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Teclas Option na inicialização	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Recurso TXT	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Memória gráfica total	Selecione qualquer uma das opções a seguir: • **256 MB** • **512 MB**
TouchPad	Selecione qualquer uma das opções a seguir: • **Automático** • **Desativar**
TrackPoint	Selecione qualquer uma das opções a seguir: • **Automático** • **Desativar**
Modo USB30	Selecione qualquer uma das opções a seguir: • **Automático** • **Desativar** • **Ativar**

Suporte da BIOS a USB	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso a porta USB	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Prioridade de inicialização PXE UEFI	Selecione qualquer uma das opções a seguir: • **IPv4 primeiro** • **IPv6 primeiro**
Recurso VTd	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Tecnologia de virtualização	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

Sair de suspensão por LAN	Selecione qualquer uma das opções a seguir: • **CA apenas** • **CA e bateria** • **Desativar** • **Ativar**
Acesso a LAN sem fio	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**
Acesso a WAN sem fio	Selecione qualquer uma das opções a seguir: • **Desativar** • **Ativar**

7. Clique em **Avançar**.
8. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
9. Clique em **Concluído**.

BitLocker do Windows

Como administrador, você pode atualizar em massa a chave de recuperação para um conjunto de dispositivos Windows 10 criptografados, carregando um arquivo Excel com o GUID do dispositivo e a senha de recuperação.

Para carregar o arquivo Excel para a atualização em massa da chave de recuperação:

1. Acesse **Administrador > BitLocker do Windows**.
2. Clique em **Fazer download do arquivo csv de amostra** para fazer download do arquivo CSV de amostra e exibir uma amostra de um arquivo .csv.
3. Crie e adicione os registros para o arquivo .csv das chaves de recuperação do BitLocker.
4. Clique em **Upload das senhas de recuperação**
5. Clique em **Escolher arquivo** para fazer o upload do arquivo .csv criado.
6. Clique em **Upload**. Fazer o upload de um novo arquivo com as chaves carregadas anteriormente substituirá as entradas antigas.

> Um máximo de 1.000 registros pode ser submetido em cada upload. Após um upload bem sucedido, você pode visualizar as chaves individuais nos detalhes do dispositivo específico.

Configuração do quiosque do Windows

A configuração Quiosque do Windows é usada para configurar o quiosque de um ou vários apps nos dispositivos Windows 10. Ao aplicar essa configuração, os usuários do quiosque ficam restritos de acessar recursos fora dos apps de quiosque. É necessário o Windows Bridge para ativar essa configuração.

A seguir são mostrados três modos nos quais a configuração pode ser aplicada.

- Aplicativo Único
- Vários aplicativos (lista de busca de aplicativos do dispositivo do Windows)
- Vários aplicativos (selecione um layout existente na configuração do menu Iniciar)

Os aplicativos usados para uma configuração do quiosque do Windows já devem estar no dispositivo antes da entrada no modo de quiosque do Windows configurado.

Para definir a configuração do Quiosque do Windows:

1. Acesse **Configuração> +Adicionar**.
2. Selecione a configuração **Quiosque do Windows**.
3. Insira um nome para a configuração.
4. Insira uma descrição.

5. Na seção Definições de configuração, especifique as configurações restantes conforme descrito na tabela a seguir.

Configuração	O que fazer
Selecionar modo Quiosque: selecione qualquer uma três das opções a seguir.	
Aplicativo único	Selecione essa opção para configurar o modo de quiosque de aplicativo único para um dispositivo. a. Na seção **Selecionar dispositivo Windows (opcional)**, escolha um dispositivo Windows 10. Clique em **Buscar apps do dispositivo** para buscar a lista de apps de um dispositivo. O dispositivo selecionado deve estar sob sua supervisão e exigir registro para buscar os dados do aplicativo com êxito. Para ignorar essas etapas, selecione **Ignorar esta etapa. Você pode mudar de ideia mais tarde, se** desejar. b. Clique em **Adicionar da lista de apps buscados** para adicionar apps da lista buscada. c. Selecione um aplicativo único ao clicar no botão de seleção na coluna **Nome** do aplicativo. Clique em **Adicionar novo** para adicionar um novo aplicativo à lista. Para excluir um aplicativo da lista, clique no ícone Excluir.

Vários aplicativos (lista de busca de aplicativos do dispositivo Windows)	Selecione essa opção para configurar o modo de quiosque de vários aplicativos para um dispositivo. a. Na seção **Selecionar dispositivo Windows (opcional)**, escolha um dispositivo Windows 10. Clique em **Buscar apps do dispositivo** para buscar a lista de apps de um dispositivo. O dispositivo selecionado precisa estar sob sua supervisão, e será necessário fazer registro para poder buscar dados do aplicativo com êxito. Para ignorar essas etapas, selecione **Ignorar esta etapa. Você pode mudar de ideia mais tarde, se** desejar. b. Em **Layout do menu Iniciar e aplicativos do quiosque**, clique em **Adicionar da lista de apps buscados**. A janela **Selecionar aplicativo do quiosque** é exibida. Selecione os apps da lista buscada e clique em **Usar aplicativo selecionado**.

	c. Na seção Permitir apps adicionais, clique em **Adicionar da lista de apps buscados**. A janela **Selecionar aplicativo do quiosque** é exibida. Selecione os apps da lista buscada e clique em **Usar aplicativo selecionado**. Os aplicativos permitidos adicionais são considerados como dependências para os aplicativos selecionados em **Layout do menu Iniciar e aplicativos do quiosque**. Sem os "aplicativos permitidos", o SO não permite a execução desse aplicativo mesmo quando o ícone do aplicativo for exibido no menu Iniciar. d. Clique em **Adicionar novo** para adicionar um novo aplicativo à lista. Para excluir um aplicativo da lista, clique no ícone Excluir. É possível arrastar e mover um aplicativo na lista para qualquer posição. e. Nas **configurações Outros vários apps**, selecione as opções exigidas: • **Ocultar botão liga/desliga** • **Ocultar o lado a lado do usuário** • **Ocultar barra de tarefas**

Vários aplicativos (selecione um layout existente na configuração do menu Iniciar)	Se você criou uma configuração de layout do menu Iniciar, é possível importar a configuração e usá-la para configurar o modo de vários aplicativos ao selecionar essa opção. a. Na seção **Selecionar layout**, selecione um layout que foi anteriormente definido como uma configuração do menu Iniciar. As configurações anteriormente criadas com os parâmetros de layout aplicáveis são exibidas na lista suspensa abaixo. b. Nas configurações Outros vários apps, selecione as opções exigidas: • **Ocultar botão liga/desliga** • **Ocultar o lado a lado do usuário** • **Ocultar barra de tarefas**

6. Clique em **Avançar**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
8. Clique em **Concluído**.

> Para a configuração ter efeito, o dispositivo deve ser reiniciado após a aplicação ou a atualização de uma configuração do quiosque do Windows. Dependendo dos aplicativos para a configuração de quiosque de vários aplicativos, será necessário reiniciar o dispositivo uma segunda vez. Alguns ícones poderão estar ausentes no primeiro login, mas serão exibidos no login após a segunda reinicialização.

O dispositivo deve ser reiniciado após a aplicação, a exclusão ou a atualização de uma configuração de quiosque. Isso pode ser feito com o comando Reiniciar/Desligar no menu de ações do dispositivo. Sem reinicialização:

- O dispositivo não entra no modo Quiosque automaticamente após a aplicação de uma configuração de quiosque.
- O dispositivo não sai do modo Quiosque automaticamente após a exclusão de uma configuração de quiosque aplicada.
- O dispositivo não altera a configuração Quiosque em execução.

Se um dispositivo com uma configuração de quiosque aplicada receber uma configuração atualizada, o SO do Windows no dispositivo removerá um usuário de quiosque existente e recriará um novo usuário de quiosque com uma nova configuração de quiosque. A sessão para o usuário atual deve ser encerrada explicitamente com a reinicialização do dispositivo.

É preferível configurar com arquivos .lnk para uma configuração de quiosque de vários apps e .exe para uma configuração de quiosque de Single-App. Uma configuração importada do menu Iniciar de um dispositivo usa o formato .lnk. Os itens do menu Iniciar criados manualmente para aplicativos .exe podem não ser exibidos no menu Iniciar da configuração de quiosque de vários apps dependendo do aplicativo .exe.

Por exemplo, o Windows Media Player pode ser adicionado ao menu Iniciar usando um dos seguintes arquivos .lnk:

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

Se esse aplicativo for adicionado diretamente com algum dos arquivos .exe a seguir, um ícone correspondente não será exibido. Até mesmo o primeiro caminho .exe é usado internamente nos arquivos .lnk acima:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

Para a configuração de quiosque de Single-App, é possível adicionar argumentos ao arquivo .exe. E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. Entretanto, o ícone para o aplicativo .exe com argumentos não é exibido no menu Iniciar no caso de uma configuração de vários apps. Se precisar de um aplicativo .exe com argumentos na configuração de quiosque de vários apps, use o arquivo .lnk, que possui argumentos internamente. A extensão .lnk não funciona com uma configuração de quiosque de Single-App.

Dependências no modo de quiosque de vários apps

Os aplicativos Win32/64 podem exigir que dependências sejam adicionadas à seção Apps adicionais permitidos no modo de quiosque de vários apps. 'Apps adicionais permitidos' não são exigidos para um modo de quiosque de Single-App.

Exemplo 1: para o aplicativo Windows Media Player, as seguintes dependências são exigidas no modo de quiosque de vários apps:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

A primeira dependência corresponde aos binários do aplicativo chamados pelo arquivo .lnk correspondente. A segunda é um assistente único chamado pela primeira dependência.

Sem os apps permitidos, o SO não permite a execução desse aplicativo mesmo quando o ícone do aplicativo for exibido no menu Iniciar.

Exemplo 2: no Internet Explorer, o ícone é exibido no menu Iniciar se ele estiver configurado com algum dos itens da lista a seguir:

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- C:\Program Files\internet explorer\iexplore.exe
- %ProgramFiles%\Internet Explorer\iexplore.exe

O Internet Explorer exige as seguintes dependências:

- C:\Program Files (x86)\Internet Explorer\iexplore.exe
- C:\Program Files (x86)\Internet Explorer\ExtExport.exe
- C:\Program Files (x86)\Internet Explorer\ieinstal.exe
- C:\Program Files (x86)\Internet Explorer\ielowutil.exe

A primeira dependência corresponde aos binários do aplicativo exigidos apenas para o item .lnk. As outras dependências correspondem ao assistente único. Sem a primeira dependência, o SO bloqueia o aplicativo com a janela pop-up. Sem as outras dependências, o aplicativo é encerrado logo após a inicialização sem notificações adicionais do SO.

Configuração de licença do Windows

A configuração de Licença do Windows faz o upgrade do sistema operacional no dispositivo, por exemplo, do Windows 10 Pro para Windows 10 Enterprise. Além disso, essa configuração permite ativar ou alterar a chave de produto dos dispositivos desktop do Windows 10.

Para fazer o upgrade de uma licença do Windows:

1. Acesse **Configuração > +Adicionar**.
2. Selecione a configuração de **Licença do Windows**.
3. Insira um nome para a configuração.
4. Na seção **Definição da configuração**, digite a **Chave do produto** do Windows.
5. Clique em **Avançar**.
6. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizar
7. Clique em **Concluído**.

Configuração da cadência de recomendações de atualização de software

Os administradores têm uma opção de permitir que os usuários visualizem e atualizem os dispositivos para a versão de número maior (mais recente) ou de número menor (mais antiga), ou ambas.

Aplicável a: iOS e iPadOS14.5 (supervisionado)

Procedure

1. Acesse **Configurações** > **+Adicionar**.
2. Digite **Recomendação de atualização de software** no campo de pesquisa e clique na configuração **Cadência de recomendações de atualização de software**.
3. Insira um **Nome** e uma **Descrição** para a configuração.
4. Selecione a configuração necessária na lista suspensa:
   - Apresentar ambas as versões de atualização de software
   - Apresentar a versão de atualização de software com numeração inferior (mais antiga)
   - Apresentar apenas a versão de atualização de software com a numeração mais alta (mais recente)
5. Clique em **Avançar**.
6. Selecione a opção **Ativar esta configuração**.
7. Selecione uma das opções de distribuição a seguir:
   - Todos os dispositivos
   - Nenhum dispositivo (padrão)
   - Personalizado.
8. Clique em **Concluído**.

Políticas

As políticas definem requisitos para dispositivos e o que acontecerá se um dispositivo não cumprir os requisitos. Toda política é composta por uma regra e uma ação de conformidade (o que acontece se a regra for violada). Use a página **Políticas** para selecionar, configurar e distribuir as políticas.

Esta seção contém os seguintes tópicos:

Trabalhando com políticas

Esta seção contém os seguintes tópicos:

Implementar políticas

As políticas definem requisitos para dispositivos e o que acontecerá se um dispositivo não cumprir os requisitos. Toda política é composta por uma regra e uma ação de conformidade (o que acontece se a regra for violada). Use a página **Políticas** para selecionar, configurar e distribuir as políticas.

Os seguintes tipos de política estão disponíveis:

Tipo	O que ele faz
Dispositivos comprometidos	Sinaliza os dispositivos que foram desbloqueados (iOS) ou roteados (Android). Para ver o motivo de violação pela qual o sistema sinalizou um dispositivo Android como comprometido devido ao roteamento: 1. Clique na guia **Políticas**
. 2. Clique no link **Dispositivos comprometidos**. 3. Clique na guia **Violações ativas**
. 4. Verifique o motivo de violação na coluna Violação. Para ver o motivo de violação pela qual o sistema sinalizou um dispositivo Android como comprometido devido ao roteamento:

<table>
<tr><th>Tipo</th><th>O que ele faz</th></tr>
<tr><td></td><td>

Clique na guia Políticas
.
Clique no link Dispositivos comprometidos.
Clique na guia Violações ativas
.
Verifique o motivo de violação na coluna Violação. Será uma das seguintes razões:

<table>
<tr><th>Prioridade (1 = maior)</th><th>Violação</th></tr>
<tr><td>1</td><td>Plugin comprometido</td></tr>
<tr><td>2</td><td>Cliente violado</td></tr>
<tr><td>3</td><td>Fabricante do dispositivo desconhecido: desconhecido</td></tr>
<tr><td>4</td><td>Pasta suspeita detectada: [path]</td></tr>
<tr><td>5</td><td>Binário suspeito encontrado em: [path]</td></tr>
<tr><td>6</td><td>Pasta /data é navegável OU Pasta /data/data é navegável</td></tr>
<tr><td>7</td><td>/system/app/Superuser.apk encontrado</td></tr>
<tr><td>8</td><td>Gerenciador de pacotes comprometido</td></tr>
<tr><td>9</td><td>Aplicativo suspeito encontrado: [package]</td></tr>
</table>
</td></tr>
<tr><td>Proteção/criptografia de dados desabilitada (somente macOS)</td><td>Sinaliza dispositivos macOS que não têm senha ou criptografia habilitada.</td></tr>
<tr><td>Roaming internacional</td><td>Sinaliza os dispositivos que podem estar sendo cobrados por roaming internacional. O status é atualizado quando o dispositivo é registrado.</td></tr>
</table>

Tipo	O que ele faz
	Para iOS, o serviço usa a sinalização de roaming como configurada e reportada pelo iOS. A ação de conformidade é provocada somente pela primeira violação.
Administração de dispositivo/MDM desabilitada	Se o dispositivo estiver desativado para MDM, ele não será avaliado para nenhuma outra política ou processamento delta de configurações ou apps de forma adicional durante os registros.
Fora de contato	Sinaliza dispositivos que estavam fora de contato com o Ivanti Neurons for MDM no período especificado. Escolher as ações a serem executadas se o dispositivo não se registrar por um número especificado de horas (2-3 e 23-24) ou dias.
Cliente MI sem contato (apenas iOS)	Sinaliza clientes da Ivanti Neurons for MDM que estavam fora de contato com o Ivanti Neurons for MDM no período especificado. Escolher as ações a serem executadas se o cliente não se registrar por um número especificado de horas (2-3 a 23-24) ou dias. Também vale para dispositivos registrados por meio do iReg. A política marca um dispositivo como fora de conformidade quando não há um cliente ou quando o cliente não efetua registro por um determinado período de tempo.
Aplicativos Permitidos	Sinaliza os dispositivos que violam as regras sobre quais dispositivos são permitidos ou obrigatórios.
Política personalizada	Criar uma política personalizada baseada em condições e ações relacionadas especificadas.

Ações de conformidade

As seguintes ações de conformidade estão disponíveis:

Ação de conformidade	O que ele faz
Monitorar	Sinaliza o dispositivo na página Dispositivos do Ivanti Neurons for MDM. Por padrão, esta opção está ativada.
Bloquear	Instrui o Access e/ou o Sentry a bloquear um dispositivo se este tentar acessar um recurso via Sentry ou Access após a violação da política nos últimos detalhes de check-in.
Enviar mensagem ao usuário	• Sinaliza o dispositivo na página Dispositivos do Ivanti Neurons for MDM. • Envia um e-mail ao proprietário do dispositivo. • Envia uma notificação por push ao dispositivo.
Quarentena	• Remove a maioria das configurações do dispositivo. • Exceções: configurações de senha, configurações Wi-Fi para dispositivos somente com Wi-Fi, configurações de restrição (iOS). • Remove todos os aplicativos instalados pelo Ivanti Neurons for MDM. • Remove todo o conteúdo distribuído pelo Ivanti Neurons for MDM, incluindo arquivos iBook e ePub. • Bloqueia o acesso aos catálogos do Ivanti Neurons for MDM. • Suspende as solicitações para a instalação de apps adicionais. • Bloqueia o acesso aos aplicativos habilitados por AppConnect. • Incluir suporte a aplicativos habilitados para AppConnect. • Se ativada, suspende aplicativos pessoais no lado pessoal do dispositivo em quarentena para indicar que o usuário do dispositivo precisa corrigir os problemas de conformidade no dispositivo para deixá-lo funcional. Compatível com dispositivos Android 11 ou versão posterior provisionados como um perfil de trabalho no dispositivo de propriedade da empresa.

Localizando uma política existente

Você pode usar filtros e o recurso de pesquisa na página Políticas para encontrar uma ou mais políticas existentes.

Procedimento

1. Acesse **Políticas**.
2. Para filtrar uma lista de políticas que correspondem a determinados critérios, clique em **Filtros**.
3. Selecione um ou mais critérios para filtro.
4. Para pesquisar uma política existente pelo nome, insira o nome da política no campo **Pesquisar**.

Adicionando políticas

Procedimento

1. Acesse **Políticas**.
2. Clique em +**Adicionar** (canto superior direito).
3. Selecione um tipo de política.
4. Conclua as configurações.
5. Selecione os grupos de dispositivos que você deseja que recebam essa política.

   Você pode distribuir para no máximo 100 arquivos de configuração ao mesmo tempo.

6. Clique em **Concluído**.

Editando políticas

Procedimento

1. Acesse **Políticas**.
2. Para a política exigida, clique no ícone **Editar** (lápis) na coluna Ações.

3. Faça suas alterações.
4. Salve as alterações.

Excluindo políticas

Procedimento

1. Acesse **Políticas**.
2. Para a política exigida, clique no ícone **Remover** na coluna Ações.
3. Clique em **Sim** para confirmar.

Se você não conseguir visualizar a página Políticas, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Para obter mais informações, consulte Priorizar políticas.

Política personalizada

Políticas

Licença: Platinum

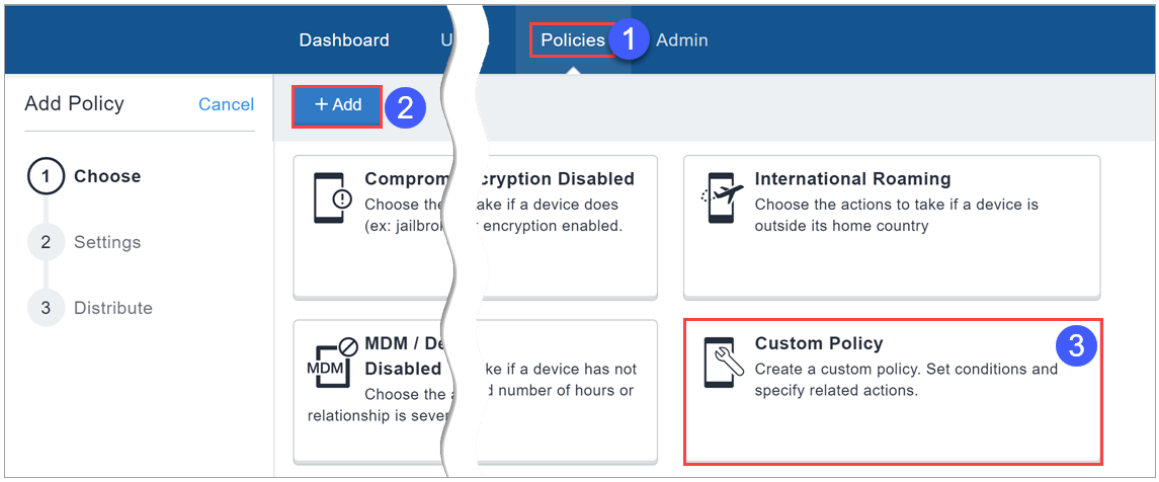
Dispositivos elegíveis: Android, iOS, macOS, Windows.

Permite criar uma política personalizada com base nos atributos de usuário e de dispositivo, critérios de seção, valores e ações de conformidade especificados por você.

A configuração de nível da correção de segurança do Android também pode ser usada ao definir uma política personalizada.

Adicionando uma política personalizada

1. Acesse **Políticas**.



2. Clique em **+ Adicionar**.
3. Selecione **Política personalizada**.
4. Forneça um nome para a política personalizada.
5. Clique em **+ Adicionar descrição** para inserir detalhes adicionais, se desejar.

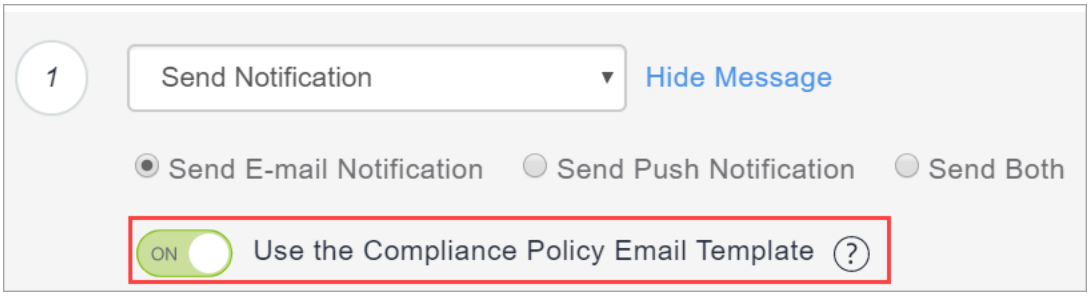
6. Use o Criador de regras para definir as condições que, se verdadeiras, acionam as ações. Consulte Understanding_the_conditions_settings para obter orientações sobre como criar as condições. A partir do Ivanti Neurons for MDM 91, o Administrador do Ivanti Neurons for MDM exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo Nome do Grupo de Usuários é selecionado no construtor de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

7. Selecione uma das ações de conformidade (consulte Ações padrão abaixo) para usar quando as condições especificadas forem atingidas. A adição da ação "**Aguardar**" entre outras ações permite que os usuários do dispositivo corrijam seu dispositivo e o coloquem em conformidade antes da execução de outras ações. Como exemplo, é possível enviar uma mensagem de aviso e aguardar 24 horas antes de aplicar uma ação de quarentena.

8. Selecione a opção **Enviar uma notificação quando o dispositivo voltar a ficar em conformidade** que é desativada por padrão.

   - **Enviar e-mail -** Envia um e-mail ao endereço de e-mail do usuário do dispositivo informando que o dispositivo agora está em conformidade.

     - Ative a opção **Usar o modelo de e-mail da política de conformidade** para inserir a mensagem configurada aqui no modelo de e-mail de notificação de política que você configurar, conforme descrito em "Personalizando um modelo de e-mail" na página 1434 em "Colocar marca em modelos de email" na página 1432. Veja "Configurando e usando e-mails de notificação de conformidade com políticas" na página 27 para ter uma visão geral.



     - É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes sobre as violações da política e outras informações relevantes. Clique nos seguintes tipos de atributo para exibir a lista completa de variáveis:

       - Atributos de política incluindo ${nameOfPolicy}, ${nextAction} e ${nonComplianceTime}.
       - Atributos do usuário incluindo ${sAMAccountName}, ${userCN} e ${userEmailAddressDomain}.
       - Atributos do dispositivo incluindo ${deviceClientDeviceIdentifier}, ${deviceIMEI} e ${deviceModel}.
       - Atributos de usuário/LDAP/dispositivo personalizado criados na página **Administrador > Atributos**.

   - **Enviar notificação por push** - Envia uma notificação por push quando o dispositivo volta a ficar em conformidade.

- **Enviar ambos** - Envia tanto uma notificação por push para o dispositivo e um e-mail ao endereço de e-mail do usuário do dispositivo informando quando o dispositivo voltou a ficar em conformidade. É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes conforme descrito anteriormente para a ação Enviar e-mail.

Ações padrão:

- **Monitorar** – Atualmente, sempre selecionada. O uso de ações de conformidade em camadas requer o Sentry versão 9.0.0 ou mais recente.
- **Não fazer nada**

- **Enviar notificação**
  - **Enviar e-mail -** Envia um e-mail ao endereço de e-mail do usuário do dispositivo informando que o dispositivo não está em conformidade.
    - Você pode usar o modelo de e-mail de notificação de políticas conforme descrito acima.
    - É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes sobre as violações da política e outras informações relevantes. Isso fornece aos usuários de dispositivos que não estão em conformidade informações relevantes sobre a política para que eles possam realizar ações reparatórias. Clique nos seguintes tipos de atributo para exibir a lista completa de variáveis:
      - Atributos de política incluindo ${nameOfPolicy}, ${nextAction} e ${nonComplianceTime}.
      - Atributos do usuário incluindo ${sAMAccountName}, ${userCN} e ${userEmailAddressDomain}.
      - Atributos do dispositivo incluindo ${deviceClientDeviceIdentifier}, ${deviceIMEI} e ${deviceModel}.
      - Atributos de usuário/LDAP/dispositivo personalizado criados na página **Administrador > Atributos**.
  - **Enviar uma Notificação por push** - Envia uma notificação por push ao dispositivo de que o dispositivo não está em conformidade.
  - **Enviar ambos** - Seleciona ambos para enviar uma notificação por push ao dispositivo e um e-mail ao endereço de e-mail do usuário do dispositivo informando que o dispositivo não está em conformidade. É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes conforme descrito anteriormente para a ação Enviar e-mail.
- **Bloquear** - Usa o Sentry para bloquear o acesso dos dispositivos gerenciados aos aplicativos de e-mail e com suporte para AppConnect. O uso da ação de bloqueio requer a versão 9.0.0 ou posterior do Sentry.

- **Desativar** - Desativa o dispositivo. **Essa ação não poderá ser desfeita**. Por exemplo, pode haver uma regra para desativar os dispositivos de todos os usuários desativados usando a condição Usuário ativado.
- **Aguardar** - Atrasa a ação por um período especificado (horas ou dias) para permitir que os usuários corrijam a violação antes de qualquer ação adicional ser executada se o dispositivo continuar em um estado de não conformidade.

- **Quarentena** - Remove o acesso aos apps, conteúdo e servidores de acordo com as seguintes ações:

(Opcional) Ações adicionais de quarentena	Descrição
Colocar em quarentena aplicativos gerenciados	Remove os aplicativos gerenciados pelo Ivanti Neurons for MDM do dispositivo e ativa a opção Bloquear downloads de novos aplicativos para bloquear a reinstalação desses aplicativos no dispositivo. Selecione uma das opções a seguir: • **Todos os aplicativos** • **Aplicativos designados** – Adicionam um ou mais aplicativos por consulta ou manualmente (usando o Nome do pacote ou o ID do pacote). Clique na guia **Visualizar apps** para revisar a lista de apps adicionados. A ação de quarentena padrão Bloquear acesso à App Store não está mais disponível. Em alguns dispositivos, a ação Colocar em quarentena não remove o aplicativo devido a determinadas limitações do dispositivo.
Bloquear downloads de novos aplicativos	Evita o download de quaisquer apps novos no dispositivo. Selecione uma das opções a seguir: • **Todos os aplicativos**

	• **Aplicativos designados** – Adicionam um ou mais aplicativos por consulta ou manualmente (usando o Nome do pacote ou o ID do pacote). Clique na guia **Visualizar apps** para revisar a lista de apps adicionados. A ação de quarentena padrão Bloquear acesso à App Store não está mais disponível. Essa opção é selecionada por padrão (tanto para Todos os aplicativos quanto Aplicativos designados) e não pode ser desmarcada. Isso impede que os aplicativos sejam instalados novamente no dispositivo.
Remover configurações	Remove as configurações do Ivanti Neurons for MDM do dispositivo. Selecione uma das opções a seguir: • **Todas as configurações** • **Configurações designadas** – Selecione uma ou mais configurações da lista ou pesquise-as. Clique na guia **Configurações selecionadas** para revisar a lista de configurações selecionadas.
Enviar configurações designadas	Distribui configurações designadas como parte de uma conformidade personalizada. Essa lista contém configurações de acordo com os seguintes critérios: • Configuração habilitada • Configuração fora do sistema • Configuração em quarentena

	• Configurações criadas no espaço atual ou delegadas no espaço padrão Para obter a lista de configurações que não podem ser colocadas em quarentena, consulte Configurações não compatíveis com quarentena. Para obter mais informações, consulte a seção "Enviando por push uma configuração designada " na página seguinte após esse procedimento.
Remover conteúdo	Remove do dispositivo todo o conteúdo e mídia associados aos aplicativos distribuídos pelo Ivanti Neurons for MDM.
Suspender aplicativos pessoais	Suspende aplicativos no lado pessoal do dispositivo em quarentena para indicar que o usuário do dispositivo precisa corrigir os problemas de conformidade no dispositivo para deixá-lo funcional. Compatível com dispositivos Android 11 ou versão posterior provisionados como um perfil de trabalho no dispositivo de propriedade da empresa.
Ações padrão de quarentena – Essas ações sempre são executadas.	
Bloquear acesso à App Store	Impede que o dispositivo acesse lojas de aplicativos por meio do Ivanti Neurons for MDM.
Bloquear acesso à loja de conteúdo	Impede que o dispositivo acesse a loja de conteúdo por meio do Ivanti Neurons for MDM.
Bloquear AppConnect	Bloqueia o uso dos recursos do AppConnect pelo dispositivo.
Bloquear AppTunnel	Bloqueia o acesso dos aplicativos do dispositivo a conteúdos e servidores via AppTunnel.
Bloquear ActiveSync	Bloqueia o acesso do dispositivo ao e-mail via servidor do ActiveSync.

1. Clique na caixa de seleção **Sim** para confirmar que você entendeu que, se essa política já foi acionada previamente em um dispositivo, a adição da política em camadas redefinirá a política e quaisquer ações de conformidade que tiverem sido aplicadas anteriormente. A nova política personalizada entra em vigência mediante o registro do próximo dispositivo. Se você tiver selecionado a ação Desativar, clique em **Sim** para confirmar que você entendeu que essa ação não poderá ser desfeita.
2. Clique em **Avançar** para configurar a quais dispositivos a política e as ações serão aplicadas.
3. Clique em **Concluído** .

A tabela a seguir ilustra o comportamento de quarentena em vários dispositivos Android quando Ivanti Neurons for MDM é o iniciador da ação de quarentena:

Dispositivos	**Comportamento de quarentena**
Dispositivos da Samsung no modo Administrador de dispositivos por meio do aplicativo Go client	• Desinstalar apps internos e públicos gerenciados • Remover determinados perfis (exceto Defesa contra Ameaças Móveis e outros)
Dispositivos que não são da Samsung no modo Administrador de dispositivos por meio do aplicativo Go client MAM por meio do aplicativo AppStation	• Não suporta que apps internos e públicos gerenciados sejam desinstalados ou ocultados • Remover determinados perfis (exceto Defesa contra Ameaças Móveis e outros)
Android Enterprise por meio do aplicativo Go client	• Ocultar apps internos e públicos gerenciados • Remover determinados perfis (exceto Defesa contra Ameaças Móveis e outros)

Enviando por push uma configuração designada

Distribui configurações designadas como parte de uma conformidade personalizada. Configure a Política personalizada para distribuir um conjunto de configurações quando um dispositivo não está mais em conformidade. Redefina o dispositivo para seu estado anterior como parte da ação de reparo quando um status do dispositivo muda de fora de conformidade para conformidade.

Ocorre um erro quando um administrador tenta delegar uma política personalizada que possui configurações não delegadas na guia Configurações designadas por push.

A seguir, estão os comportamentos quando as configurações são enviadas por push por políticas personalizadas em determinadas condições:

Condições	Comportamento
São selecionadas duas configurações do mesmo tipo que têm prioridade definida	A configuração com a prioridade mais alta será enviada por push para o dispositivo.
São selecionadas duas configurações do mesmo tipo que não têm prioridade definida	Ambas as configurações serão enviadas por push para o dispositivo. Pode resultar em comportamentos inesperados.
Quando o dispositivo já tem uma configuração do mesmo tipo que suporta a prioridade definida na política personalizada	A configuração definida na Política personalizada terá precedência e será enviada por push para o dispositivo. Aquela que está no dispositivo será removida independentemente da prioridade (mesmo se sua prioridade for superior àquela definida na política personalizada).
Quando o dispositivo já tem uma configuração do mesmo tipo que não suporta a prioridade definida na Política personalizada	A configuração definida na Política personalizada será enviada por push para o dispositivo. Ambas as configurações estarão presentes no dispositivo. Pode resultar em comportamentos inesperados.
Se a prioridade de uma configuração for alterada após a criação da política personalizada	No check-in do dispositivo, a configuração com a prioridade mais alta será enviada por push se fizer parte da política personalizada.
Quando ambas as condições forem satisfeitas: • Condição A: quando um dispositivo com uma violação teve uma configuração enviada por push como parte de uma política personalizada (e esta teve prioridade sobre uma configuração do mesmo tipo já existente no dispositivo). • Condição B: a violação foi remediada, e o dispositivo não está mais em quarentena	A configuração definida na política personalizada será removida e a do mesmo tipo no dispositivo antes da quarentena será enviada por push através do aplicativo de grupos de dispositivos existentes, revertendo o dispositivo de volta ao seu estado original.

Na ação Quarentena, se você selecionar Remover configurações juntamente com configurações designadas de push, observe as seguintes regras:

- Remover todas as configurações + Configurações designadas por push: nesse cenário, todas as configurações do dispositivo seriam removidas e as configurações selecionadas em Configurações designadas por push seriam enviadas por push ao dispositivo.
- Remover configurações designadas (em uma política personalizada) + Enviar Configurações Designadas (em outra política personalizada) com configurações comuns na seleção de ambas: como as configurações estão selecionadas em duas políticas de conformidade diferentes, a abordagem mais restritiva seria adotada, ou seja, as configurações serão removidas do dispositivo.

Você pode delegar uma política personalizada do espaço padrão para um espaço personalizado. Para a política personalizada ser delegada, as configurações mencionadas na política personalizada na guia Push Designated Configurations precisam ser delegadas aos espaços.

Na página Dispositivos, você pode clicar no nome do dispositivo para ir para a página de detalhes do dispositivo. Na guia Configurações, a coluna Método de distribuição indica o método de distribuição para a configuração enviada por push para o dispositivo. Pode ser "Grupo de dispositivo" ou "Ação em conformidade".

Na página Configurações, para cada configuração, o Ivanti Neurons for MDM exibe uma contagem de dispositivos que recebe a configuração por meio de um grupo de dispositivos e ação de conformidade.

Compreensão das configurações de condições

A tabela a seguir descreve alguns campos disponíveis para criar regras:

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Capacidade APNS	Esse campo indica se o dispositivo é compatível com APNS.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android
Token de inicialização disponível	Esse campo indica se há um token de inicialização disponível para um dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	macOS
Último registro do cliente	Este campo indica a hora do último registro do cliente.	Os possíveis operadores são: • é menor que • é maior que Insira o valor numérico do horário do último registro. Selecione uma das opções a seguir para a duração: • horas • dias Exemplo: o último registro do cliente foi há menos de 12 horas.	iOS/macOS/Android

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Cliente registrado	Esse campo indica o status do cliente registrado.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android
Comprometido	Esse campo indica se o dispositivo está enraizado/comprometido.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são: • desbloqueado ou modificado • não comprometido	iOS/Android
Nome do País Atual	Esse campo indica o nome do país atual que corresponde ao Código móvel do país (MCC) ou Código móvel da rede (MNC) que o dispositivo reporta para se conectar atualmente.	Os possíveis operadores são: • é igual a • é diferente de O valor possível é um valor em uma lista suspensa que indica o nome do país de origem.	iOS/macOS/Android

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
MCC atual	Este campo indica o código móvel de país atual.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de	iOS/macOS/Android
MNC atual	Este campo indica o código móvel da rede atual.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de	iOS/macOS/Android
Atributo de dispositivo personalizado	Este campo permite adicionar um atributo de dispositivo personalizado existente como uma condição de uma regra para verificar seu valor.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de • contém • não contém O valor pode ser uma string de caracteres ASCII, incluindo Espaço e caracteres Unicode.	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Atributo LDAP personalizado	Este campo permite adicionar um atributo LDAP personalizado existente como uma condição de uma regra para verificar seu valor.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de • contém • não contém O valor pode ser uma string de caracteres ASCII, incluindo Espaço e caracteres Unicode.	iOS/macOS/Android/Windows
Atributo de usuário personalizado	Este campo permite adicionar um atributo de usuário personalizado existente como uma condição de uma regra para verificar seu valor.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de • contém • não contém O valor pode ser uma string de caracteres ASCII, incluindo Espaço e caracteres Unicode.	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Roaming de dados	Este campo permite usar o roaming de dados como a condição de uma regra para verificar seu valor.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não. O valor padrão será Não se o dispositivo compatível não reportar informações sobre esse campo.	iOS/Android
Tipo de dispositivo	Esse campo representa o dispositivo móvel.	Os possíveis operadores são: • é igual a • é diferente de • começa com • termina com O valor possível é um valor de texto.	iOS/macOS/Android/Windows
Criptografia ativada	Esse campo determina se o dispositivo está com a criptografia/proteção de dados ativada.	Sim - O dispositivo está com a criptografia/proteção de dados ativada. Não - O dispositivo não está com a criptografia/proteção de dados ativada.	iOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
GUID	Esse campo indica o GUID do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • começa com • termina com	iOS/macOS/Android/Windows
Nome do País de Origem	Este campo indica o nome do país de origem que corresponde ao Código móvel do país (MCC) ou Código móvel da rede (MNC) que é programado no SIM ou eSIM do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de O valor possível é um valor em uma lista suspensa que indica o nome do país de origem.	iOS/Android/Windows
Atualização do Windows com falha	Esse campo determina se o dispositivo não está em conformidade com as regras de atualização mais recentes.	Sim - Dispositivo não está em conformidade com as atualizações mais recentes. Não - Dispositivo está em conformidade com as atualizações mais recentes.	Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
MCC inicial	Este campo indica o Código móvel de país inicial.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de	iOS/macOS/Android
MNC inicial	Este campo indica o Código móvel de rede inicial.	Digite o valor do atributo a ser verificado. Os possíveis operadores são: • é igual a • é diferente de	iOS/macOS/Android
IMEI	Este campo indica o número IMEI do primeiro slot do SIM.	Os possíveis operadores são: • é igual a • é diferente de • começa com • termina com	iOS/Android/Windows
IMEI2	Este campo indica o número IMEI do segundo slot do SIM.	Os possíveis operadores são: • é igual a • é diferente de • começa com • termina com	Android

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
IMSI	Este campo indica o número IMSI do cartão SIM.	Os possíveis operadores são: • é igual a • é diferente de • começa com • termina com	Android/Windows
Último check-in	Este campo permite definir condições relacionadas ao horário do último registro do dispositivo gerenciado por meio do canal MDM.	Os possíveis operadores são: • é menor que • é maior que Insira o valor numérico do horário do último registro. Selecione uma das opções a seguir para a duração: • horas • dias Exemplo: o último registro foi há mais de 12 horas.	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Última ID do Hotfix	Este campo permite que você defina condições relacionadas ao último ID do hotfix.	Os possíveis operadores são: • é igual a • é diferente de • é menor que • é menor que ou igual a • é maior que • é maior que ou igual a • contém • não contém • começa com • não começa com • termina com • não termina com	Windows
Último Hotfix instalado no	Este campo permite que você defina condições relacionadas ao último hotfix que foi instalado.	Os possíveis operadores são: • é menor que • é maior que	Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Serviços do localizador ativados	Esse campo indica se o dispositivo possui um serviço de localizador de dispositivos (como o Find My iPhone) ativado.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS
Fabricante	Este campo permite definir condições relacionadas ao fabricante do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são: • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
Gerenciado por MDM	Esse campo determina se o dispositivo está com o MDM/Administrador do dispositivo ativado.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
SO	Esse campo representa o tipo de SO do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são: • macOS • Android • iOS • Windows	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Versão de desenvolvimento do SO	Este campo representa a versão de desenvolvimento do SO do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • é menor que • é menor que ou igual a • é maior que • é maior que ou igual a • contém • não contém • começa com • não começa com • termina com • não termina com	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Versão do SO	Esse campo representa a versão do SO do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • está no intervalo O valor possível é texto.	iOS/macOS/Android/Windows
Propriedade	Esse campo indica o tipo de propriedade do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são: • propriedade do usuário • não definido • propriedade da empresa	iOS/macOS/Android/Windows
Senha compatível com perfis	Este campo indica se a senha do dispositivo é compatível com perfis.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Hotspot pessoal ativado	Esse campo indica se o recurso Hotspot pessoal está ativado no dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não. A configuração Hotspot pessoal está disponível somente para determinadas operadoras.	iOS
Número de telefone	Este campo indica o número de telefone do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • contém • começa com • termina com	iOS/Android/Windows
Roaming	Esse campo indica o status do roaming do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Sentry bloqueado	Indica se o dispositivo foi bloqueado pelo Sentry.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Status	Este campo indica o status de registro.	Os possíveis operadores são: • é igual a • é diferente de O valor possível padrão é "Ativo". Todos os outros valores possíveis são removidos para limitar o estado do dispositivo para Ativo nas políticas personalizadas, uma vez que a avaliação da política é feita quando o dispositivo faz o registro e apenas os dispositivos Ativos farão o registro e terão suas políticas avaliadas.	iOS/macOS/Android

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Número de série	Esse campo indica o número de série do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • começa com • termina com	iOS/macOS/Android/Windows
Supervisionado	Esse campo indica se o dispositivo está sendo supervisionado.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Versão de compilação suplementar	Este campo representa a versão de compilação suplementar do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • é menor que • é menor que ou igual a • é maior que • é maior que ou igual a • contém • não contém • começa com • não começa com • termina com • não termina com • não em branco • em branco	iOS/macOS

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Extra da versão/SO suplementar	Este campo representa a versão de compilação suplementar do SO do dispositivo.	Os possíveis operadores são: • é igual a • é diferente de • é menor que • é menor que ou igual a • é maior que • é maior que ou igual a • contém • não contém • começa com • não começa com • termina com • não termina com • não em branco • em branco	iOS/macOS

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Usuário ativado	Este campo indica se o usuário está ativado.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android/Windows
Grupo de usuários	Este campo representa o grupo de usuários.	Os possíveis operadores são: • é igual a • é diferente de	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Roaming de voz	Esse campo indica se o roaming de voz está ativado no dispositivo.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não. A configuração de roaming de voz está disponível somente para determinadas operadoras. Desabilitar o roaming de voz também desabilita o roaming de dados. É diferente de será o valor padrão se o dispositivo compatível não reportar informações sobre esse campo.	iOS
Acesso bloqueado	Indica se o dispositivo está bloqueado pelo Access.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android/Windows

Campo UI	Descrição	Valores possíveis	Plataformas compatíveis
Conformidade	Indica se o dispositivo é compatível ou não.	Os possíveis operadores são: • é igual a • é diferente de Os valores possíveis são Em Conformidade e Fora de Conformidade.	iOS/macOS/Android/Windows
Ação de conformidade bloqueada	Indica se o dispositivo está bloqueado ou não.	Os possíveis operadores são: • é igual a • é diferente de Os possíveis valores são Sim e Não.	iOS/macOS/Android/Windows

Configurações não compatíveis com quarentena

A tabela a seguir mostra a lista de configurações não compatíveis com quarentena:

SO	Configurações não compatíveis com quarentena
Android	• Catálogo de aplicativos para Android • Criptografia para Android • Android corporativo • Aplicativo Android Enterprise • Android Zebra • Proteção Anti-phishing • Desafio de trabalho (Work Challenge) do Android

SO	Configurações não compatíveis com quarentena
	• Senha do dispositivo • Download de arquivo • Bloqueio e quiosque: modo administrador de dispositivo Android • Bloqueio e quiosque: Samsung Knox padrão • Somente MAM • Dispositivo gerenciado com Perfil de trabalho/Perfil de trabalho no Dispositivo de propriedade da empresa • Dispositivos gerenciados de trabalho (proprietário do dispositivo) • Restrições do telefone Samsung • Certificação SafetyNet • Perfil de trabalho em dispositivo de propriedade da empresa
iOS e macOS	• Proteção Anti-phishing (iOS) • Notificações do aplicativo (iOS) • Sites AppStation (iOS) • Chave de recuperação do FileVault (macOS) • FileVault 2 (macOS) • Proxy global (iOS) • Layout da tela inicial (iOS) • Controle do aplicativo para iOS • Restrições do iOS

SO	Configurações não compatíveis com quarentena
	• Atualizações de software do iOS (iOS) • Firewall do macOS • Atualizações de software do Mac OS • Somente MAM (iOS) • Privacidade do MI Client (iOS/macOS) • Uso de rede (iOS) • Criação de conta do Office 365 (macOS) • Modo de Single-App (iOS) • Controle de política do sistema (macOS) • Gerenciamento da política do sistema (macOS) • Opções da Regra de política do sistema (macOS) • Servidor de tempo (macOS) • Filtro de conteúdo da Web (iOS)
Windows	• Controle do aplicativo Windows • DDF (Arquivo de definição de dados) de restrições do Windows • Firewall do Windows • Proxy de rede do Windows • Restrições do Windows • Atualização do Windows
Todos	• Active Directory

SO	Configurações não compatíveis com quarentena
	• Serviços do cliente • Gerenciamento de Dispositivo Móvel • Ativação da Defesa contra ameaças móveis • Ações locais da Defesa contra ameaças móveis • Senha • Privacidade • Declaração de privacidade • ServiceConnect • Sincronização

Se você não conseguir visualizar a página Política, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento de dispositivos
- Somente leitura do dispositivo

Monitorar e controlar apps permitidos

Licença: Silver

Para controlar quais aplicativos são instalados nos dispositivos, crie uma política de Aplicativos permitidos. Esta política também oferece suporte aos aplicativos internos MobileIron Packager (MIP) para macOS. A política contém as seguintes informações:

- **Apps permitidos**[1]
- **Apps bloqueados**[2]
- **aplicativos obrigatórios**[3]
- **ações de conformidade**[4]

Se um aplicativo for, ao mesmo tempo, obrigatório e bloqueado, a avaliação dele em relação à lista de obrigatórios terá precedência. Por exemplo, se um aplicativo A1 estiver presente na lista de itens obrigatórios e na lista de bloqueados, então a avaliação da política de apps para esse dispositivo se comportará da seguinte forma:

- O dispositivo estará em conformidade se A1 estiver instalado nele.
- O dispositivo não estará em conformidade se A1 não estiver instalado nele.

Dispositivos suportados

- Android 4.2 ou versões mais recentes com suporte
- iOS 8.0 ou versões mais recentes com suporte
- macOS 10.12 ou versões mais recentes com suporte

---

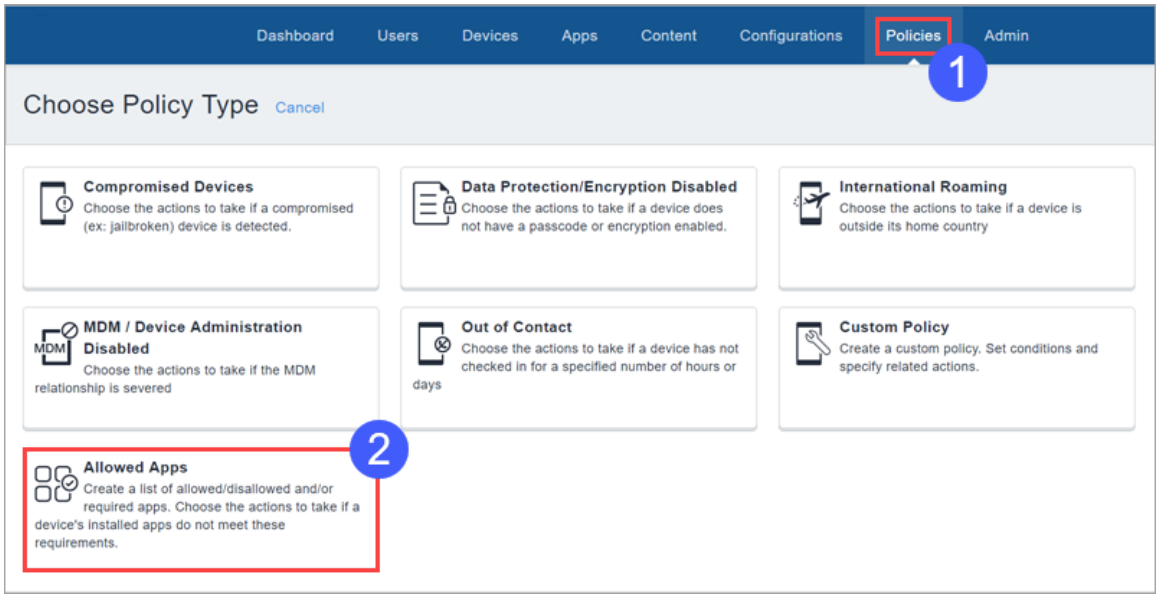
[1]applications that are allowed on a device. A device that has other apps installed is considered out of compliance.
[2]applications that are not approved for installation on a device. A device that has any of these apps installed is considered out of compliance.
[3]applications that must be installed on a device. A device that is missing any of these apps is considered out of compliance.
[4]automated responses to a device that violates rules for managed devices.

Pré-requisitos

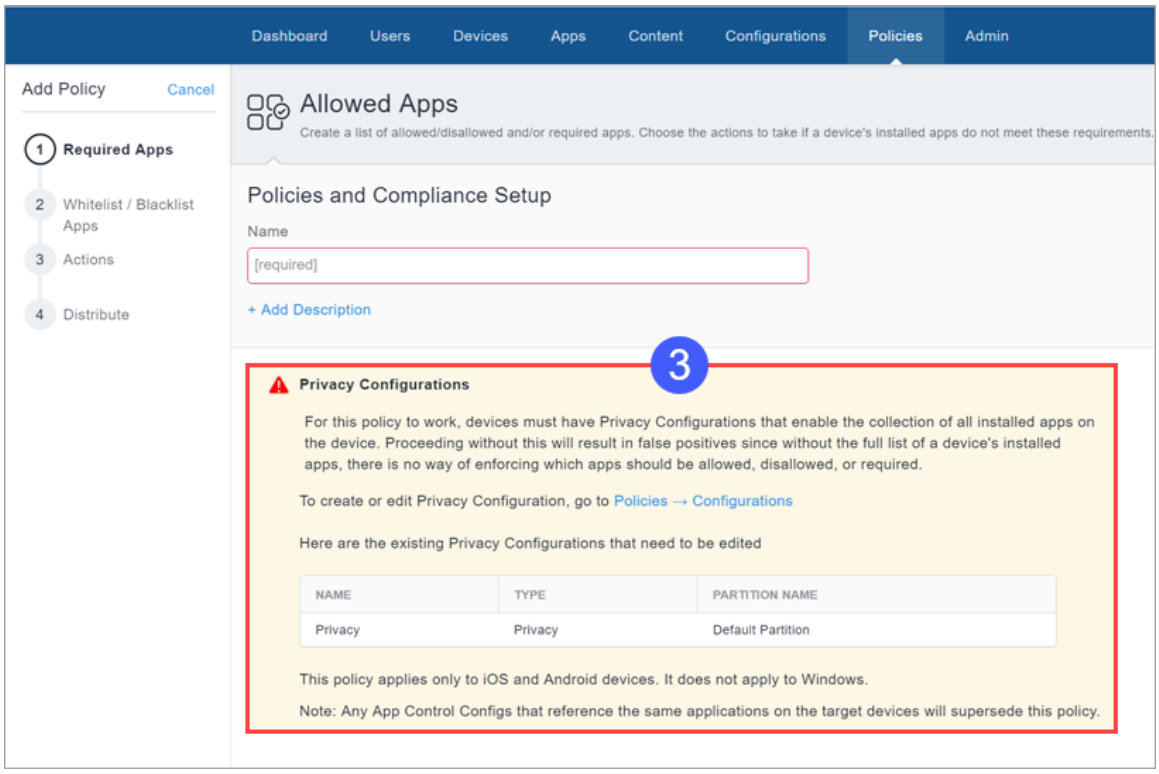
- A configuração de privacidade atribuída ao dispositivo deve permitir a coleta de informações de aplicativo para que a política de aplicativos permitidos funcione corretamente. Verifique as configurações de privacidade atribuídas aos dispositivos aos quais a política de Aplicativos permitidos for aplicada.

Caso não tenha certeza sobre quais configurações são afetadas:

1. Acesse **Políticas**.



2. Clique em **Aplicativos permitidos**.



3. Em **Configurações de privacidade**, observe as configurações que precisam ser editadas.
4. Vá até **Configurações**.
5. Para cada configuração de privacidade observada:
   a. Selecione a configuração.
   b. Clique em **Editar**.
   c. Em **Coletar Inventário de aplicativos**, selecione **Para todos os aplicativos no dispositivo**.
   d. Clique em **Concluído**.

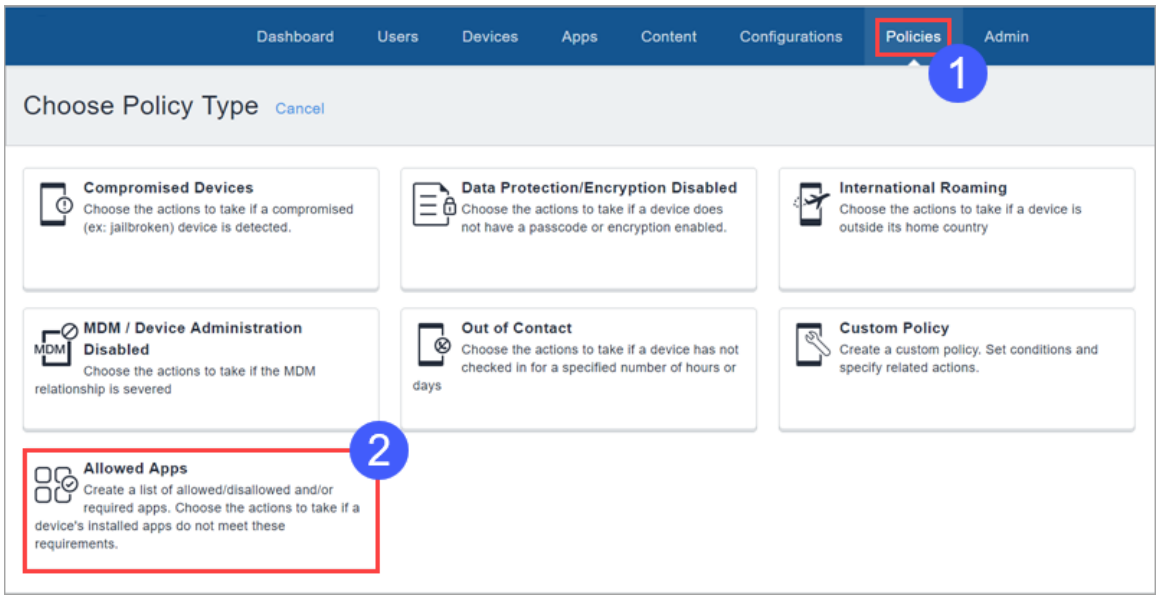
Criando uma política de aplicativos permitidos

Pré-requisitos

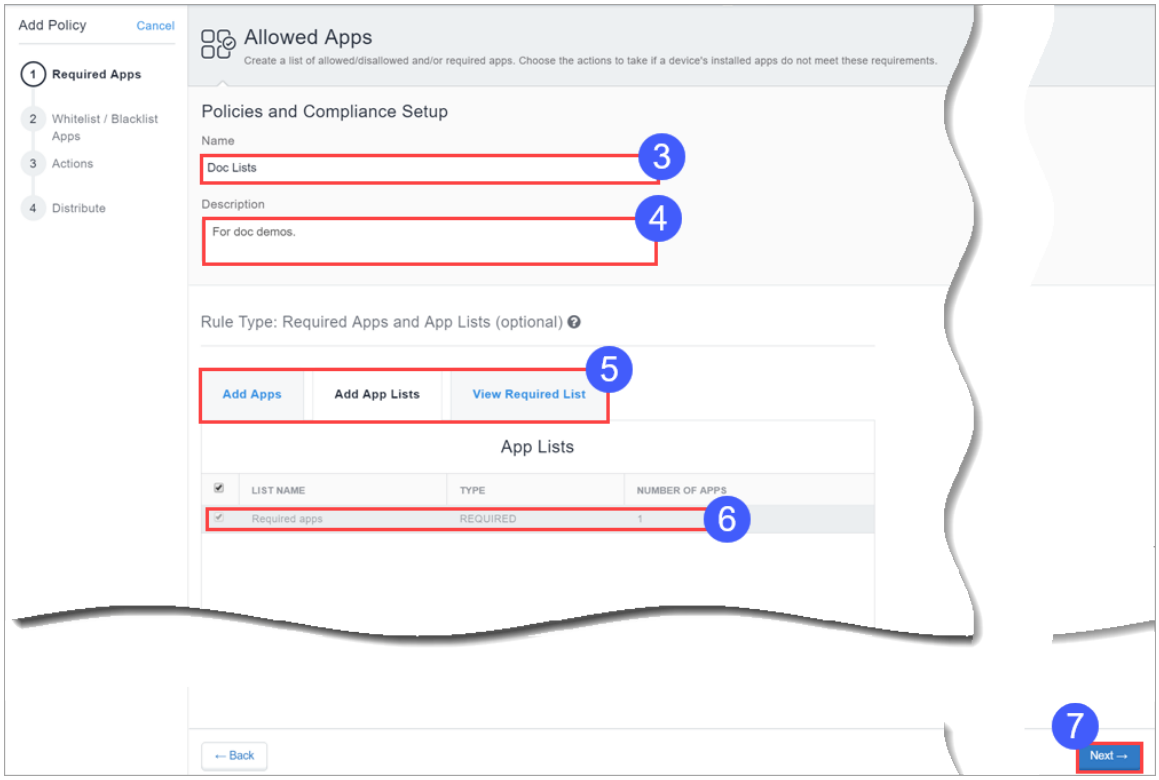
- Ative o Android Enterprise para acessar a Google Play Store e adicionar novos aplicativos à política de apps permitidos.

Procedimento

1. Acesse **Políticas** e clique em **+ Adicionar**.



2. Clique em **Aplicativos permitidos**.

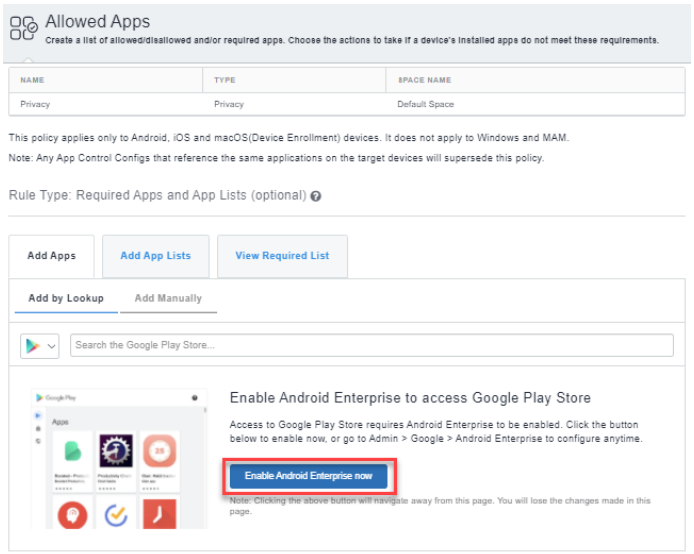


3. No campo **Nome**, digite um nome para esta política.

4. No campo **Descrição**, digite o texto opcional que explica a finalidade da política.

   Escolha os apps para a lista de permitidos ou de bloqueados clicando em uma ou ambas as guias a seguir:

- Clique em Adicionar por pesquisa para pesquisar e selecionar aplicativos da App Store ou do App Catalog.
  Lembre-se de ativar o Android Enterprise para acessar a Google Play Store.

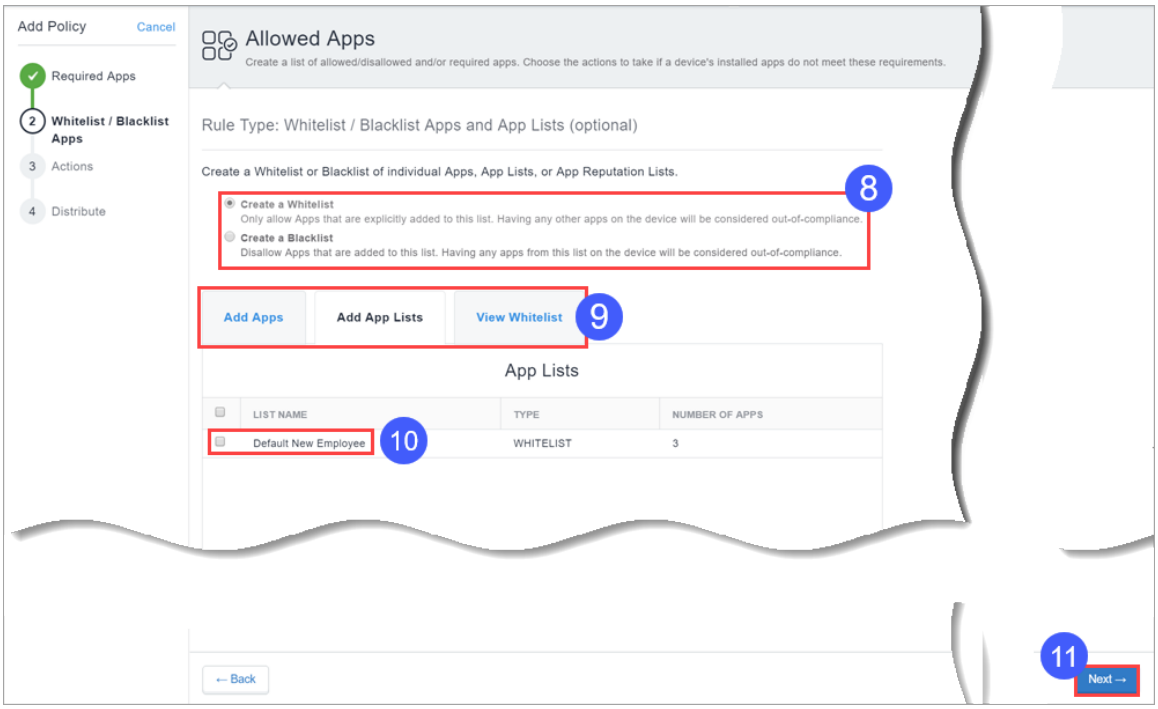


- Clique em **Adicionar manualmente** para escolher apps inserindo o ID do pacote de apps do sistema do Android, do iOS ou do macOS.

5. Selecione a guia **Adicionar listas de aplicativos** e selecione as listas de apps obrigatórios desejadas.
6. Use os campos resultantes para selecionar os aplicativos obrigatórios ou as listas de aplicativos.

> Clique na guia **Exibir lista de obrigatórios** para ver a lista de aplicativos selecionados até o momento.

7. Clique em **Avançar**



8. Selecione se deseja criar uma lista de permitidos ou de bloqueados.

> Não é possível ter uma lista de permitidos e uma lista de bloqueados simultaneamente para um dispositivo. Criar uma lista de permitidos significa que todos os outros apps estão bloqueados.

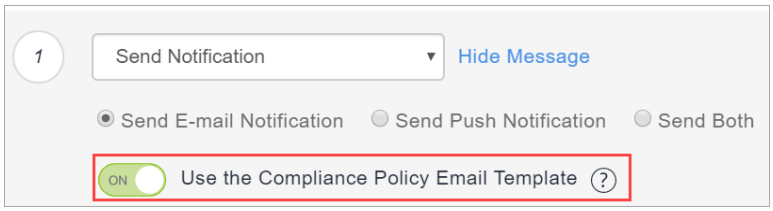
9. Use a seção **Apps permitidos/bloqueados e listas de apps** para selecionar apps e listas de apps.
   - Selecione a guia **Adicionar listas de aplicativos** e selecione as listas de apps desejadas.
10. Use os campos resultantes para selecionar os aplicativos obrigatórios ou as listas de aplicativos.

> Clique na guia **View Allowlist or Blockedlist** para ver uma lista de apps selecionados até o momento.

11. Clique em **Avançar**.
12. Selecione as ações que serão executadas quando um dispositivo não estiver em conformidade:

Ação	O que fazer
Monitorar	No momento sempre selecionada. O uso de ações de conformidade em camadas requer o Sentry versão 9.0.0 ou mais recente.
Não fazer nada	Selecione para não executar nenhuma ação se o dispositivo não estiver em conformidade.
Enviar notificação	

Ação	O que fazer

Enviar e-mail	Selecione para enviar um e-mail ao endereço de e-mail do usuário do dispositivo notificando que o dispositivo não está em conformidade.
	
	• Ative a opção **Usar o modelo de e-mail da política de conformidade** para inserir a mensagem configurada aqui no modelo de e-mail de notificação de política que você configurar, conforme descrito em "Personalizando um modelo de e-mail" na página 1434 em "Colocar marca em modelos de email" na página 1432. Veja "Configurando e usando e-mails de notificação de conformidade com políticas" na página 27 para ter uma visão geral.
	
	 
	
	• É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes sobre as violações da política e outras informações relevantes. Isso fornece aos usuários de dispositivos que não estão em conformidade informações relevantes sobre a política para que eles possam realizar ações reparatórias. Clique nos seguintes tipos de atributo para exibir a lista completa de variáveis:
	
	  • Atributos de política incluindo ${BlockedlistAppsInViolation}, ${requiredAppsInViolation} e ${AllowlistAppsInViolation}.
	
	  • Atributos do usuário incluindo ${sAMAccountName}, ${userCN} e ${userEmailAddressDomain}.
	
	  • Atributos do dispositivo incluindo ${deviceClientDeviceIdentifier}, ${deviceIMEI} e ${deviceModel}.

Enviar uma Notificação por push	Selecione para enviar uma notificação push ao dispositivo que não está em conformidade.

Ação	O que fazer
Enviar ambos	Selecione para enviar uma notificação por push ao dispositivo e um e-mail ao usuário do dispositivo notificando-o de que o dispositivo não está em conformidade. É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes conforme descrito anteriormente para a ação Enviar e-mail.
Aguardar	Selecione para atrasar a ação por um período especificado para permitir que os usuários corrijam a violação antes de qualquer ação adicional ser executada se o dispositivo continuar em um estado de não conformidade.
Bloquear	Usa Sentry para bloquear o acesso dos dispositivos gerenciados ao e-mail aos aplicativos com suporte para AppConnect.
Quarentena	Selecione para remover o acesso a apps, conteúdos e servidores de acordo com as ações na tabela a seguir. A ação de remoção de todos os apps não é permitida.
Enviar uma notificação quando o dispositivo entrar em conformidade	

Ação	O que fazer

Enviar e-mail	Envia um e-mail ao endereço de e-mail do usuário do dispositivo informando que o dispositivo agora está em conformidade.
	• Você pode usar o modelo de e-mail de notificação de políticas conforme descrito acima.
	• É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes sobre as violações da política e outras informações relevantes. Clique nos seguintes tipos de atributo para exibir a lista completa de variáveis:
	  • Atributos de política incluindo ${nameOfPolicy}, ${nextAction} e ${nonComplianceTime}.
	  • Atributos do usuário incluindo ${sAMAccountName}, ${userCN} e ${userEmailAddressDomain}.
	  • Atributos do dispositivo incluindo ${deviceClientDeviceIdentifier}, ${deviceIMEI} e ${deviceModel}.
	  • Atributos de usuário/LDAP/dispositivo personalizado criados na página **Administrador > Atributos**.

Enviar uma Notificação por push	Envia uma notificação por push quando o dispositivo volta a ficar em conformidade.
Enviar ambos	Envia tanto uma notificação por push para o dispositivo e um e-mail ao endereço de e-mail do usuário do dispositivo informando quando o dispositivo voltou a ficar em conformidade. É possível personalizar as mensagens incluindo variáveis opcionais de substituição para fornecer aos destinatários mais detalhes conforme descrito anteriormente para a ação Enviar e-mail.

A política de Apps permitidos oferecerá suporte a ações de conformidade em camadas se você tiver licença Platinum.

(Opcional) Ações adicionais de quarentena	Descrição
Colocar em quarentena aplicativos gerenciados	Remove os aplicativos gerenciados pelo Ivanti Neurons for MDM do dispositivo e ativa a opção Bloquear downloads de novos aplicativos para bloquear a reinstalação desses aplicativos no dispositivo. Selecione uma das opções a seguir: • **Todos os aplicativos** • **Aplicativos designados** – Adicionam um ou mais aplicativos por consulta ou manualmente (usando o Nome do pacote ou o ID do pacote). Clique na guia **Visualizar apps** para revisar a lista de apps adicionados. A ação de quarentena padrão Bloquear acesso à App Store não está mais disponível. Em alguns dispositivos, a ação Colocar em quarentena não remove o aplicativo devido a determinadas limitações do dispositivo.
Bloquear downloads de novos aplicativos	Evita o download de quaisquer apps novos no dispositivo. Selecione uma das opções a seguir: • **Todos os aplicativos** • **Aplicativos designados** – Adicionam um ou mais aplicativos por consulta ou manualmente (usando o Nome do pacote ou o ID do pacote). Clique na guia **Visualizar apps** para revisar a lista de apps adicionados. A ação de quarentena padrão Bloquear acesso à App Store não está mais disponível.
Remover configurações	Remove as configurações do Ivanti Neurons for MDM do dispositivo. Selecione uma das opções a seguir: • **Todas as configurações** • **Configurações designadas** – Selecione uma ou mais configurações da lista ou pesquise-as. Clique na guia **Configurações selecionadas** para revisar a lista de configurações selecionadas.

(Opcional) Ações adicionais de quarentena	Descrição
Remover conteúdo	Remove do dispositivo todo o conteúdo e mídia associados aos aplicativos distribuídos pelo Ivanti Neurons for MDM.
Suspender aplicativos pessoais	Suspende aplicativos no lado pessoal do dispositivo em quarentena para indicar que o usuário do dispositivo precisa corrigir os problemas de conformidade no dispositivo para deixá-lo funcional. Compatível com dispositivos Android 11 ou versão posterior provisionados como um perfil de trabalho no dispositivo de propriedade da empresa.
Ações padrão de quarentena – Essas ações sempre são executadas.	
Bloquear acesso à App Store	Impede que o dispositivo acesse lojas de aplicativos por meio do Ivanti Neurons for MDM.
Bloquear acesso à loja de conteúdo	Impede que o dispositivo acesse a loja de conteúdo por meio do Ivanti Neurons for MDM.
Bloquear AppConnect	Bloqueia o uso dos recursos do AppConnect pelo dispositivo.
Bloquear AppTunnel	Bloqueia o acesso dos aplicativos do dispositivo a conteúdos e servidores via AppTunnel.
Bloquear ActiveSync	Bloqueia o acesso do dispositivo ao e-mail via servidor do ActiveSync.

13. Clique em **Avançar**.
14. Configure a distribuição.
15. Clique em **Concluído**.

Para mais informações sobre definir políticas mais altas ou baixas a uma política de Apps permitidos, consulte Priorizar políticas.

Priorização de políticas

A política de Aplicativos permitidos permite a definição de uma prioridade, de forma semelhante às Configurações. Uma prioridade é usada para determinar qual política do mesmo tipo é distribuída para múltiplos grupos de dispositivos, e o caso em que o mesmo dispositivo aparece nesses múltiplos grupos de dispositivos. Por exemplo, a prioridade de políticas é útil para determinar a distribuição da política quando:

- O "Aplicativo necessário A" precisa ser distribuído para o Grupo de dispositivos 1;
- O "Aplicativo necessário B" precisa ser distribuído para o Grupo de dispositivos 2; e
- O dispositivo do usuário é membro de ambos os grupos de dispositivos.

É possível priorizar políticas da seguinte forma:

1. Acesse **Políticas > Política e conformidade**.
2. Selecione **Ações > Priorizar políticas**. Se **Ações** não for exibido, você não tem várias políticas que exigem prioridades.
3. Use as setas para listar as prioridades das mais altas (parte superior) até as mais baixas (parte inferior). Um ícone de trava significa que a prioridade da política não pode ser alterada sem editar a definição de distribuição Todos os dispositivos na política.
4. Clique em **Salvar**.

Política de Hardware do Windows

Manter a verificação regular do inventário de hardware determinará se um item de hardware é adicionado, copiado, removido, substituído ou movido em um dispositivo Windows 10. Usando a política de Hardware do Windows, é possível selecionar os tipos de hardware para monitorar e as ações a serem executadas quando forem detectadas alterações em um dispositivo.

1. Acesse **Políticas**.
2. Clique em **+Adicionar**.
3. Selecione **Hardware do Windows**.
4. Forneça um nome para a política de hardware.
5. Clique em **+ Adicionar descrição** para inserir detalhes adicionais, se desejar.
6. Na seção **Definir regras de hardware**, configure as seguintes opções:

Opção	Descrição
Objeto de hardware	Selecione o tipo de hardware entre as seguintes opções: • **BIOS** • **Unidade de hardware** • **Unidade de CD-ROM** • **Processador** • **Memória física**
Evento de alteração	Selecione o tipo de evento de hardware que deve ser verificado: • **Adicionar** • **Copiar** • **Remover** • **Substituir**

	• **Mover**

Escolher ações	Selecione o tipo de ação a ser executada:
	• **Não fazer nada**
	• **Enviar notificação**: selecione uma das opções a seguir:
	  • **Enviar notificação de e-mail** – Insira o assunto e o corpo na seção da **mensagem de e-mail** para enviar a notificação.
	  • **Enviar notificação por push** – Insira a mensagem da notificação por push.
	  • **Enviar ambas** – Insira a mensagem de e-mail e a da notificação por push.
	• **Aguardar**: na lista suspensa, selecione o número de dias/horas a aguardar.
	  • **1** a **31** para **dias**.
	  • **1** a **24** para **horas**.

7. Clique em **Avançar**.
8. Selecione uma das opções de distribuição a seguir:
    - **Todos os dispositivos**
    - **Nenhum dispositivo (padrão)**
    - **Personalizada**
9. Clique em **Concluído**.

Administrador

A seção Admin ajuda a gerenciar usuários, dispositivos e configurações do portal Ivanti Neurons for MDM. As seções a seguir contêm a lista de todas as tarefas que você pode executar como administrador:

Sistema

Esta seção contém os seguintes tópicos:

Atributos

Use a página Atributos para realizar as seguintes tarefas:

- Gerenciar os tipos de informação que podem ser registrados para usuários, dispositivos e aplicativos
- Visualizar os tipos predefinidos de informação que o Ivanti Neurons for MDM monitora.

Os atributos de usuário personalizados incluem informações tais como Departamento ou um ID interno. Cada atributo tem uma variável correspondente que você pode usar para criar grupos ou distribuir configurações.

Ao criar critérios de grupo para regras de usuários, se os atributos personalizados tiverem valor numérico, o Ivanti Neurons for MDM não aceitará operações com inteiros.

Criação de atributos personalizados

Procedimento

1. Faça login no Portal Administrativo.
2. Navegue até **Administrador** > **Sistema** > **Atributos**.
3. Em **Atributos personalizados**, clique em **+Adicionar**
4. No campo **Nome do atributo**, insira o texto que representará o atributo.

   O texto que você inserir será usado para criar a variável correspondente no campo **Uso**.

5. Selecione qualquer tipo de atributo dentre as seguintes opções de **Tipo de atributo**.
   - **Usuário**
   - **Dispositivo**
   - **Aplicativo**

6. Se o tipo de atributo for Dispositivo, selecione uma das seguintes opções de **Tipo de dados**:
   - **Numérico**
   - **Texto**
7. Clique em **Adicionar**.

   O atributo de usuário personalizado que foi criado é exibido na seção **Adicionado pelo administrador** na página Atributos.

A combinação de atributos personalizados ${deviceattribute} + ${custom-attribute} + ${userattribute} + ${Static String} é compatível em qualquer ordem.

Renomeação de um atributo personalizado

Se um atributo personalizado for renomeado, serão renomeadas todas as referências a esse atributo que são usadas nas seguintes entidades:

- Política personalizada
- Grupo de usuários
- Grupo de dispositivos
- Filtro de distribuição de aplicativo
- Espaços

Referências ao atributo personalizado em quaisquer outras entidades, como configurações, modelos de e-mail de convite, e-mail ou mensagens push em ações de conformidade com políticas e assim por diante não serão atualizadas.

Procedimento

1. Em **Adicionado pelo administrador**, clique em **+Editar** ao lado do atributo que deseja renomear.
2. No campo **Nome do atributo**, digite um novo nome para representar o atributo.

   O texto que você inserir será usado para criar a variável correspondente no campo **Uso**.
3. Clique em **Salvar**.

Exclusão de um atributo personalizado

Excluir um atributo personalizado removerá os valores dele de todos os usuários ou dispositivos associados. Não é possível reverter.

Não será possível excluir um atributo personalizado caso ele seja usado em alguma das seguintes entidades:

- Política personalizada
- Grupo de usuários
- Grupo de dispositivos
- Filtro de distribuição de aplicativo
- Espaços

Remova o atributo personalizado das entidades antes de tentar excluir o atributo personalizado.

Se o atributo que deve ser excluído não tiver referências a qualquer uma das entidades acima, quando você clicar em **Excluir** ao lado do atributo, será exibida uma mensagem pop-up para confirmar a ação. Confirme a ação e clique em **Excluir**.

Visualização dos atributos do sistema

Atributos do sistema são atributos pré-definidos que você pode usar em suas configurações como variáveis. A lista completa se encontra na seção **Atributos do sistema** da página **Administrador** > **Sistema** > **Atributos**. Os atributos do sistema incluem os seguintes tipos de atributos:

- Atributos do usuário
- Atributos do dispositivo
- Atributos do modelo de e-mail
- Atributos do Sistema
- Atributos de indicação horária
- Atributos de usuário personalizados do AAD
- Atributos da política

Atributos do usuário

Use os atributos de usuário para especificar informações sobre os usuários.

Chave	Descrição
${department}	atributo departamento (requer Azure Active Directory)
${edipi}	Sem descrição
${managedAppleId}	ID Apple gerenciado do usuário
${sAMAccountName}	atributo sAMAccountName (requer Active Directory)
${userCN}	Atributo Nome Comum (CN) extraído do nome distinto (requer LDAP)
${userDisplayName}	Nome de exibição
${userDN}	Nome Distinto (requer LDAP)
${userEmailAddressDomain}	A parte do domínio do endereço de e-mail (parte após '@')
${userEmailAddressLocalPart}>	A parte local do endereço de e-mail (parte antes de '@')
${userEmailAddress}	Endereço de e-mail
${userFirstName}	Nome
${userLastName}	Sobrenome
${userLocale}	Local
${userOU}	Atributo Unidade Organizacional (OU) extraído do nome distinto (requer LDAP)
${userREALM}	Informações do Realm Kerberos (requer Active Directory)
${userUIDDomain}	A parte do domínio do ID de login (parte após '@')
${userUIDLocalPart}	A parte local do ID de login (parte antes de '@')
${userUID}	ID de login (formato de endereço de e-mail)
${userUPN}	Atributo userPrincipalName (requer Active Directory)

Atributos do dispositivo

Use atributos de dispositivo para especificar informações sobre um dispositivo móvel.

Chave	Descrição
${clientLastCheckin}	Data em que o cliente fez check-in pela última vez (check-in mais recente - MDM ou Cliente)
${deviceAltSN}	Número de série alternativo
${deviceClientDeviceIdentifier}	Identificador usado pelo aplicativo cliente
${deviceGUID}	Identificador de dispositivo globalmente exclusivo
${deviceIccIdentifier}	Sem descrição
${deviceIMEI2}	IMEI2
${deviceIMEI}	IMEI
${deviceIMSI}	IMSI
${deviceLastCheckin}	Data em que o dispositivo fez check-in pela última vez (check-in mais recente - MDM ou Cliente)
${deviceMdmChannelId}	Identificador de dispositivo interno
${deviceMdmDeviceIdentifier}	Identificador usado para MDM
${deviceMEIdentifier}	Sem descrição
${deviceModel}	Modelo
${deviceName}	Nome do dispositivo
${devicePhoneNumber}	Número de telefone do dispositivo
${devicePK}	Identificador de dispositivo exclusivo do cluster
${deviceSN}	Número de série
${deviceUDID}	UDID do iOS
${deviceWifiMacAddress}	Endereço MAC do Wi-Fi

Quando você cria um atributo personalizado e faz referência ele em uma configuração de aplicativo gerenciado, se o valor do atributo for atualizado, o atributo referenciado na configuração também será atualizado, e a configuração do aplicativo gerenciado será reenviada ao dispositivo.

Quando os atributos Personalizado ou Dispositivo são atualizados e a configuração é enviada a um dispositivo, a configuração de identidade visual do quiosque Android também deve ser atualizada.

Atributos de aplicativo

Use atributos de aplicativo para especificar informações sobre aplicativos e criar grupos de aplicativos personalizados.

Chave	Descrição
${appAdded}	Data em que o aplicativo foi adicionado ao AppCatalog
${appName}	Nome do aplicativo
${appOsPlatform}	Sistema operacional do aplicativo
${appPackageId}	Pacote de aplicativo ou ID do pacote
${appSource}	Descreve a origem de onde o aplicativo foi importado
${IsVpp}	Descreve se um aplicativo de iOS ou macOS é VPP ou não

Atributos do modelo de e-mail

Chave	Descrição
${policyMessageContent}	Sem descrição
${policyMessageTitle}	Sem descrição

Atributos de indicação horária

Chave variável	Descrição
${timestampMS}	Carimbo de data/hora atual (milissegundos desde a época)

Atributos do modelo de política

Chave	Descrição
${nameOfPolicy}	Nome de política violado
${nextAction}	Próxima Ação de Conformidade Estratificada (diferente de esperar e desativar) a ser executada após o envio da mensagem
${nonComplianceTime}	Contagem de dias que o dispositivo esteve em estado não conforme
${policyViolationFirstTime}	Carimbo de data/hora de quando a violação da política foi acionada pela primeira vez (formato UTC DD-MM-AAAA)
${ruleConditions}	Definição de regra (string de consulta do jeito que aparece agora)

Tópicos relacionados:

- "Como atribuir atributos personalizados aos usuários" na página 175
- "Como atribuir atributos personalizados aos dispositivos" na página 290
- "Como remover atributos personalizados dos usuários" na página 176
- "Como remover atributos personalizados dos dispositivos" na página 291
- "Variáveis" na página 503

Configurações de Limpeza de Dispositivo

A limpeza de dispositivo automatiza o ciclo de vida dos dispositivos não utilizados. Você pode desativar os dispositivos que estejam fora de contato há um número específico de dias definido por você. Você pode excluir dispositivos que estejam desativados há um número específico de dias definido por você. A página Trilhas de Auditoria captura as configurações de Desativar Dispositivo, Excluir Dispositivo e Excluir Dispositivo Apagado.

- Os dispositivos em modo empresarial Android são excluídos das configurações de limpeza de dispositivo.

Pré-requisitos

Você deve ter permissões de gerenciamento de sistema para acessar esta configuração.

Desativar dispositivo

Procedimento

1. Acesse **Administrador**> **Sistema** > **Limpeza do dispositivo**. A página Limpeza do Dispositivo é exibida.
2. Selecione a guia **Desativar dispositivo**.
3. Use a tabela **Desativar dispositivos** localizada abaixo deste procedimento para especificar os detalhes.
4. Clique em **Mostrar lista de dispositivos que não fizeram check-in**. Mostra a lista dos dispositivos que estão sem fazer check-in há um número específico de dias.
5. Clique em **Desativar dispositivos agora**; como alternativa, você pode agendar a desativação do dispositivo.
6. O portal administrativo do Ivanti Neurons for MDM desativará os dispositivos especificados.
7. Clique em **Salvar** para salvar sua configuração.
8. (Opcional) Se você atualizar os valores, poderá clicar em **Redefinir** para redefinir as configurações de volta ao estado inicial.

Desativar dispositivos

Campo	Descrição
Desativar dispositivos que não fazem check-in há mais de (dias)	Dias: 30 dias é o padrão, 365 dias é o número máximo de dias permitido.
Máximo de dispositivos a serem desativados em cada sessão	Selecione 100, 500 ou 1000 (Padrão - 100).
Desativar automaticamente dispositivos seguindo um agendamento	Marque a caixa de seleção para desativar os dispositivos com base em um agendamento predefinida.
Configuração do agendamento de desativação	Selecione uma das seguintes opções para definir a frequência das desativações: • **Diariamente -** defina para desativar dispositivos todos os dias. • **Semanalmente -** especifique o dia da semana para agendar a desativação. • **Mensalmente -** defina para desativar os dispositivos no primeiro dia de cada mês.

Excluir dispositivos desativados

Procedimento

1. Acesse **Administrador**> **Sistema** > **Limpeza do dispositivo**. A página Limpeza do Dispositivo é exibida.
2. Selecione **Excluir Configurações de Dispositivos Desativados**.
3. Use a tabela **Desativar dispositivos desativados** localizada abaixo deste procedimento para especificar os detalhes.
4. Clique em **Mostrar lista de dispositivos desativados**. Mostra a lista dos dispositivos que estão desativados há um número específico de dias.
5. Clique em **Desativar dispositivos desativados agora**; como alternativa, você pode agendar a exclusão do dispositivo.
6. O portal administrativo do Ivanti Neurons for MDM excluirá os dispositivos especificados.

7. Clique em **Salvar** para salvar sua configuração.
8. (Opcional) Se você atualizar os valores, poderá clicar em **Redefinir** para redefinir as configurações de volta ao estado inicial.

Excluir dispositivos desativados

Campo	Descrição
Excluir dispositivos que estão desativados há mais de (dias)	Dias: 30 dias é o padrão, 365 dias é o número máximo de dias permitido.
Máximo de dispositivos desativados a serem excluídos em cada sessão	Selecione 100, 500 ou 1000 (Padrão - 100)
Excluir automaticamente dispositivos desativados seguindo um agendamento	Marque a caixa de seleção para excluir os dispositivos com base em um agendamento predefinida.
Configuração do agendamento de exclusão	Selecione uma das seguintes opções para definir a frequência da exclusão: • **Diariamente -** defina para excluir dispositivos desativadas todos os dias. • **Semanalmente -** especifique o dia da semana para agendar a exclusão. • **Mensalmente -** defina para excluir os dispositivos desativados no primeiro dia de cada mês.

Excluir dispositivos apagados

Procedimento

1. Acesse **Administrador**> **Sistema** > **Limpeza do dispositivo**. A página Limpeza do Dispositivo é exibida.
2. Selecione **Excluir dispositivo apagado**.
3. Use a tabela **Excluir dispositivos apagados** para especificar os detalhes.
4. Clique em **Mostrar lista de dispositivos apagados**. Mostra a lista dos dispositivos que estão desativados há um número específico de dias.

5. Clique em **Excluir dispositivos apagados agora** ou, como alternativa, agende a exclusão dos dispositivos apagados.
6. O portal administrativo do Ivanti Neurons for MDM excluirá os dispositivos especificados.
7. Clique em **Salvar** para salvar sua configuração.
8. (Opcional) Se você atualizar os valores, poderá clicar em **Redefinir** para redefinir as configurações de volta ao estado inicial.

Excluir dispositivos

Campo	Descrição
Excluir dispositivos que foram apagados há mais de (dias)	Dias: 30 dias é o padrão, 365 dias é o número máximo de dias permitido.
Máximo de dispositivos apagados a serem excluídos em cada sessão	Selecione 100, 500 ou 1000 (Padrão - 100)
Excluir automaticamente dispositivos apagados seguindo um agendamento	Marque a caixa de seleção para excluir os dispositivos com base em um agendamento predefinida.
Configuração do agendamento de exclusão de apagados	Selecione uma das seguintes opções para definir a frequência da exclusão: • **Diariamente -** defina para excluir dispositivos desativadas todos os dias. • **Semanalmente -** especifique o dia da semana para agendar a exclusão. • **Mensalmente -** defina para excluir os dispositivos desativados no primeiro dia de cada mês.

Perfis do GDPR

O portal administrativo Ivanti Neurons for MDM agora contém a página de perfis GDPR que permite atribuir perfis GDPR a grupos de usuários. Você pode atribuir o perfil GDPR apenas a grupos de usuários, e não a usuários individuais.

Observe os seguintes pontos:

- Você deve primeiro habilitar os Perfis GDPR para atribuí-los a um grupo específico de usuários.
- Se você desabilitar o perfil GDPR, desativará todas as restrições de perfil que já foram atribuídas ao grupo de usuários.
- Depois de habilitar o perfil GDPR, a funcionalidade Editar ficará limitada ou desativada em alguns dos campos.

Campos que ficam ocultos após a atribuição do perfil GDPR

Se o usuário tem um perfil GDPR, o Ivanti Neurons for MDM oculta por padrão os campos a seguir ao exibir informações sobre o usuário:

- **ID do usuário**
- **Nome do usuário**
- **Endereço de e-mail**
- **Número de série**
- **ICCID**
- **IMSI**
- **MEID**
- **Endereço IP**
- **Número do telefone**
- **IMEI**
- **Identificador eSIM**

Habilitando o perfil GDPR

Você pode habilitar o perfil GDPR e selecionar campos específicos que devam ser ocultados no portal administrativo do Ivanti Neurons for MDM e nos dispositivos.

ProcedureProcedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá até **Administrador** > **Sistema** > **Perfis GDPR**.
3. Clique em **Habilitar**.

4. Clique no ícone de edição (lápis).
5. Selecione os campos que devem ser ocultados.
6. Clique em **Salvar**. Os campos selecionados serão mascarados e não exibirão os valores dos usuários específicos.

Atribuir perfil GDPR a grupos de usuários

Depois de habilitar o perfil GDPR, você pode atribuí-lo a grupos de usuários específicos.

ProcedureProcedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Usuários** > **Grupos de usuários**.
3. Selecione um grupo de usuários na lista.
4. Clique na lista suspensa **Ações** e selecione **Atribuir perfil GDPR**. O Perfil GDPR será atribuído a todos os usuários desse grupo específico, e todos os valores selecionados terão a visualização mascarada no portal administrativo e nos dispositivos dos usuários.

> Como o administrador também está no grupo Todos os usuários, não atribua perfis GDPR a esse grupo.

E-mails de notificação

Licença: Silver

Você pode configurar a lista de endereços de e-mail dos usuários que devem receber notificações por e-mail com base no nível de gravidade da notificação.

O recurso E-mail de notificação é opcional e você pode ativá-lo ou desativá-lo conforme necessário. É preciso ter a função Gerenciamento de sistema para poder usar esse recurso.

1. Selecione **Administrador > E-mails de notificação**. A página **E-mails de notificação** é exibida.
2. Na seção Configurações de e-mails de notificação, clique em **Ativar** para ativar o recurso de E-mails de notificação.
3. Clique em **Adicionar destinatário**. A janela pop-up **Adicionar destinatário** é exibida.
4. Na janela pop-up **Adicionar destinatário**, atualize os seguintes campos:
    - ID de e-mail do destinatário – Insira o ID de e-mail do destinatário ao qual a notificação deve ser enviada.
    - Tipos de notificação a serem enviados – Selecione o tipo de notificação por meio da caixa de seleção. Estas são as opções de tipo de notificação: **Notificação crítica, Notificações de cuidado, Notificação de informação**.
5. Clique em **OK**. Os detalhes das configurações são exibidos em uma tabela.
6. Clique em **Salvar** para aplicar as alterações.

Gerenciamento de funções

Funções são grupos compilados de permissões que permitem conceder um conjunto de permissões a um usuário administrativo ao mesmo tempo em que limitam seu acesso para controlar áreas específicas da funcionalidade. O Ivanti Neurons for MDM oferece um conjunto de funções do sistema que podem ser atribuídas (ou editadas) e um recurso de criação de funções personalizadas. A partir do Ivanti Neurons for MDM 91, você pode pesquisar uma permissão específica com base na categoria, e todas as opções associadas à função ou permissão específica na interface do usuário são exibidas. Uma dica de ferramenta é exibida para as permissões adicionadas como permissões dependentes.

A página Gerenciamento de Funções e as opções associadas ficam ocultas para os locatários convergentes que têm acesso ao Ivanti Neurons for UEM e ao Ivanti Neurons for MDM.

Existem dois tipos de permissões disponíveis e, portanto, dois tipos de funções:

- **Funções específicas ao espaço** – As permissões são específicas ao espaço e, portanto, se aplicam somente a um espaço específico. Os exemplos incluem Gerenciamento de dispositivos e Gerenciamento de aplicativos em um Espaço.
- **Funções entre espaços** – As permissões são, por natureza, aplicáveis a todas as funções. Exemplos incluem configurações no nível do locatário, como certificados MDM e configurações do App Catalog.

Criar uma função personalizada

É possível criar funções personalizadas entre espaços ou específicas a um espaço. Quando você seleciona uma permissão, as permissões dependentes são selecionadas automaticamente. Portanto, um usuário com uma função personalizada pode apenas realizar as ações específicas (como desativar, limpar) disponíveis quando ele visita a página Dispositivos ou a página Detalhes do dispositivo.

Quando você aplica a função personalizada Visualizar PIN de Registro do Usuário, os usuários podem visualizar o PIN de outros usuários que tenham o mesmo nível de acesso ou privilégios menores e não podem criar PINs para outros usuários.

A função personalizada recém-criada não pode ser atribuída a ninguém automaticamente. O superadministrador de locatário precisa atribuí-la aos usuários do administrador necessário que, posteriormente, pode atribuí-la a outros funcionários conforme necessário.

Procedimento

1. Acesse **Admin** > **Gerenciamento de funções**.
2. Clique em **+Adicionar função personalizada**.
3. Na página **Criar função**, insira o **Nome** da nova função.
4. (Opcional) Adicione uma descrição para a nova função.
5. Em **Tipo de função**, selecione um dos seguintes tipos:
   - **Função entre espaços**
   - **Função específica do espaço**
6. Em **Permissões**, selecione as permissões granulares necessárias.

   Para permissões de administrador e de usuário, veja a tabela a seguir.
7. Clique em **Salvar**.

A tabela a seguir relaciona as permissões, funções e atributos que você pode usar para criar uma função personalizada:

Tipo de função	Categoria de permissões	Permissões granulares
Função entre espaços Administrador		
	Gerenciar atributos personalizados	• Adicionar atributo personalizado • Excluir Atributo Personalizado • Editar atributo personalizado • Visualizar atributo personalizado
	Administradores de suporte	• Adicionar administradores de suporte • Excluir administradores de suporte

Tipo de função	Categoria de permissões	Permissões granulares
	Autoridade de certificação	• Desativar administradores de suporte • Visualizar administradores de suporte e mostrar histórico de login • Adicionar Autoridade de certificação • Excluir Autoridade de certificação • Editar Autoridade de certificação • Visualizar autoridade de certificação
	Conector	• Adicionar logs do Connector • Excluir Connector • Visualizar Connector • Atualizar Connector
	Gerenciamento da LDAP	• Adicionar usuário/grupo/OU • Adicionar Servidor • Navegar no servidor

Tipo de função	Categoria de permissões	Permissões granulares
		• Excluir servidor • Pesquisar servidor • Sincronizar servidor • Remover usuário/grupo/OU • Exibir servidor Todas as permissões do LDAP nesta seção requerem permissão Visualizar Connector. Será selecionado automaticamente na seção Connector quando você selecionar qualquer uma dessas permissões do LDAP.
Usuários	Gestão de licenciamento	Exibir licenças
	Ações de gerenciamento de usuários	• Visualizar usuário • Atualizar usuário • Enviar mensagem ao usuário • Anexar/Atribuir funções ao usuário • Criar usuário • Excluir usuário • Convidar usuário

Tipo de função	Categoria de permissões	Permissões granulares
	Atribuir atributo de usuário personalizado	• Visualizar PIN de registro do usuário • Excluir atributo • Visualizar atributo
	Grupos de usuários	• Adicionar/editar atributo • Exibir grupo de usuários • Editar Grupo de Usuários • Anexar/Atribuir funções ao grupo de usuário • Criar Grupo de Usuários • Excluir grupo de usuários
Dispositivos	Inscrição em massa	• Criar inscrição em massa • Atualizar inscrição em massa • Atribuir usuário à inscrição em massa • Exibir inscrição em massa • Excluir inscrição em massa
Função específica do espaço **Dispositivos**	Ações do dispositivo	• Atribuir dispositivo ao usuário

Tipo de função	Categoria de permissões	Permissões granulares
		• Limpar bloqueio de ativação do dispositivo • Excluir dispositivo • Desabilitar Modo de dispositivo perdido • Habilitar Modo de dispositivo perdido • Check-in forçado do dispositivo • Bloquear dispositivo • Desbloquear dispositivo • Forçar logout do dispositivo • Reinstalar apps do sistema do dispositivo • Reiniciar dispositivo • Programar atualizações do iOS do dispositivo • Renunciar à propriedade do dispositivo

Tipo de função	Categoria de permissões	Permissões granulares
	Designar atributos de dispositivo personalizado	• Desativar dispositivo • Cancelar dispositivo desativado • Desligar dispositivo • Exibir dispositivo • Apagar Dispositivo • Cancelar dispositivo apagado • Atualizar versão de SO do dispositivo • Atribuir em massa via upload • Adicionar/Editar atributo personalizado do dispositivo • Excluir atributo personalizado do dispositivo • Visualizar atributo personalizado do dispositivo

Tipo de função	Categoria de permissões	Permissões granulares
		Todas as permissões Atribuir atributo de dispositivo personalizado nesta seção requerem permissão de leitura do dispositivo. Será selecionado automaticamente na seção Ações do dispositivo quando você selecionar qualquer uma dessas permissões Atribuir atributo de dispositivo personalizado.
	Configurações de dispositivo	• Excluir perfil • Enviar perfil • Enviar perfil excluído • Repetir instalação em caso de erro
	Grupos de dispositivos	• Adicionar grupo de dispositivos • Excluir grupo de dispositivos • Editar grupo de dispositivos • Visualizar grupo de dispositivos
	Inventário de aplicativos	• Visualizar inventário de aplicativo
Configurações	Configurações	• Visualizar/Exportar configurações

Tipo de função	Categoria de permissões	Permissões granulares
Políticas	Políticas	• Editar/Priorizar configurações • Adicionar/Clonar configurações • Excluir configurações • Visualizar políticas • Editar/Priorizar políticas • Adicionar/Clonar políticas • Excluir políticas

Para editar essa função, acesse a página Gerenciamento de funções de administrador e clique no ícone de editar, em **Ações**, próximo ao nome da função. O usuário não pode editar uma função entre espaços para uma função de espaço específico ou vice-versa.

Tópicos relacionados:

- Para atribuir uma função personalizada a um usuário, consulte Atribuindo funções.
- Consulte Funções do usuário para obter uma lista de funções padrão.

Espaços

Espaços

Licença: Silver

Os espaços são usados para separar um sistema de Gerenciamento de terminal unificado (UEM) em entidades gerenciadas de forma independente para fins de administração delegada. Os espaços podem ser criados para refletir uma hierarquia organizacional. O Ivanti Neurons for MDM suporta delegação de nível único com uma entidade de gerenciamento central chamada de Espaço Padrão e várias entidades de gerenciamento subordinadas chamadas de Espaços Delegados. Todo sistema UEM é criado com um espaço padrão.

A página Espaços e as opções associadas ficam ocultas para os locatários convergentes que têm acesso ao Ivanti Neurons for UEM e ao Ivanti Neurons for MDM.

Um Espaço permite realizar a administração delegada dos seguintes componentes do sistema. No momento, os usuários e os grupos de usuários não podem ser delegados.

- Dispositivos
- Configurações
- Políticas
- Grupos de dispositivos
- Aplicativos
- Um App Catalog
- Um token do Apps and Books da Apple

Quando um administrador faz login no Portal do administrador do Ivanti Neurons for MDM em um locatário com ao menos um espaço delegado, o pop-up de promoção de login do portal é exibido. O pop-up de promoção não é exibido após a criação do espaço delegado nem durante o login de usuário caso um espaço delegado já tenha sido criado.

Funções para administradores de Espaço globais e delegados

Um usuário administrador com as funções apropriadas para acessar o espaço padrão é chamado de administrador global. O acesso ao espaço padrão pode ser somente leitura ou acesso de leitura e gravação. Um administrador global com as funções administrativas apropriadas pode criar espaços delegados e designar administradores delegados para gerenciá-los. Um administrador delegado pode ser atribuído para gerenciar um ou mais espaços delegados.

Os espaços que um determinado administrador pode acessar estão listados no menu suspenso Seletor de espaços no canto superior esquerdo das guias Dispositivos e apps. Para visualizar e gerenciar um espaço, use o menu suspenso Espaços para alternar para o espaço desejado.

Um administrador global tem visibilidade e controle sobre todos os espaços delegados, além do espaço padrão. Um administrador delegado tem visibilidade e controle apenas sobre os espaços atribuídos a ele por um administrador global. Um administrador global mantém o controle central sobre os espaços delegados, enquanto um administrador delegado possui autonomia para gerenciar os espaços que foram delegados a ele. Esse nível de autonomia é determinado por a delegação ser herdada ou copiada do espaço padrão.

A seguir estão relacionadas as diferentes funções de usuário e as tarefas que elas podem realizar:

Aplicativo herdado em um Espaço delegado

- Classificações e análises no momento da delegação são herdadas e visíveis para os usuários no espaço delegado, incluindo o nome de usuário do autor.
- Um administrador delegado não pode excluir Classificações/análises de um aplicativo herdado.
- Um administrador delegado pode exportar Classificações/análises de um aplicativo herdado.
- Usuários em espaços delegados podem adicionar Classificações/análises a aplicativos herdado.
- Usuários em espaços delegados podem visualizar Classificações/análises de usuários em espaços delegados, incluindo o nome de usuário do autor.

Aplicativo em um Espaço delegado (adicionado, não herdado)

- Apenas um administrador global pode ativar ou desativar Análises em **Apps > Configurações de catálogo > Classificações e análises**.
- Usuários em espaços delegados podem adicionar Classificações/análises.
- Um administrador delegado pode excluir análises adicionadas por usuários no mesmo espaço delegado.

- Usuários em outros espaços delegados, incluindo o padrão, não podem visualizar Classificações ou análises adicionadas por usuários em cada espaço delegado.
- Um administrador delegado pode exportar análises adicionadas por todos os usuários, incluindo nomes de usuário.

Aplicativo delegado em um Espaço padrão

- Um administrador global pode excluir classificações ou análises adicionadas por um usuário em um espaço delegado.
- Um administrador global pode exportar todas as classificações e análises, incluindo aquelas adicionadas por usuários em espaços delegados.
- Usuários em espaço padrão podem visualizar classificações ou análises adicionadas por usuários em espaços delegados, incluindo nome de usuário.

Prioridade de um Espaço delegado

O espaço padrão em um sistema UEM sempre tem a menor prioridade. A prioridade de um espaço delegado em relação a outros espaços delegados é definida pelo administrador global e pode ser alterada a qualquer momento. Os espaços delegados são classificados de forma ordenada, da prioridade mais alta à mais baixa, na página Espaços na guia Administrador no Portal de Administração.

Delegação por herança ou cópia

Um conceito-chave na administração delegada é se um componente do sistema é herdado ou copiado do Espaço padrão.

Gerenciamento de espaços

Espaços permitem que você designe grupos de dispositivos para gerenciamento por diferentes administradores (administração delegada). O administrador de um espaço pode definir as **configurações**[1] e as **políticas**[2] aplicadas aos dispositivos no espaço. Após criar os espaços, você pode atribuir cada um ao administrador relevante ou apropriado. Não é possível editar ou excluir o espaço padrão.

O usuário pode visualizar apenas os espaços atribuídos, e não todos os espaços disponíveis. A partir de agora, essa configuração se aplica somente aos módulos **Dispositivos**, **Grupos de Dispositivos**, **Aplicativos**, **Inventário de Aplicativos**, **Conteúdo**, **Configurações**, **Políticas** e **Gerenciamento de Certificados**. Os espaços selecionados na lista Espaços durante a visualização de qualquer um desses módulos são salvos como a seleção padrão preferencial do administrador para tal módulo. Essas preferências não são salvas apenas para a sessão de login atual, mas também para as sessões futuras.

Os espaços criados herdam todas as configurações do espaço padrão. Portanto, qualquer configuração criada posteriormente no espaço padrão poderá ser aplicada a outros espaços. Entretanto, as alterações feitas em uma configuração existente não são herdadas.

Os espaços que você cria recebem cópias apenas das políticas que existem no espaço padrão naquele momento. Qualquer política criada posteriormente no espaço padrão será aplicada somente ao espaço padrão.

Crie as regras que definem os dispositivos que estão no espaço. Essas regras podem ser filtradas usando os operadores aplicáveis, incluindo os operadores "começa com", "termina com", "contém", "não contém", "não começa com", "não termina com", "é menor que", "é maior que", "está no intervalo", "é igual a" e "é diferente de". As regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). A precisão das regras pode ser analisada utilizando o texto que aparece no fim das regras.

O Administrador do Ivanti Neurons for MDM exibe o número de grupos de usuários duplicados e o número correspondente de GUIDs para identificar grupos duplicados, quando o atributo Nome do grupo de usuários é selecionado no Criador de regras. Além disso, uma tabela dentro desta regra exibe a lista dos grupos de usuários duplicados e seus detalhes, como Nome do grupo de usuários, GUID, Origem e nome distinto (DN).

As regras podem identificar dispositivos por:

[1]collections of settings that you send to devices.

[2]sets of requirements and compliance actions defined for devices.

- AAD inscrito
- Capacidade APNS
- Número de série alternativo (Android apenas, aplicável a dispositivos Samsung no modo Administrador do dispositivo ou Proprietário do dispositivo)
- Fatiamento de rede Android 5G ativado
- Dispositivo Gerenciado de Trabalho Não GMS com Android (AOSP) habilitado
- Dispositivo dedicado Android
- Compatível com Android corporativo
- Dispositivo gerenciado Android com Work Profile
- Tipo de certificação Android SafetyNet
- Android Work habilitado
- Dispositivos gerenciados de trabalho com Android (Proprietário do dispositivo) ativados
- Perfil de trabalho Android ativado
- Perfil de trabalho do Android ativado em dispositivos de propriedade da empresa
- Registro de dispositivo automatizado registrado
- Registrado por Autopilot
- Código de status do cliente Azure
- Hora do relatório de conformidade do dispositivo do Azure
- Status de conformidade do dispositivo do Azure
- Identificador de dispositivo do Azure
- Sentry bloqueado
- Acesso bloqueado
- Token de inicialização disponível

- Tipo provisionado em massa (Apple Configurator, Nenhum ou Registro automatizado de dispositivo registrado)
- Operadora
- Último registro do cliente
- Cliente registrado
- Conformidade
- Ação de conformidade bloqueada
- Nome do país atual (selecione o nome do país na lista suspensa)
- MCC atual
- MNC atual
- Atributo de dispositivo personalizado
- Atributo LDAP personalizado
- Atributo de usuário personalizado
- Roaming de dados
- Origem do dispositivo
- Tipo de dispositivo
- Nome de exibição
- Criptografia ativada
- Nome do país de origem (selecione o país de origem na lista suspensa)
- MCC inicial
- MNC inicial
- Endereço IP
- Modo de quiosque
- Último check-in

- Somente MAM
- Fabricante
- Modo multiusuários
- SO
- Versão do SO
- Propriedade
- Número de telefone
- Em quarentena
- Bloqueio de recuperação habilitado
- Roaming
- Status de Secure Apps
- Número de série
- Status
- Supervisionado
- Versão de compilação suplementar
- Extra da versão/SO suplementar
- Token de desbloqueio disponível (iOS)
- Registro de usuário registrado
- Grupo de usuários
- Nome de Usuário
- Roaming de voz
- Chave de recuperação pessoal do macOS garantida
- Tipo de chave de recuperação do macOS

Essas regras estão disponíveis apenas para licenças **Silver** e superiores.

Como criar um espaço

Procedimento

1. Acesse **Administrador** > **Espaços**.
2. Clique em **Gerenciar**.
3. Clique em **Criar novo espaço**.
4. Clique em **Pré-visualizar** para ver quais dispositivos serão atribuídos ao espaço.
5. Clique em **Salvar** quando estiver satisfeito com os dispositivos no espaço.

> Para excluir, clique no ícone Excluir do espaço criado.

Priorização de Espaços

O Ivanti Neurons for MDM avalia os espaços na ordem de aparição. Para alterar a ordem, clique nas setas no canto superior direito da definição do espaço.

Como atribuir um administrador a um Espaço

Procedimento

1. Acesse **Usuários**.
2. Pesquise pelo usuário que será o administrador.
3. Clique no link do usuário para exibir os detalhes.
4. Selecione **Ações** > **Atribuir funções**.
5. Selecione **Gerenciamento de dispositivos**.
6. Em **Gerenciamento de dispositivos**, selecione o espaço deste administrador.
7. Clique em **Concluído**.

Quando esse administrador fizer o login, somente os dispositivos, configurações e políticas no espaço atribuído estarão visíveis.

Como clonar uma configuração ou uma política

É possível clonar uma configuração ou uma política para duplicá-los com algumas diferenças. Também é possível associar as configurações ou políticas clonadas a diferentes grupos de dispositivos. Todas as políticas podem ser clonadas dentro de um espaço. Todas as configurações, exceto pelo Certificado de identidade fornecido pelo usuário e pela Defesa contra ameaças, podem ser clonadas dentro de um espaço. As seguintes configurações também podem ser clonadas entre espaços do espaço padrão:

- Restrições do iOS
- Web clip
- Certificado
- Senha
- SCEP (iOS e Windows)
- Certificado de identidade (gerado dinamicamente)

- O nome de uma configuração ou tipo de política deve ser exclusivo no espaço. Todas as demais propriedades de uma configuração ou política podem ser clonadas.
- As configurações serão clonadas para todos os espaços aos quais você, o administrador, tenha acesso. Você não precisa ser um administrador global para clonar uma configuração.

Clonar uma configuração ou uma política

Procedimento

1. Acesse **Configurações** ou **Políticas**, dependendo do que você deseja clonar.
2. Clique no link da configuração ou da política para exibir os detalhes.
3. Clique no ícone **Clonar**.
4. Na janela pop-up, insira um **Nome** e, opcionalmente, uma **Descrição**.
5. Clique em **Avançar**.
6. Modifique a configuração ou a política segundo seus requisitos.
7. Clique em **Avançar**.

8. Configure a distribuição.
9. Clique em **Concluído**.

Para obter mais informações, consulte Exemplos de espaços.

Exemplos de espaços

Este tópico oferece exemplos de como administradores podem usar os espaços.

Administrador por local

ACME, Inc. tem escritórios na América do Norte e na Europa. Devido aos problemas de fuso horário e idioma, o ACME quer um administrador nos Estados Unidos para gerenciar os dispositivos da América do Norte e um administrador na Alemanha para gerenciar os dispositivos na Europa.

Para definir esses Espaços, o ACME fez as seguintes alterações:

1. Criou um grupo de usuários no Ivanti Neurons for MDM para os usuários na Europa.
2. Criou um grupo de usuários no Ivanti Neurons for MDM para os usuários na América do Norte.
3. Foi criado um espaço Europa com a seguinte regra:

   Grupo de usuários = Europa
4. Foi criado um Espaço América do Norte com a seguinte regra:

   Grupo de usuários = América do Norte
5. Foi atribuída a função de Gerente de dispositivo para cada Espaço ao administrador adequado.

Agora, o ACME possui os seguintes Espaços:

- Europa
- América do Norte
- Padrão

Administrador por SO, por local

O ACME decidiu que somente os especialistas em Android devem administrar dispositivos Android. Foi adicionado um especialista em Android na organização da América do Norte e um na da Europa. Por isso, são necessários dois novos Espaços.

Para adicionar os Espaços, o ACME fez estas mudanças:

1. Foi criado um espaço Europa-Android com a seguinte regra:

   Grupo de usuários = Europa

   SO = Android

2. Foi criado um Espaço América do Norte-Android com as seguintes regras:

   Grupo de usuários = América do Norte

   SO = Android

3. Foi atribuída a função de Gerente de dispositivo para cada Espaço ao administrador adequado.

Agora, o ACME possui os seguintes Espaços:

- Europa-Android
- América do Norte-Android
- Europa
- América do Norte
- Padrão

Administrador para executivos

Os executivos do ACME decidiram que eles queriam um serviço especial de um administrador especial. Estão na lista somente os executivos mais importantes.

Para adicionar esse Espaço, o ACME fez as seguintes alterações:

1. Criou um espaço Executivos com as seguintes regras:

   Nome de Usuário = jdoe@acme.com

   Nome de Usuário = gkunz@acme.com

   Nome de Usuário = prizzo@acme.com

   Nome de Usuário = fvanhoff@acme.com

2. Moveu o Espaço para o topo da lista na página **Espaço**.

Caso contrário, os executivos com dispositivos Android teriam o administrador errado.

3. Foi atribuída a função de Gerente de dispositivo do Espaço ao administrador especial.

Agora, o ACME possui os seguintes Espaços:

- Executivos
- Europa-Android
- América do Norte-Android
- Europa
- América do Norte
- Padrão

Administrador para todos os outros dispositivos

Quando o ACME abrir um novo escritório no Japão, os dispositivos adicionados serão atribuídos ao administrador do Espaço padrão até que alguém crie um Espaço para o Japão.

Delegação de dispositivos

Os espaços são usados para separar seus dispositivos em entidades gerenciadas de forma independente. A associação para espaços é determinada pelas regras que você cria. A delegação de dispositivos permite que um administrador global particione e gerencie dispositivos de forma independente em um sistema UEM. Quando dispositivos são delegados, o acesso a esses dispositivos pode ser atribuído a um subconjunto de administradores delegados, distribuindo, assim, as responsabilidades de administração.

Os dispositivos delegados podem ser agrupados em grupos de dispositivos, e diferentes configurações personalizadas podem ser aplicadas a eles sem afetar os dispositivos que estão no Espaço padrão ou em outros Espaços.

Criação de regas para delegação de dispositivos

As regras definidas para um Espaço determinam quais dispositivos pertencem ao Espaço. Um dispositivo pode pertencer somente a um Espaço. Dispositivos que não correspondem às regras do espaço criadas pertencem automaticamente ao espaço padrão.

1. Selecione **Qualquer** se quiser que os dispositivos sejam incluídos na definição caso atendam a alguma das regras.
2. Selecione **Todas** se quiser que os dispositivos sejam incluídos na definição caso atendam a todas as regras.
3. Selecione um dos seguintes tipos de regra do menu suspenso:
    - **Atributo LDAP personalizado:** para regras baseadas em atributos LDAP.
    - **SO:** para regras baseadas no sistema operacional do dispositivo.
    - **Grupo de usuários:** para regras baseadas no grupo de usuários do dispositivo (conforme definido no serviço de gerenciamento do dispositivo).
    - **Nome de usuário:** para regras baseadas no nome de usuário associado ao dispositivo.

4. Defina o critério para o tipo de regra selecionado:
    - **Atributo LDAP personalizado:** insira o nome do atributo LDAP personalizado que foi configurado nas configurações LDAP.
    - **SO**: selecione Android, iOS, macOS ou Windows.
    - **Grupo de usuários**: selecione um dos grupos de usuários exibidos no menu suspenso. Esses são os grupos de usuários definidos em **Usuários > Grupo de usuários**.
    - **Nome de usuário**: digite um nome de usuário.
5. Para adicionar outra regra para esse Espaço, clique em + ao lado da regra anterior.
6. Clique em **Pré-visualizar** para ver quais dispositivos serão atribuídos ao Espaço.
7. Clique em **Salvar** quando estiver satisfeito com os dispositivos no Espaço.

Os dispositivos que não corresponderem mais às regras de um Espaço serão movidos automaticamente para o próximo Espaço correspondente. Se o dispositivo não corresponder às regras de um Espaço existente, ele será movido para o Espaço padrão. Por exemplo, remover um usuário de um grupo de usuários pode fazer com que seus dispositivos sejam movidos para outro Espaço. Movimentações para um Espaço diferente podem resultar em alterações em políticas e configurações.

Delegação de apps

A delegação de aplicativos permite que um Administrador global particione e gerencie aplicativos de forma independente no Ivanti Neurons for MDM. O administrador global pode fornecer e distribuir centralmente apps públicos e internos, enquanto mantém a separação e o controle proporcionados pelos Espaços delegados.

Ao distribuir de forma centralizada um aplicativo, o administrador global pode predefinir o comportamento de gerenciamento do aplicativo por meio das configurações do aplicativo, bem como das regras de distribuição dos apps. Então, o aplicativo pode ser delegado e disponibilizado no App Catalog do Espaço delegado.

O aplicativo delegado é, então, distribuído a usuários em um determinado Espaço delegado. Quando aplicativos são delegados, é possível atribuir o acesso a esses aplicativos a um subconjunto de administradores delegados, distribuindo, assim, as responsabilidades de administrador.

A delegação de aplicativos exige que um ou mais espaços delegados sejam definidos primeiro. Quando é delegado, um aplicativo é atribuído a todos os Espaços. O Espaço de delegação de aplicativo é classificado como:

- Espaço padrão
- Espaços delegados

Adição de aplicativo a um Espaço delegado

Um aplicativo pode ser adicionado a um Espaço Delegado por um Administrador Delegado ou Global. O aplicativo aparece apenas no App Catalog do espaço delegado onde foi adicionado. Se você adicionar a um Espaço Delegado um aplicativo anteriormente delegado no Espaço Padrão, ocorrerá um erro. Nesse caso, é necessário primeiro desativar a herança do aplicativo no espaço padrão para poder adicioná-lo a um espaço delegado. Para obter mais informações, consulte **Adicionando uma configuração** em "Trabalhando com configurações" na página 445.

Distribuição de aplicativos em um Espaço delegado

Quando um aplicativo é delegado do espaço padrão, suas regras de distribuição são herdadas. Este aplicativo será distribuído para todos os dispositivos atribuídos ao espaço delegado que correspondem às regras de distribuição do aplicativo.

A partir da versão 81 do Ivanti Neurons for MDM, os administradores globais poderão delegar administradores de espaço para editar o certificado de identidade gerado dinamicamente para todos os dispositivos e para a opção de distribuição personalizada.

As alterações de distribuição são aplicáveis somente ao espaço específico. Todos os outros espaços continuam herdando as configurações de distribuição de espaço padrão.

Para obter mais informações, consulte **Adicionando uma configuração** em "Trabalhando com configurações" na página 445.

Administradores de suporte

Crie um administrador de suporte temporário para habilitar a equipe de suporte de serviço a fazer login com suas funções e permissões. Esse usuário expira automaticamente em 7 dias ou você pode encerrar o acesso a qualquer momento. Criar um administrador de suporte facilita a resolução de problemas por parte da equipe de suporte.

Criação de um administrador de suporte

Procedimento

1. Na página **Support Administrators**, clique em **Adicionar usuário de suporte**.
2. Clique em **Criar usuário** para confirmar.

   Essa etapa envia um e-mail à equipe de suporte do serviço de gerenciamento do dispositivo.

> O campo **Nome de exibição** mostra "(desativado)" até que um membro da equipe de suporte ative a nova conta. O nome de exibição terá o seguinte formato:
>
> support-[ID_aleatório]-[seu_nome_de_usuário]@[sua_empresa].com
>
> Após criar um administrador de suporte, selecione **Administrador > Support Administrators** para ir diretamente à lista de administradores de suporte existentes. Entretanto, se você precisar criar usuários de suporte adicionais, vá diretamente para a etapa 2 acima.

Visualizar histórico do usuário

Na página **Administradores do suporte**, clique em **Histórico do usuário** para visualizar o histórico de login dos administradores do suporte. A disponibilidade dos dados do histórico de login na página Administradores do suporte é restrita aos dados dos últimos 90 dias.

Desativação do acesso de um administrador de suporte

Procedimento

1. Na página **Support Administrators**, clique no link **Excluir** à direita da conta que você deseja remover.
2. Quando solicitado, clique em **Remover usuário** para confirmar.

Suspensão do acesso de um administrador de suporte

Na página **Support Administrators**, clique no link **Desabilitar** à direita da conta que você deseja suspender.

Admin > Notificação de uso do sistema

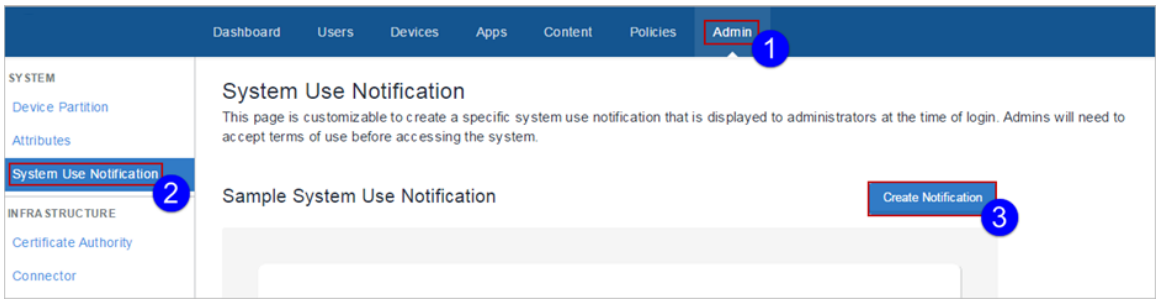
Licença: Silver

Use o recurso Notificação de uso do sistema para criar uma notificação personalizada de uso do sistema que será exibida aos administradores no momento do login e exigirá que eles aceitem os termos de uso antes de acessar o sistema.

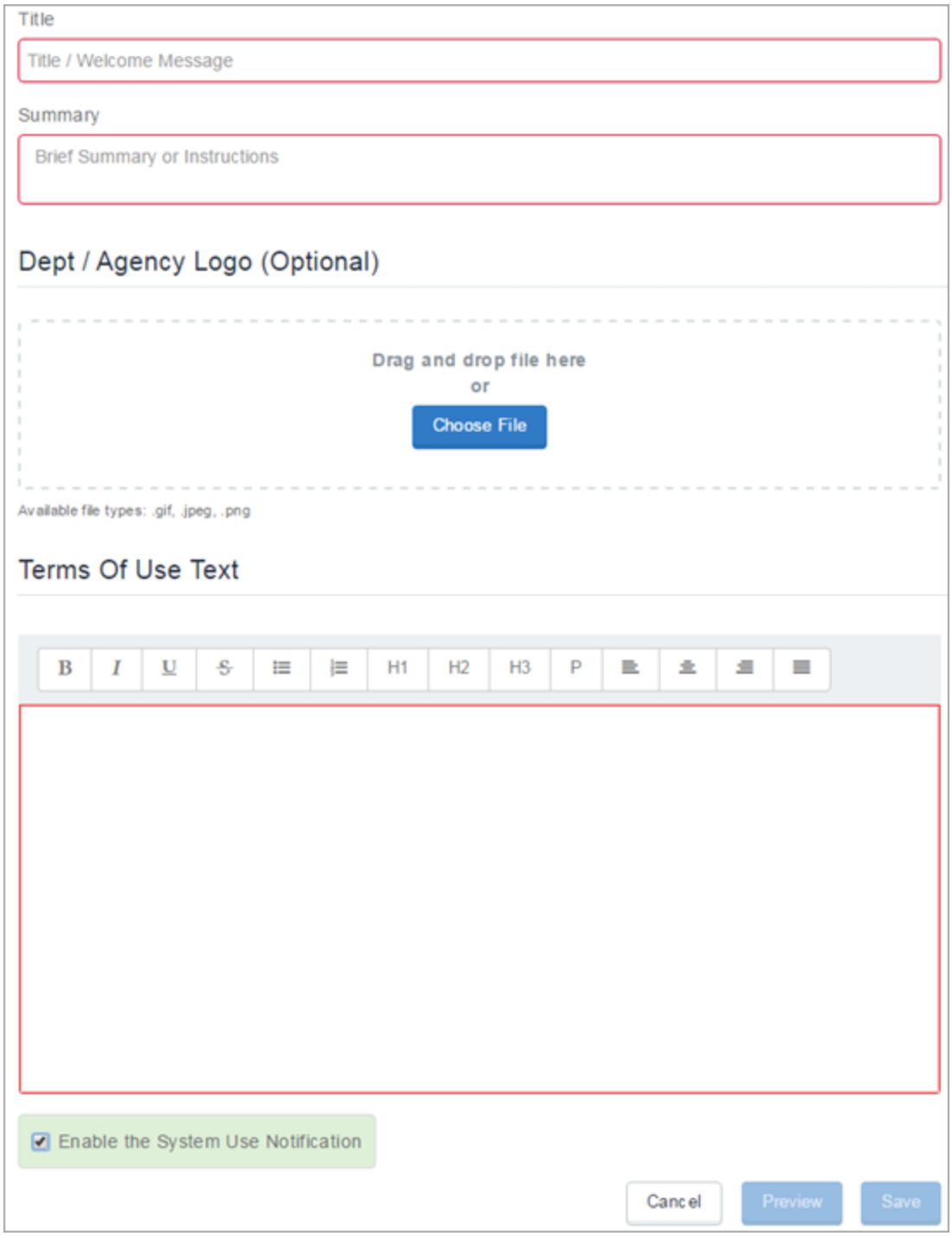
Criação da notificação de uso do sistema

Procedimento

1. Selecione **Admin > Notificação de uso do sistema**.
2. Clique em **Criar notificação**.



A página de detalhes da notificação de uso do sistema é exibida.



3. Insira um título no campo **Título**.

4. Insira um resumo ou instruções no campo **Resumo**.
5. Se quiser, escolha um logotipo.
6. Insira o texto dos termos de uso no campo **Texto dos termos de uso**. Esse é o texto que o administrador terá de aceitar no momento do login.
7. Marque a caixa de seleção **Habilitar notificação de uso do sistema** para ativar a notificação.
8. Clique em **Pré-visualizar** para solicita uma pré-visualização da notificação de uso do sistema.
9. Clique em **Salvar** quando estiver satisfeito com a notificação de uso do sistema.

Infraestrutura

Esta seção contém os seguintes tópicos:

Acesso

Aplicável a: dispositivos iOS e Android.

O Access mantém os dados de negócios seguros e permite uma experiência do usuário contínua e produtiva em qualquer dispositivo ou aplicativo. O Access estabelece um limite de dados que evita que usuários acessem serviços de cloud corporativa em dispositivos, aplicativos ou serviços de cloud sem segurança.

Documentação mais recente

Acesse Documentação do produto e clique em Access para obter mais informações sobre o Access e como configurar o Access. Selecione o documento apropriado para a sua versão do Access.

Listas de aplicativos

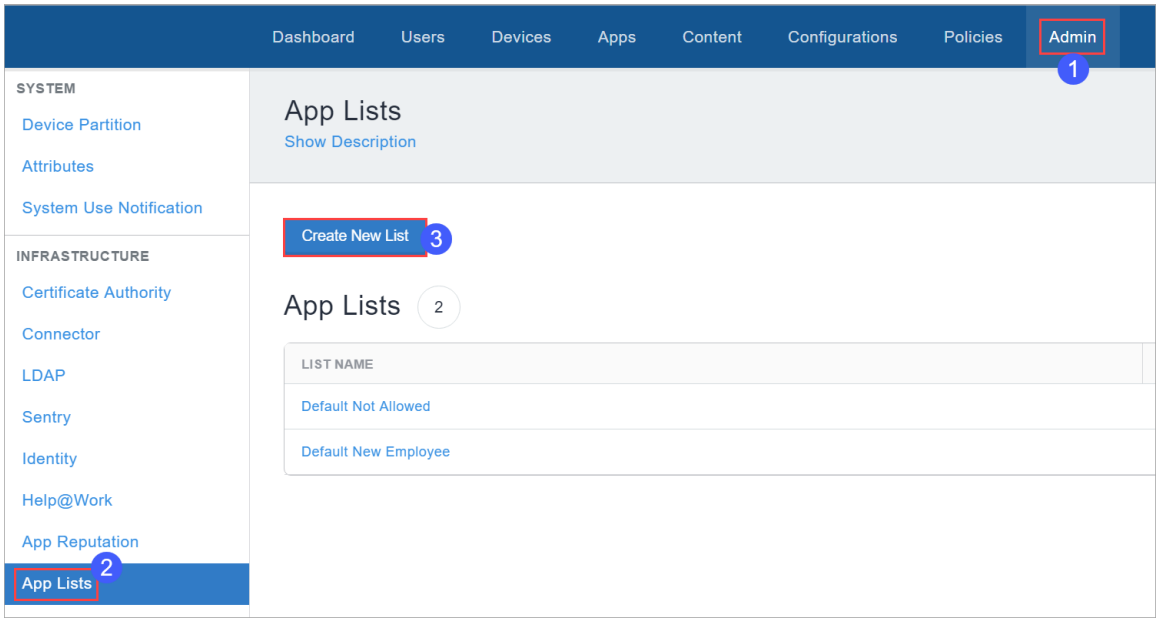
Licença: Silver

É possível criar listas de apps obrigatórios, permitidos e bloqueados para uso com a política de Apps permitidos, que permite usar essas listas para ajudar a especificar as ações a tomar se os apps instalados de um dispositivo não atenderem aos requisitos indicados nas listas de apps. Não é possível editar listas de aplicativos depois de criadas porque elas podem ser citadas nas políticas de Aplicativos permitidos. De forma semelhante, não é possível excluir listas de aplicativos citadas por qualquer política de aplicativos permitidos.

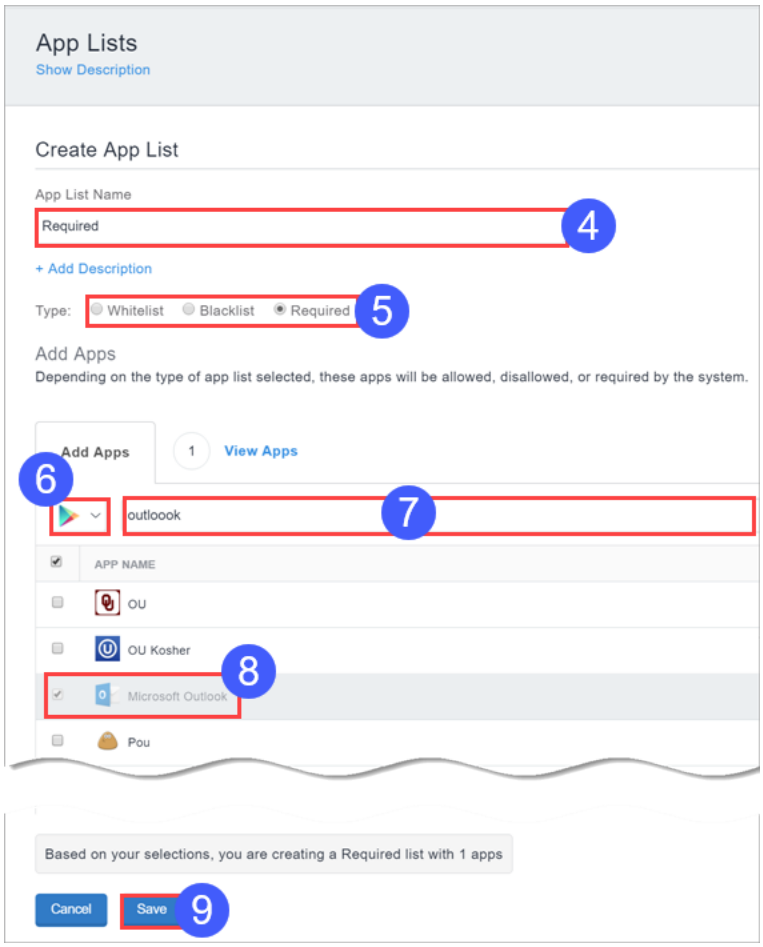
Criação de listas de aplicativos

Procedimento

1. Clique em **Administrador**.



2. Clique em **Listas de aplicativos**.
3. Clique em **Criar nova lista**.



4. Configure um nome para a lista.
5. Selecione o tipo de lista: **Lista de permitidos**, **Lista de bloqueados** ou **Obrigatórios**.
6. Selecione o tipo de aplicativo **App Store**, **OS X Store**, **Google Play** ou **App Catalog**.
7. Insira critérios de busca para restringir suas opções.
8. Use as caixas de seleção para escolher os apps. É possível usar várias buscas e habilitar mais de uma caixa de seleção.

   Clique na guia Visualizar aplicativos para ver uma lista de aplicativos selecionados até o momento.
9. Clique em **Salvar**.

Agora, é possível usar essa lista ao configurar a política de Aplicativos permitidos.

Se você não conseguir visualizar a página **Listas de apps,** pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Exportação de trilhas de auditoria

A exportação de trilhas de auditoria é um recurso usado para exportar e carregar todas as informações de trilhas de auditoria para um local de servidor específico. O servidor deve estar acessível a partir da porta padrão. Os usuários podem definir configurações da Exportação de trilhas de auditoria para carregar arquivos das Trilhas de auditoria automaticamente em um local específico diariamente.

A exportação de trilhas de auditoria é compatível em servidores SFTP baseados em Linux e Windows.

Para definir as configurações para as Trilhas de auditoria:

1. Selecione **Administrador > Infraestrutura > Trilhas de auditoria**. A página **Trilhas de auditoria** é exibida.
2. Na página **Trilhas de auditoria**, clique em **LIGADO** para habilitar a exportação de trilhas de auditoria.

   Na seção **Exportar**, atualize os campos a seguir:

Recurso	Descrição
Formato de exportação	Selecione qualquer um dos formatos a seguir em que os dados de Trilhas de auditoria devem ser exportados: • **JSON** • **CEF** (formato de evento comum) A mensagem de log CEF contém os seguintes valores padrão: • Versão: número de versão do formato CEF. v25 é a versão com suporte atual. • Fornecedor do dispositivo: Ivanti Inc • Produto no dispositivo: Ivanti Neurons for MDM • Versão do dispositivo: versão mais recente de Ivanti Neurons for MDM no momento da geração do evento. • ID da classe de eventos do dispositivo: ID exclusivo da entidade por trilha • Nome: nome da entidade e ação por trilha. Exemplo: definições de configuração de distribuição de promoção Criar. • Severidade: especifica a importância do evento. Exemplo: baixa. A mensagem de log CEF inclui também campos de extensão que são uma coleção dos seguintes paredes de chave-valor: • CS1 e CS1Label: metadados de trilhas de auditoria, como createdAt, entityType, entityName e actionType. • CS2 e CS2Label: informações do ator. • CS3 e CS3Label: estado antes da ação. • CS4 e CS4Label: estado após a ação.

Recurso	Descrição
	Na exportação CEF, se qualquer um dos campos (exemplo: chaves CS3 ou CS4) exceder as limitações especificadas, o valor real será substituído pelo texto "O valor para esta chave excede a extensão permitida para a chave do dicionário mapeada".
Servidor	Insira o nome do servidor para exportar as Trilhas de auditoria.
Usuário	Insira o nome de usuário para efetuar login no servidor.
Senha	Insira a senha de login do servidor.
Caminho do servidor	Insira o caminho do servidor e certifique-se de que o caminho dado exista no servidor. Exemplo: /Usuários/Teste/Exportar.
Algoritmo de troca de chaves	Selecione a lista de algoritmos de troca de chaves para exportar o log de auditoria para a configuração de SFTP de saída. Os seguintes algoritmos de troca de chaves são selecionados por padrão: • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **diffie-hellman-group-exchange-sha256** (selecionado por padrão)
Cifras	Selecione a lista de cifras de criptografia para exportar o log de auditoria para a configuração de SFTP de saída. Os seguintes códigos de criptografia são selecionados por padrão: • **aes128-ctr** • **aes192-ctr** • **aes256-ctr** (selecionado por padrão)
HMAC	Selecione a lista de algoritmos HMAC para exportar o log de auditoria para a configuração de SFTP de saída. **hmac-sha1** é o algoritmo HMAC selecionado por padrão.

Os campos mencionados acima estarão no modo somente leitura se esses campos já estiverem configurados. Para editar os campos configurados, você deve clicar no botão **Editar**. Se o administrador já configurou a exportação de SFTP, todos os algoritmos de chave serão selecionados após a atualização.

3. Clique em **Testar conexão e salvar** para testar a conexão e salvar a configuração de exportação das Trilhas de auditoria.

   Os arquivos das Trilhas de auditoria arquivados estão disponíveis no formato JSON em um arquivo .zip.

   Verifique as definições de configuração em todos os campos antes de salvar as configurações de exportação das trilhas de auditoria. Uma mensagem de erro será exibida se algum dos valores do campo digitado for inválido.

Gerenciamento de certificado

Licença: Silver

Usar a autenticação de certificado é uma forma eficaz de proteger seus dispositivos móveis. Os certificados são mais seguros que senhas, além de possibilitarem o uso de uma única credencial para proteger VPNs, redes sem fio, e-mail etc. Se a sua organização tem acesso a uma autoridade de certificação externa, use um Connector para acessá-la. Se sua organização não tem acesso a uma autoridade de certificação, você pode usar Ivanti Neurons for MDM como uma autoridade de certificação. Você também pode usá-la como uma autoridade de certificação intermediária para outras autoridades de certificação. Os certificados gerados pelo Ivanti Neurons for MDM são chamados de certificados autoassinados.

- Os certificados SHA-1 são preteridos durante a criação dos certificados de identidade. Você pode escolher outros algoritmos. Ao atualizar os certificados, se os certificados mais antigos usarem SHA-1, o mesmo algoritmo SHA-1 poderá ser utilizado. Se os certificados mais antigos usarem um algoritmo acima de SHA-1, a reversão para SHA-1 não será permitida.
- Durante a configuração da autoridade de certificação local ou externa, selecione a opção **Armazenar identidades em cache no Ivanti Neurons for MDM** para armazenar os certificados com o serviço do Ivanti Neurons for MDM. Sempre que necessário, limpe o cache para gerar identidades.
- Ao editar um certificado existente, no menu **Ações**, é possível selecionar a opção **Limpar certificados em cache e emitir novos com atualizações recentes**, se necessário. Os certificados que não estão armazenados em cache serão emitidos de novo automaticamente.
- Para melhorar a eficácia do sistema, os certificados das configurações criadas pelo administrador são gerados offline, usando uma fila do tipo "Primeiro a entrar, primeiro a sair" (FIFO). Durante o período em que as configurações estiverem sendo geradas offline, o estado da configuração será **Geração de certificado pendente** na coluna **Status** em **Configurações** na página **Detalhes do dispositivo**. Depois que os certificados são gerados, as configurações mudam para o estado **Instalação pendente** e são enviadas, junto com os certificados, para os dispositivos por meio de check-ins forçados automáticos.
- Todos os certificados de Autoridade de Certificação, incluindo os certificados assinados pela DigiCert PKI Platform ou Autoridades de Certificação externas da GlobalSign, são revogados quando um dispositivo é desativado, apagado e quando os certificados são gerados novamente.

Como administrador, você agora pode gerar certificados do Ivanti Neurons for MDM para login de cartão inteligente e IDs de objetos personalizados (OIDs). É possível gerar certificados para as seguintes opções de autenticação:

- Autenticação do cliente – ativada por padrão

- IPSEC – opcional, pode ser ativada pelo administrador
- Login de cartão inteligente – opcional, pode ser ativada pelo administrador
- OIDs personalizados – opcionais, podem ser ativados pelo administrador

Este recurso só é aplicável para as seguintes autoridades de certificação:

- Autoridade de certificação local
- Autoridade de certificação intermediária
- Autoridade de certificação externa – configure as políticas do aplicativo do modelo de autoridade de certificação no servidor NDES para oferecer suporte a IPSEC, login de cartão inteligente e OIDs personalizados

Nos modos Administrador do Dispositivo, Estação de Aplicativos ou outros modos não Android Enterprise, não há suporte para Gerenciamento de Certificados em dispositivos Samsung usando APIs Samsung. Recomenda-se verificar a transição para o Android Keystore com base na recomendação da Samsung.

Para mais informações, consulte "Configuração do certificado" na página 538.

Conectar a uma autoridade de certificação SCEP local

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Instale e configure um Connector (**Administrador > Connector**). Para mais informações, consulte "Conector" na página 1232.
3. Acesse **Administrador** > **Infraestrutura** > **Gerenciamento de certificados**.
4. Clique em **Adicionar** na seção **Autoridade de Certificação**.
5. Selecione **Adicionar uma autoridade de certificação SCEP local** e clique em **Continuar:**
6. Insira um nome que identifique a configuração.
7. Selecione um dos tipos de autoridade certificação a seguir:

- Microsoft
- EJBCA
- Servidor SCEP genérico
  A opção Servidor SCEP genérico pode ser utilizada com a maioria dos servidores SCEP com uma senha de desafio estática.

8. Preencha o formulário exibido.
9. Clique em **Concluído**.

Como criar uma autoridade de certificação externa

Escolha essa opção se deseja usar uma Autoridade de certificação hospedada por terceiros.

Procedimento

1. Na página **Gerenciamento de certificados**, clique em **Adicionar** na seção **Autoridade de certificação**.
2. Na página Adicionar autoridade de certificação, em Criar uma autoridade de certificação externa, clique em **Continuar**.
3. Selecione GlobalSign ou Plataforma DigiCert PKI como Autoridade de certificação externa.
4. Preencha os campos restantes no formulário exibido.
5. Clique em **Concluído**.

Exibição do certificado de uma autoridade de certificação externa

É possível visualizar os detalhes de um certificado e carregar o certificado root intermediário/alternativo para essa autoridade de certificação substituir a cópia existente armazenada.

Procedimento

1. Em **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Ações** ao lado da autoridade de certificação externa e clique em **Ver certificado**. A janela **Exibir certificado** é exibida.

2. Na janela **Exibir certificado**, clique em **Carregar certificado**. A janela **Carregar certificado: CA externa** é exibida.
3. Clique em **Escolher arquivo** para selecionar o certificado a ser carregado.
4. Clique em **Concluído**.

Criação de uma autoridade de certificação intermediária

- Se você precisa de um certificado, gere um CSR e envie-o à autoridade de assinatura. Após receber o certificado da autoridade de assinatura, faça o upload do certificado.
- Se você já tiver o certificado necessário, carregue-o.

Gere uma CSR (solicitação de assinatura de certificado)

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Adicionar**
2. Na seção Adicionar autoridade de certificação, em Criar uma autoridade de certificação intermediária, clique em **Gerar CSR**.
3. Preencha o formulário exibido.
4. Clique em **Gerar**.
5. Copie o conteúdo entre BEGIN CERTIFICATE REQUEST e END CERTIFICATE REQUEST para um arquivo de texto.
6. Carregue o arquivo de texto na autoridade de certificação.
7. Clique em **Concluído**.

Como fazer o upload do certificado assinado

Após receber o certificado assinado da autoridade de certificação, você pode fazer o upload do certificado assinado.

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, localize a entrada para o CSR que você gerou.
2. Na seção, selecione **Ações > Carregar novo certificado assinado**.
3. Clique em **Escolher arquivo**.
4. Selecione o novo certificado assinado.
5. Clique em **Concluído**.

Como fazer o upload de um certificado existente

Este tópico descreve como fazer upload de um certificado assinado.

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Adicionar**.
2. Na seção Adicionar autoridade de certificação, em Criar uma autoridade de certificação intermediária, clique em **Carregar identidade existente**.
3. No campo **Nome**, insira um nome para diferenciar esse certificado dos outros.
4. Clique em **Upload**.
5. Selecione o certificado.
6. Insira a senha para o certificado.
7. Clique em **Upload**.

Exibição do certificado de uma autoridade de certificação intermediária

É possível visualizar os detalhes de um certificado e obter o URL da CRL (Lista de Certificados Revogados) da autoridade de certificação.

Procedimento

1. Na seção **Autoridade de certificação**, clique em **Ações** ao lado da autoridade de certificação e clique em **Ver certificado**. A janela **Exibir certificado** é exibida.
2. Na janela **Exibir certificado**, é possível visualizar a URL no campo **URL da CRL**.

3. Clique em **Copiar** para copiar o URL para a área de transferência e colá-lo em outro aplicativo. Esta URL pode ser usada para configurar o Office 365 para aceitar certificados emitidos pela autoridade de certificação.

Como criar uma Autoridade de certificação independente

Escolha esta opção se desejar criar uma autoridade de certificação totalmente independente (local e autoassinada).

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Adicionar**.
2. Na página Adicionar autoridade de certificação, em Criar uma autoridade de certificação independente, clique em **Continuar**.
3. Preencha o formulário exibido.
4. Clique em **Gerar**.

Configuração do período de expiração da autoridade de certificação independente

Você pode configurar o período de expiração da autoridade de certificação independente (local). Por padrão, o tempo de vida do certificado está configurado como 30 anos.

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Ações** ao lado da autoridade de certificação autônoma.
2. Clique em **Editar**.
   A janela **Editar autoridade de certificação** será exibida.
3. Na seção Modelo de certificado de cliente, no campo **Tempo de vida do certificado**, insira o novo período de expiração em dias.
4. Clique em **Salvar**.

Você pode receber notificações e e-mails (se forem habilitados como opção) quando o certificado emitido por uma autoridade de certificação local está perto de expirar ou já está expirado.

- Notificação sobre os dias para a expiração do certificado - Notificações são geradas em intervalos pré-determinados durante um período de expiração do certificado. A primeira notificação ocorre 365 dias antes expiração, seguida por notificações adicionais que ocorrem 180 dias, 60 dias, 45 dias e 7 dias antes expiração. Você receberá esta notificação até substituir o certificado navegando até **Admin > Gerenciamento de certificados > Ações > Carregar novo certificado assinado**.
- Notificação no certificado expirado - Você recebe uma notificação quando o certificado expira. Você deve substituir o certificado para voltar para o serviço normal.
- Notificar quando um novo certificado válido é carregado. A notificação será enviada quando o novo certificado assinado for carregado.

Visualizar o certificado da autoridade de certificação independente

É possível visualizar os detalhes de um certificado e obter o URL da CRL (Lista de Certificados Revogados) da autoridade de certificação local.

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Ações** ao lado da autoridade de certificação local e clique em **Exibir certificado**. A janela **Exibir certificado** é exibida.
2. Na janela **Exibir certificado**, é possível visualizar a URL no campo **URL da CRL**.
3. Clique em **Copiar** para copiar o URL para a área de transferência e colá-lo em outro aplicativo. Esta URL pode ser usada para configurar o Office 365 para aceitar certificados emitidos pela autoridade de certificação local.

Visualizar uma vida útil do CRL de uma autoridade de certificação

Você pode visualizar e editar a vida útil do CRL de uma autoridade de certificação local ou intermediária.

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Ações** ao lado da autoridade de certificação local e clique em **Editar**. A janela **Editar autoridade de certificação** será exibida.
2. Na janela **Editar autoridade de certificação**, é possível visualizar a CRL no valor de vida útil. O valor padrão mínimo é de 24 horas. O valor máximo que pode ser inserido é de 10.950 horas.
3. Editar o valor de vida útil CRL e clique em **Salvar**.

Criação de uma Autoridade de certificação de Cloud

Escolha essa opção se deseja usar uma Autoridade de certificação de Cloud.

Procedimento

1. Na seção **Autoridade de certificação** na página **Gerenciamento de certificados**, clique em **Adicionar**.
2. Na página Adicionar autoridade de certificação, em Criar uma autoridade de certificação Cloud, clique em **Continuar**.
3. Selecione a Autoridade de certificação em Cloud. As opções disponíveis são as seguintes:
   - **Atos IDnomic CMS**
   - **Plataforma DigiCert PKI**
   - **Entrust**
   - **GlobalSign**
4. Preencha os campos restantes no formulário exibido.
5. Clique em **Concluído**.

Como usar a Pesquisa avançada em certificados

Você pode usar a opção Pesquisa avançada para pesquisar certificados emitidos com base em regras, a fim de identificar e visualizar os certificados com critérios específicos. Essas regras podem ser criadas usando os operadores aplicáveis, incluindo os operadores "começa com", "termina com", "contém", "não contém", "não começa com", "não termina com", "é menor que", "é maior que", "está no intervalo", "é igual a" e "é diferente de". As opções de regras podem ser agrupadas utilizando as opções QUALQUER (OU) ou TODAS (E). Os certificados emitidos que correspondem às regras são exibidos abaixo da seção. A partir do Ivanti Neurons for MDM versão 76, os operadores para todos os modelos de gerenciamento de certificado possuem operadores padrão. Os operadores dos seguintes modelos são padronizados nesta versão:

- Administrador > Gerenciamento de certificado > Certificados emitidos > Pesquisa avançada

Pesquisa avançada em certificados emitidos

Procedimento

1. Na seção **Certificados emitidos** na página **Gerenciamento de certificados**, clique no link **Pesquisa avançada**.
2. Clique em **Qualquer** se os usuários precisarem corresponder a pelo menos uma das regras, ou clique em **Todos** se o certificado precisar corresponder a todas as regras.
3. Crie uma regra que defina os critérios de pesquisa para os seguintes atributos:
   - **CA**
   - **Nome da configuração**
   - **Expiração**
   - **É chave privativa**
   - **SO**
   - **Número de série**
   - **Status**
   - **Tipo de uso**
   - **Usuário**
4. (Opcional) Clique em + para criar regras adicionais, se necessário.
5. (Opcional) Clique em **Salvar** para salvar a consulta.
6. Clique em **Pesquisar**. A lista de usuários que correspondem aos critérios de pesquisa é exibida na página.

Pesquisa avançada em certificados fornecidos pelo usuário

Procedimento

1. Na seção **Certificados Fornecidos pelo Usuário** na página **Gerenciamento de certificados**, clique no link **Pesquisa avançada**.
2. Clique em **Qualquer** se os usuários precisarem corresponder a pelo menos uma das regras, ou clique em **Todos** se o certificado precisar corresponder a todas as regras.

3. Crie uma regra que defina os critérios de pesquisa para os seguintes atributos:
    - **Nome do certificado**
    - **Data da expiração**
    - **Emitido por**
    - **Transferido em**
4. (Opcional) Clique em + para criar regras adicionais, se necessário.
5. (Opcional) Clique em **Salvar** para salvar a consulta.
6. Clique em **Pesquisar**. A lista de usuários que correspondem aos critérios de pesquisa é exibida na página.

Como carregar as consultas de pesquisa para certificados emitidos

Para ver a lista de consultas de pesquisa salvas.

Procedimento

1. Na seção **Certificados emitidos** na página **Gerenciamento de certificados**, clique no link **Pesquisa avançada**.
2. Clique no ícone Pasta. A janela **Pesquisa avançada** é exibida. A lista das consultas de pesquisa criadas é exibida na seção **Consulta carregada**. Os seguintes detalhes são exibidos nessa seção:
    - **Nome da consulta** - O nome da consulta carregada.
    - **Conteúdo da consulta** - Exibe o conteúdo sobre as regras que definem a consulta de pesquisa.
    - **Ações** - Selecione a ação a ser executada na consulta.
3. Clique em **Carregar consulta** na coluna **Ações** para exibir a lista de certificados emitidos que correspondem aos critérios definidos na consulta carregada.
   Para excluir uma consulta carregada, clique no ícone Excluir.

Clique em **Exportar para o CSV** para fazer download do conteúdo reportado pelo resultado da pesquisa em um arquivo CSV para referência ou análise posteriores.

Visualização do período de expiração dos certificados emitidos

Na seção **Certificados emitidos**, na coluna **Expira (em dias)** você pode ver os dias restantes até o certificado expirar se a expiração ocorrer nos próximos 30 dias. Se o certificado já tiver expirado nos últimos 30 dias, a coluna **Expira (em dias)** para o certificado exibe o número de dias decorridos desde a data de expiração.

Para obter mais informações, consulte configuração SCEP para autoridades de certificado externas.

Exportar para CSV

Você pode exportar os certificados para um arquivo CSV para consulta ou análise posteriores.

Procedimento

1. Na página **Gerenciamento de certificados**, vá para uma das guias seguintes.
   - **Autoridade de certificação**
   - **Certificados emitidos**
   - **Certificados fornecidos pelo usuário**
2. Clique em **Exportar para CSV**.
3. Clique em **Baixar**.
4. (Opcional) Clique em **Excluir** para excluir o relatório.

Configuração SCEP para Autoridades de certificado externas

Esse recurso permite o suporte à configuração do Protocolo de Registro de Certificado Simples (SCEP) para autoridades de certificação externas para dispositivos Windows 10.

Configure uma Autoridade de certificação externa

Primeiro, configure uma CA externa. Se você já tiver uma CA externa, pule para a próxima seção.

1. Acesse **Administrador > Infraestrutura > Gerenciamento de certificados**.
2. Clique em **+Adicionar**.
3. Insira um nome para a Autoridade de certificação.
4. Use o menu suspenso para selecionar a Microsoft como o **Tipo de autoridade de certificação**.
5. Insira a **URL do SCEP**.
6. Insira o **Nome de usuário** e a **Senha**.
7. Insira a **URL do Challenge**.
8. Clique em **Salvar**.

Configuração SCEP

Agora, você pode continuar com a configuração SCEP.

1. Acesse **Configuração > +Adicionar**
2. Selecione o ícone do Windows.
3. Selecione **Certificado de identidade** para acessar a página **Criar configuração do certificado de identidade**.
4. Insira um nome para a configuração.
5. Selecione **Configuração Windows** na lista de configurações de SCEP no menu suspenso **Distribuição de certificação**.
6. Selecione a CA externa.

7. Insira os detalhes da Distribuição de certificação.
    - Insira o assunto. Por exemplo: `CN=${userEmailAddress}`
    - Selecione o número de tentativas a partir do menu suspenso **Nova tentativa**.
    - Selecione o número de segundos a aguardar antes de cada entrada no menu suspenso **Atraso de nova tentativa**.
    - Selecione um tamanho de chave a partir do menu suspenso **Tamanho de chave**.
    - Selecione pelo menos uma opção de uso de certificado.
    - Digite o período de tempo no campo e menu suspenso **Validade**.
    - Insira a digital da CA.

      Vá para a URL de desafio do SCEP, copie a impressão digital da CA e cole-a aqui ou clique em **Criar do certificado**... para carregar o certificado a partir do qual a impressão digital da CA pode ser criada.
    - Selecione pelo menos um algoritmo de hashing nas opções **Família de algoritmo de hash**.
8. Clique em **Avançar**.

Fornecedores de credenciais derivadas

Na página Fornecedores de credenciais derivadas, é possível ver a lista de fornecedores de credenciais derivadas utilizados para distribuição do certificado. Você pode especificar quais fornecedores de credenciais derivadas devem ser definidos como padrão e também adicionar outros fornecedores personalizados que você utiliza.

Para definir um fornecedor de credenciais derivadas como padrão:

1. Acesse **Administrador > Fornecedores de credenciais derivadas**. A página lista os seguintes fornecedores de credenciais derivadas.
   - **Entrust**
   - **Intercede**
   - **Purebred**
2. Para o provedor que você deseja definir como padrão, clique em **Definir como padrão** na coluna **Ações**. Após a definição, o ícone de verificação é exibido na coluna **Fornecedor padrão** para o fornecedor em questão, indicando que este é o fornecedor padrão de credenciais derivadas.

Para adicionar um fornecedor de credenciais derivadas personalizado:

1. Acesse **Administrador > Fornecedores de credenciais derivadas**.
2. Clique em **+Adicionar** .
3. Digite o nome do fornecedor de credenciais derivadas no campo de texto na coluna **Nome**.
4. Clique em **Salvar**.
   Após ser adicionado, este fornecedor de credenciais derivadas fica disponível para seleção no campo **Marca** durante a definição da distribuição de Credencial derivada, na configuração **Certificado de identidade**.

Para excluir um fornecedor de credenciais derivadas, clique em **Excluir** na coluna **Ações**.

Não é possível excluir fornecedores de credenciais derivadas que estão definidos como padrão.

Conector

Licença: Silver

O Conector Ivanti Neurons for MDM proporciona o acesso do seu serviço Ivanti Neurons for MDM a recursos corporativos, tais como um servidor LDAP ou uma Autoridade de Certificação (CA). Configure um conector por recurso que você deseja acessar.

Se você usa o Microsoft Active Directory ou um servidor LDAP hospedado na Amazon Web Services (AWS), pode hospedar o Conector Ivanti Neurons for MDM na AWS. Um conector presencial não é necessário.

O Connector é atualizado automaticamente para a versão mais recente do software.

Para obter o mais recente Guia de Instalação do Conector Ivanti Neurons for MDM, acesse https://help.ivanti.com/#106 e pesquise "Connector".

Opções de hospedagem do conector

Você pode hospedar o Conector Ivanti Neurons for MDM no seu datacenter local ou na Amazon Web Services (AWS):

- Hospede o conector no AWS se estiver usando um Microsoft Active Directory hospedado pelo AWS ou se estiver usando um Microsoft Active Directory autogerenciado no AWS. Um conector presencial não é necessário neste caso.
- Para acesso presencial aos recursos, como servidor LDAP ou um CA, configure o conector no local.

Como hospedar o conector no AWS

Os clientes podem hospedar o Connector no AWS e usá-lo com as seguintes opções do Microsoft Active Directory hospedado no AWS:

- AWS Directory Service for Microsoft Active Directory
- Microsoft Active Directory gerenciado pelo cliente no Amazon VPC

Para obter mais informações sobre o AWS Directory Service for Microsoft Active Directory, consulte https://aws.amazon.com/directoryservice. Consulte a documentação do AWS sobre hospedagem no Microsoft Windows Server e Microsoft Active Directory em um Amazon VPC. O Conector Ivanti Neurons for MDM é compatível com Windows Server 2012, 2012 R2, 2015.

Configurando o AMI do Conector Ivanti Neurons for MDM na AWS

Para configurar o AMI do Conector Ivanti Neurons for MDM:

1. Faça login na AWS com credenciais de administrador.
2. Na página de serviços da AWS, selecione **EC2** em **Computar**.
3. Expanda **Imagens** e selecione **AMIs** no painel esquerdo.
4. Selecione **Imagens públicas** na lista suspensa no painel direito.
5. Procure o Ivanti Neurons for MDM Connector usando palavras-chave como "Ivanti Neurons for MDM Cloud Connector."
6. Selecione a versão mais recente do conector na lista e clique em **Executar**.
7. Siga as instruções para instalar o conector na seção "Deploying Ivanti Neurons for MDM Connector in AWS" no *Guia de Instalação do Conector Ivanti Neurons for MDM*, disponível em https://help.ivanti.com/mi/help/en_us/cld/<*versão*>/inst/default.htm, onde *versão* é a versão do Conector Ivanti Neurons for MDM que você está instalando. Por exemplo, para a versão 74 do Conector Ivanti Neurons for MDM, o guia se encontra em https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm.

Como hospedar o conector presencial

Para hospedar o Conector Ivanti Neurons for MDM localmente no seu datacenter, clique em **Baixar Conector** para baixar e instalar o Conector Ivanti Neurons for MDM. Extraia o conteúdo do pacote baixado e siga as instruções de configuração no Guia de instalação do Conector Ivanti Neurons for MDM, incluso no pacote.

Acesso aos registros do Connector

É possível acessar os registros do Connector no serviço Connector para solucionar problemas relacionados ao Connector. Você deve ter função de Gerenciador do sistema ou o de Somente leitura do sistema.

1. Acesse **Administrador > Connector** para exibir a página do Connector.
   A interface do Connector exibe o status do Connector (ativado ou desativado), nome do Connector, conexão (conectado ou não conectado), número da versão, nível de registro, ações (desativar ou remover o Connector).

2. Use o menu suspenso **Nível de registro** para selecionar um nível.
   Os níveis de registro disponíveis são exibidos no menu suspenso em ordem do nível de registro mais baixo para o mais alto:

   - Erro
   - Aviso
   - Informações
   - Depuração
   - Rastreio

   O nível de informação é a configuração de nível de registro padrão. Se você escolher outro nível de registro, é exibido um ícone de Sincronização  que indica que a informação está sendo coletada no nível do registro selecionado. O nível de registro retornará ao Nível de informação após uma hora. O Nível de rastreio é a configuração de registro mais alta . Use este nível para coletar todas as mensagens em todos os outros níveis. O ícone de sincronização é exibido durante a solicitação.

3. Se necessário, passe o mouse sobre o ícone de Sincronização  para visualizar o ícone Cancelar  . Clique no ícone Cancelar para cancelar a alteração do nível de registro.

4. Passe o cursor do mouse sobre o ícone Solicitar para exibir as informações de solicitação. Clique no ícone Solicitar  para solicitar os arquivos da pasta de registro atual em um arquivo .zip.
   Os arquivos de registro são adicionados a um arquivo .zip quando uma solicitação é feita. Quando uma nova solicitação é feita, o arquivo .zip da solicitação anterior é excluído.

5. Se necessário, passe o mouse sobre o ícone Solicitar  e ele se transformará no ícone Cancelar  . Clique no ícone Cancelar para interromper a solicitação.

   Quando uma solicitação é cancelada antes da conclusão, o ícone Download  não é exibido, pois o arquivo .zip anterior foi excluído do servidor. Os arquivos de registro originais no Connector ainda estão disponíveis para solicitação.

6. Clique no ícone Download  quando a solicitação for concluída, para baixar o arquivo .zip do registro que possui os arquivos de registro coletados durante a solicitação mais recente.
   O nome do arquivo de registro tem o formato: `kocab.log`. O nome do arquivo zip que é baixado é composto pelo nome do servidor, pela versão da conexão e pelo carimbo de data e hora, incluindo dia, mês, ano e o horário no formato: `<Nome_do_host_do_Connector>_<Versão_do_Connector>_<Data_e_hora>.zip`. O nome do arquivo .zip arquivado está no formato: `kocab.aaaa-mm-dd.0.log.gz`.

7. Como opção, use o menu suspenso **Ações** para Desativar ou Remover o Connector.

Se você não conseguir visualizar a página do **Connector**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Para obter mais informações, consulte Usando o comando httproxy para o Connector.

Uso do comando httpproxy para o Connector

Um novo comando klish shell foi criado para ajudar a editar a configuração do Connector para sua instalação do Ivanti Neurons for MDM. Use este comando para alterar as informações de login e outros parâmetros para configurar o Connector.

O comando httpproxy agora está disponível nesta versão com os seguintes requisitos.

- klish shell

Para configurar o Connector

1. Entre no klish shell.
2. Insira ? para obter uma lista de comandos klish shell disponíveis.
3. Insira **httpproxy** para mostrar o valor real desses parâmetros:
    a. ativado
    b. esquema
    c. servidor
    d. authtype
    e. nome de usuário
    f. senha

4. Insira **httpproxy ?** para ver uma lista de comandos disponíveis para uso com o httpproxy.
    a. authtype – Configura o tipo de autenticação do proxy http para NONE, BASIC ou NTLM
    b. disable - Desativa o proxy http
    c. enable - Ativa o proxy http
    d. host - Define o host do proxy http; deve ser um FQDN ou um IP http ou https
    e. password - Configura a senha da Autenticação do proxy http
    f. port - Define a porta do proxy http
    g. scheme - Define o esquema do proxy http, deve ser http ou https
    h. show - Exibe as configurações atuais do proxy http
    i. username - Define o nome de usuário da autenticação do proxy http
5. Use os comandos listados acima para configurar a sua instância do Connector.

Help@Work

Licença: Platinum

Suportado em: dispositivos Android e iOS, conforme suportado pelo Ivanti Neurons for MDM

Use o Help@Work para Android/iOS para fornecer assistência remota aos usuários de dispositivos Android e iOS. Help@Work for Android/iOS é baseado no aplicativo TeamViewer QuickSupport. Você precisará de uma conta do TeamViewer para usar o Help@Work para Android/iOS. Se não tiver uma, acesse teamviewer.com para obter mais informações.

O Help@Work transforma a experiência do help desk para dispositivos com iOS 11.0+ e Android ao permitir que os usuários peçam ajuda com o clique de um botão e compartilhem a sua tela com um agente do help desk. Os usuários não precisam mais gastar seu tempo valioso tentando verbalizar o problema, e a equipe de TI consegue resolver os problemas do dispositivo de forma muito mais eficiente. Não há suporte para dispositivos iOS somente MAM.

O TeamViewer é compatível com dispositivos com proprietário do dispositivo Android no modo de quiosque.

Os comandos de início do TeamViewer deixarão de existir se o aplicativo for encerrado ou se o dispositivo for reiniciado.

Nos dispositivos Android, se o aplicativo Teamviewer QuickSupport não estiver instalado, é solicitado que o usuário faça o download do aplicativo. Nos dispositivos iOS, o aplicativo deve ser acionado pelo App Catalog ou, se já estiver instalado no dispositivo, ele deve ser convertido como um aplicativo gerenciado.

O aplicativo Teamviewer QuickSupport deve estar em execução em segundo plano durante a sessão. O aplicativo host do TeamViewer é necessário para o modo autônomo.

A versão do aplicativo para desktop que o administrador instalar deve ser compatível com a versão do Quicksupport instalada no dispositivo do cliente para oferecer suporte para sessões remotas.

Configuração do Help@Work para Android ou iOS

Veja a seguir as etapas de configuração para aplicar identidade visual e distribuir o Help@Work a Androidou iOS:

1. Acesse a guia **Administrador**.
2. Em Infraestrutura, clique em **Help@Work**.
3. O **Help@Work** requer o TeamViewer.Na seção Ativar TeamViewer, ative a opção **TeamViewer assistido** ou **TeamViewer autônomo (somente Android)** clicando no botão **Ativar agora**.
4. Revise o contrato de licença do TeamViewer e clique em **Concordo** para continuar. Sua licença corporativa agora está ativada. Isso identifica os clientes da Ivanti para o TeamViewer para que o acesso seja concedido.

   A opção **Remover ativação** fica disponível ao ativar o TeamViewer. Quando você clica em **Remover ativação** na seção **Ativar TeamViewer**, a janela **Confirmar remoção de ativação** aparece na tela. Clique em **Remover ativação** para remover a ativação do TeamViewer, que por sua vez removerá a funcionalidade Help@Work em todos os dispositivos suportados. No entanto, você pode ativar o TeamViewer usando uma conta existente ou outra conta posteriormente.

   Se quiser excluir a conta **TeamViewer** no modo autônomo, você deve desprovisionar os dispositivos associados para os quais o modo autônomo está ativado. Para desprovisionar os dispositivos associados, você deve cancelar a distribuição do aplicativo **TeamViewer** nos dispositivos associados e forçar o check-in. Certifique-se de que o aplicativo TeamViewer esteja excluído de todos os dispositivos e, em seguida, exclua a vinculação da conta do Admin Console.
5. Certifique-se de que o aplicativo TeamViewer esteja excluído de todos os dispositivos e, em seguida, exclua a vinculação da conta do Admin Console.
6. Distribua o aplicativo TeamViewer para os usuários com os quais deseja iniciar sessões remotas usando o fluxo de trabalho de distribuição do aplicativo padrão. Isso é específico para os modos **Assistido** e **Autônomo**. Se o administrador quiser controlar o dispositivo, também será necessário distribuir a este um complemento universal ou específico do modelo/OEM pelo TeamViewer. Consulte Configuração do aplicativo para obter instruções.

Início de uma sessão remota usando o Help@Work para Android ou iOS

Uma sessão típica do Help@Work para Androidou iOS é iniciada quando um usuário final precisa de ajuda.

Para iniciar a sessão do Help@Work com o dispositivo do usuário:

1. No Ivanti Neurons for MDM, acesse **Dispositivos**.
2. Na página da lista de dispositivos, clique no dispositivo que precisa de suporte.
3. No menu Ações, clique em **Iniciar controle remoto do TeamViewer** para dispositivos Android ou **Exibição remota** para dispositivos iOS. Você verá duas opções:
   - Modo assistido (padrão) - esta opção requer que o aplicativo **TeamViewer Quick Support** seja instalado e colocado na lista de permissões no dispositivo de destino.
   - Modo autônomo (disponível apenas no Android) - esta opção requer que o aplicativo **TeamViewer Host** seja instalado e colocado na lista de permissões no dispositivo de destino.

   A opção de modo autônomo também funciona no modo Quiosque. Ela deve ser habilitada na página de integração do TeamViewer. O controle remoto autônomo requer o aplicativo host do TeamViewer no dispositivo, ativação única em um dispositivo e uma licença de complemento MI. Para a ativação única, o prompt de permissão será exibido quando o aplicativo host TeamViewer for instalado e iniciado pela primeira vez. O administrador pode usar o "Início automático (de parâmetros na configuração de Aplicativo Gerenciado)" do aplicativo TeamViewer após a instalação, se desejar. O número de licenças é calculado com base na distribuição do aplicativo host do TeamViewer. Se o aplicativo host do TeamViewer for distribuído a um dispositivo, será consumida uma licença de sessão de host remoto autônoma. Além do aplicativo host do TeamViewer, outros aplicativos complementares podem ser necessários e devem ser permitidos no modo quiosque ou quiosque compartilhado. Outros complementos podem ser necessários dependendo do modelo e do fabricante do dispositivo.

   Os dispositivos Google Pixel não mantêm essa concessão de permissão e exigem consentimento de permissão em cada sessão.
4. Se o administrador tiver um token válido do TeamViewer, o cliente de desktop começa com uma sessão de suporte para o dispositivo. Caso contrário, o administrador precisará fazer login com o TeamViewer e conceder permissões.

Para iniciar rapidamente uma sessão de remoção, os administradores podem fazer o login no aplicativo desktop previamente.

Como instalar o TeamViewer

Instale o aplicativo TeamViewer no desktop para acessar e fornecer suporte para os dispositivos remotos dos usuários. Para instalar o TeamViewer:

1. Faça download do pacote de instalação da versão completa do TeamViewer para Mac, Windows ou Android aqui: https://www.teamviewer.com/en/download/
2. Inicialize o programa de instalação do TeamViewer.
3. Selecione **Instalação básica**.
4. Selecione **Empresa / Uso comercial**.
5. Clique em **Aceitar - encerrar**.

Como solicitar uma conta do TeamViewer

É necessário ter uma conta do TeamViewer para fornecer suporte usando o TeamViewer. Para obter uma conta do TeamViewer:

1. Acesse https://login.teamviewer.com/.
2. Insira seu e-mail, nome e senha.
3. Clique em **Conectar**.
4. Use a conta de e-mail que você inseriu na etapa 2 para receber um e-mail de ativação da conta do TeamViewer.
5. Siga as instruções do e-mail para ativar sua conta do TeamViewer.

Como confirmar a ID de seção do TeamViewer

O TeamViewer gera uma ID de seção quando a conexão é estabelecida entre o administrador do computador e o usuário do dispositivo móvel.

1. Quando a ID da sessão é gerada, o Ivanti Neurons for MDM a passa para o aplicativo TeamViewer QuickSupport usando a configuração do aplicativo gerenciado, que por sua vez, usa essa ID de sessão para invocar o cliente do TeamViewer no dispositivo. Para o iOS, a ID de sessão expira após 30

minutos.

2. O usuário deve aceitar o EULA do TeamViewer.

Identidade de infraestrutura

Esta seção contém os seguintes tópicos:

Configuração de provedor de identidade

Licença:Silver

Configure um provedor de identidade (IdP) para autenticar usuários que desejam registrar dispositivos no Ivanti Neurons for MDM, acessar este Portal de administrador ou acessar o Portal de autosserviço. É necessário um diretório de usuários compatível com LDAP local. O Ivanti Neurons for MDM funciona com qualquer IdP compatível com SAML 2.0. Autenticação do Microsoft Azure AD (Azure AD), Microsoft ADFS (Active Directory Federation Services), Okta, OneLogin, PingOne e PingFederate do Ping Identity foram verificados para funcionar com o Ivanti Neurons for MDM.

Anteriormente, se você configurasse, a autenticação SAML/IdP, a autenticação SAML era utilizada tanto para o registro de dispositivos quanto para a autenticação do portal. Agora, um botão de alternância é fornecido para escolher diferentes métodos de autenticação para o acesso ao portal do administrador e ao registro de dispositivos. A alternância de bypass é aplicável apenas ao registro de dispositivos.

Durante o registro do dispositivo, o administrador pode dispensar a opção do provedor de identidade e fornecer ao usuário a opção de autenticar usando um PIN em vez de autenticar usando a página do provedor de identidade.

Visão geral

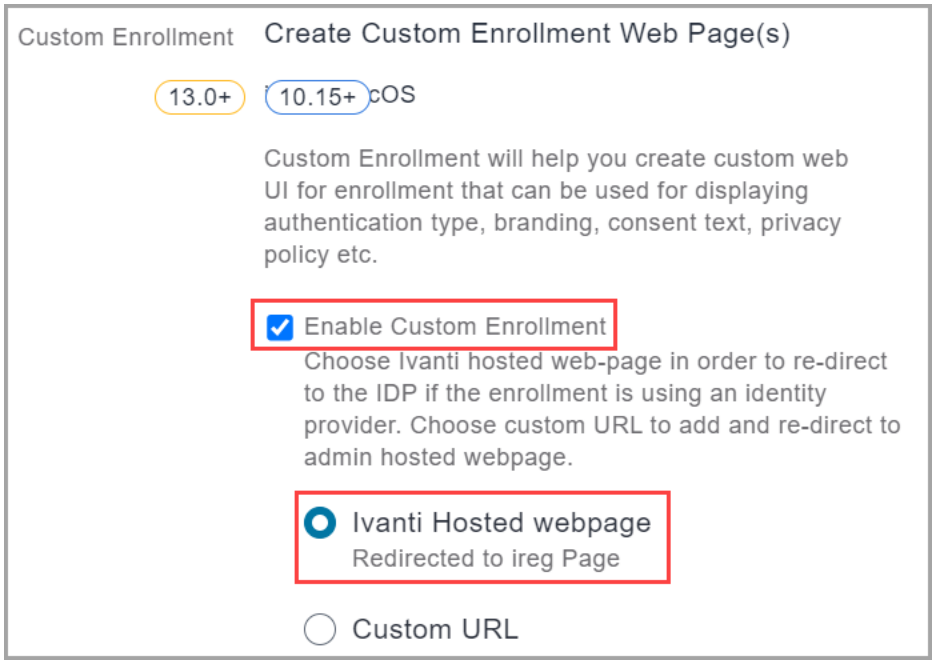
- Se você estiver usando Microsoft AD ou outro diretório LDAP local, será necessário configurar o Connector para se conectar e importar usuários do Ivanti Neurons for MDM. Configure o Connector ou o LDAP caso ainda não tenha feito.
- Quando um IdP é adicionado, a autenticação do usuário muda automaticamente de LDAP para IdP.
- Apenas um provedor IdP é permitido.
- Caso seu IdP fique inacessível, use a conta de Administrador de locatário (TA) do Ivanti Neurons for MDM para acessar esse Portal de administrador e solucionar problemas. O TA é uma conta local e não exige autenticação externa. A conta TA é criada quando seu Ivanti Neurons for MDM é provisionado e as informações são fornecidas ao contato técnico da sua organização ou equivalente. Se você não tiver as informações da sua conta de TA, entre em contato com seu representante de suporte.

- O Ivanti Neurons for MDM oferece suporte ao Azure Active Directory (Azure AD) da Microsoft para autenticação de usuários durante o registro de dispositivos Windows 10.

  Defina o tipo de autenticação para os usuários LDAP usando as ferramentas fornecidas pelo seu fornecedor de IdP. O esquema de autenticação de seu IdP terá precedência sobre as configurações do Ivanti Neurons for MDM. As definições de Autenticação do Ivanti Neurons for MDM podem ser encontradas aqui: **Usuários > Configurações do usuário > Configuração de registro do dispositivo > Tipo de autenticação do registro do dispositivo**.

- Os registros de dispositivos do Registro de dispositivos e Configurator da Apple não usam IdP na autenticação do usuário.

- Para configurar um provedor de identidade para funcionar no registro de dispositivos iOS e macOS do Apple Business Manager, você deve habilitar a opção **Ativar registro personalizado** e as configurações relacionadas da **página web hospedada da Ivanti**, localizadas em **Administrador > Apple > Registro de dispositivo >** *editar um perfil de registro de dispositivo*. Consulte "Registro de dispositivos" na página 1278 para mais informações:



Tipos de configuração de IdP

A página Identidade do Ivanti Neurons for MDM o guiará por meio da configuração dos seguintes tipos de provedores de IdP:

- **Configuração de IdP do Ivanti Neurons for MDM**- os provedores de identidade suportados no Ivanti Neurons for MDM são Azure AD, OneLogin, Okta e PingOne.
- **Configuração de IdP local** – os provedores de IdP local compatíveis são ADFS 3.0, PingFederate 8.2.1 e PingFederate 8.1.3.
- **Configuração de IdP genérico** – este é um caminho de configuração genérica que você poderá usar se não estiver utilizando Microsoft ADFS, Okta, OneLogin ou PingFederate.

Configuração de provedor de identidade (IdP)

Procedimento

1. Vá para **Administrador** > **Identidade** > **Autenticação SAML**.
2. Clique em um tipo de configuração do provedor de identidade:
   - **Configuração de IDP do Ivanti Neurons for MDM**
   - **Configuração de IDP local**
   - **Configuração de IdP genérico**
3. Selecione um IdP correspondente. Se você selecionou **Configuração de IdP genérico** na Etapa 3, pule esta etapa e vá para a Etapa 5.
4. Siga as instruções na tela em relação ao IdP escolhido.
5. Clique em **Concluído**.

Os administradores têm permissão para fazer login único por até duas horas a partir da autenticação inicial com o IdP.

Tarefas de configuração que devem ser concluídas

Dependendo do IdP escolhido, você será guiado pelas seguintes páginas e etapas associadas:

IdP	Procedimento
• Azure AD • Okta • OneLogin • PingOne	• Gerar uma chave para fazer o upload do seu IdP. • Fazer login em seu IdP e upload da chave gerada. • Exportar um arquivo de metadados do seu IdP e importá-lo no Ivanti Neurons for MDM.
• ADSF 3.0 • PingFederate 8.2.1 • PingFederate 8.1.3	• Baixe o arquivo de metadados do Ivanti Neurons for MDM. • Configurar uma "Terceira Parte Confiável" no ADFS ou uma "Conexão SP" no PingFederate e importar o arquivo de metadados do Ivanti Neurons for MDM. • Exportar o arquivo de metadados do seu IdP e importá-lo no Ivanti Neurons for MDM.

• IdP genérico	1. Baixe o arquivo de metadados do Ivanti Neurons for MDM. 2. Siga as instruções fornecidas pelo seu fornecedor IdP para configurar seu servidor ou serviço IdP para se comunicar com o serviço Ivanti Neurons for MDM como "Provedor de Serviços". Isso pode incluir: a. Transferir o arquivo de metadados da Etapa 1 acima para seu IdP. Esse arquivo de configuração contém as informações essenciais para que o Ivanti Neurons for MDM, como provedor de serviços SAML 2.0, se comunique com seu provedor de identidade SAML 2.0. As URLs, os certificados e as configurações padrão do SAML 2.0 estão incluídos no arquivo de metadados. Ivanti Neurons for MDM espera um IdP compatível com SAML 2.0 para conseguir importar e processar um metadado XML exportado de um Provedor de Serviços. b. Configurar seu IdP para usar RSA-SHA1 para assinar solicitações de autenticação de SAML. As informações sobre o Certificado de assinatura usado para verificar as solicitações de autenticação estão incluídas no arquivo de metadados baixado na Etapa 1. c. Configurar seu IdP para incluir um nome de usuário nas respostas SAML enviadas ao Ivanti Neurons for MDM. Especificar o nome de usuário no elemento [Id do nome] da resposta de SAML do IdP. 3. Exportar um arquivo de metadados do seu IdP e importá-lo no Ivanti Neurons for MDM. 4. (Opcional) - Incluir nome de usuário na solicitação de autenticação SAML: para incluir o nome do usuário a ser autenticado na solicitação de autenticação e remover uma entrada de usuário adicional ao autenticar com IdP. Se você habilitar esta opção, poderão ocorrer falhas de autenticação. Se tiver certeza sobre a validação do IdP, selecione a opção **Compreendo o impacto desta alteração** e alterne a configuração **Incluir nome de usuário na solicitação de autenticação SAML** para **ATIVADO**. O Ivanti Access é um IdP validado para esta configuração.

Permitir que usuários locais ignorem a autenticação de IdP

Quando um IdP ou a conectividade do Ivanti Neurons for MDM cai e se faz necessária resolução por meio do Ivanti Neurons for MDM, alguns administradores precisam fazer login no Ivanti Neurons for MDM sem depender de sistemas externos, como LDAP ou IdP, para autenticação. Somente usuários locais com funções de administrador do sistema podem ignorar a Autenticação IdP.

Crie uma lista de usuários locais para ignorar a autenticação IdP.

Procedimento

1. Clique em **Administrador > Identidade**.
2. Na seção Ignorar a autenticação IdP por usuários locais, clique em **+Adicionar usuários**.
3. Na lista exibindo somente os usuários locais com funções de administrador do sistema, selecione alguns usuários.
4. Clique em **Salvar**.

Para remover um usuário da lista de usuários locais que ignoram a autenticação de IdP, clique no ícone de remoção ao lado da entrada que deseja excluir.

Se você não conseguir visualizar a página Identidade, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Provisionamento de Usuários - Azure Active Directory

O Provisionamento de Usuários do Azure Active Directory (AAD) substituiu a Origem do Usuário AAD. O Provisionamento de Usuários Azure AD usa o protocolo SCIM para sincronizar o AAD com o Ivanti Neurons for MDM e permite sincronização parcial de usuários e grupos. O Provisionamento de Usuários Azure AD usa o protocolo SCIM para criar e atualizar automaticamente objetos de usuário e grupo originados do Azure AD para o Ivanti Neurons for MDM. Ivanti Neurons for MDM Os administradores podem optar por sincronizar todo o serviço de diretório ou objetos específicos de usuário e grupo com o Ivanti Neurons for MDM. Assim como a integração atual com o Azure AD, o processo de provisionamento de usuários e grupos é automatizado; se forem feitas alterações no usuário ou grupo no Azure AD, as mesmas alterações serão refletidas no Ivanti Neurons for MDM. A diferença mais importante é que o Provisionamento de Usuários do Azure AD agora permite que usuários e grupos específicos sejam provisionados. Isso fornece aos administradores controles mais rígidos para identificar quais usuários e grupos são adicionados, atualizados e desativados no Ivanti Neurons for MDM. A página Provisionamento de Usuários do Azure AD no portal administrativo do Ivanti Neurons for MDM exibe os estágios do fluxo de trabalho de migração de usuários e grupos de usuários do Azure AD para o Ivanti Neurons for MDM.

Como o valor do nome de usuário é único no Ivanti Neurons for MDM, o atributo Nome Principal do Usuário não pode ser atualizado no Azure AD se o usuário já estiver provisionado.

Esta seção contém os seguintes tópicos:

- "Gerar um token a partir do Ivanti Neurons for MDM" abaixo
- "Estabelecer a conexão entre Azure AD e Ivanti Neurons for MDM" na página seguinte
- "Provisionar usuários e grupos atribuídos" na página 1253
- "Provisionar todos os usuários e grupos" na página 1253
- "Verificar o provisionamento de um grupo" na página 1254

Gerar um token a partir do Ivanti Neurons for MDM

Para iniciar o Provisionamento de Usuários do Azure AD, gere um token e um URL de destino no Ivanti Neurons for MDM.

Certifique-se de salvar o token e o URL de destino.

No máximo dois tokens podem ser gerados a qualquer momento.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Vá para **Administrador** > **Identidade** > **Provisionamento de Usuários**.
3. Na lista suspensa **Escolher provedor de identidade (IdP)**, selecione **Azure AD**.
4. Para gerar um novo token, clique em **Gerar**. Uma mensagem de notificação é exibida, clique em **Gerar**. Uma nova página se abre com os detalhes do token e o URL do SCIM de destino.
5. Clique em **Copiar** para copiar o token ou o URL do SCIM.
6. Atualize a página. A página **Provisionamento de Usuários do Azure AD** exibe a tabela Status do Token.

Alterar o status do token no Ivanti Neurons for MDMIvanti Neurons for MDM

Você pode alterar o estado de um token existente.

Procedimento

1. Clique no menu suspenso **Selecionar** na página **Provisionamento de Usuários do Azure AD**.
2. Clique em **Selecionar** e faça as seguintes alterações no token:
   - **Definir como ativo**
   - **Definir como inativo**
   - **Renovar**
   - **Remover**

Estabelecer a conexão entre Azure AD e Ivanti Neurons for MDM

Após criar os usuários e os grupos em seu aplicativo Azure AD corporativo, será possível estabelecer a conexão entre o Azure AD e o Ivanti Neurons for MDM.

Considerações sobre migração

- Ao migrar de Origem do Usuário AAD para Provisionamento de Usuários AD (SCIM), selecione Sincronizar Todos os Usuários e Grupos.

- Depois que os usuários e grupos forem atualizados com uma fonte SCIM AAD, retorne à página Provisionamento do Azure no Azure e defina os usuários e grupos específicos a serem gerenciados pelo Provisionamento de Usuários do Azure AD usando a opção Sincronizar somente usuários e grupos atribuídos.
- Quando a sincronização estiver concluída, você poderá remover os usuários e grupos que não estão definidos no Azure das listas Usuários e Grupos do Ivanti Neurons for MDM.
- Quando a migração começa, a página Origem do Usuário AAD fica acessível em estado somente leitura.

Procedimento

1. Faça login no portal do Azure AD.
2. Acesse **Aplicativo corporativo** > clique em **+ Criar seu próprio aplicativo**. A janela Criar seu próprio aplicativo é aberta.
3. Especifique o nome do aplicativo (**padrão: Inexistente na galeria**) e clique em **Criar**. Por exemplo, Provisionamento de Usuários do Ivanti Neurons for MDM.
4. Acesse **Provisionamento** > **Editar provisionamento** > **Credenciais do administrador**.
5. Copie e cole o URL do SCIM de destino do portal administrativo do Ivanti Neurons for MDM no campo **URL do locatário** no portal do Azure AD.
6. Copie o Token do Ivanti Neurons for MDM e cole-o no campo **Token secreto** no portal do Azure AD.
7. Execute uma das seguintes etapas:
   a. Selecione **Sincronizar apenas usuários e grupos atribuídos**. Para mais informações, consulte Provisionar usuários e grupos atribuídos
   b. Selecione **Sincronizar todos os usuários e grupos**. Para mais informações, consulte Provisionar todos os usuários e grupos.

      Selecione a opção Sincronizar todos os usuários e grupos para migrar usuários.
8. Clique em **Testar conexão**. Um pop-up com um visto verde confirma a conexão.
9. Clique em **Salvar**.

Procedimento

1. Expanda **Mapeamentos** na página **Provisionamento**, no portal do Azure AD.

2. Clique em **Provisionar usuários do Azure Active Directory**. A página Mapeamento de Atributos é aberta.
3. Clique em **Excluir** nos atributos não suportados.

Provisionar usuários e grupos atribuídos

Após a conexão entre Azure AD e Ivanti Neurons for MDM ser estabelecida, você pode provisionar usuários ou grupos.

Ao provisionar grupos, o Azure AD não adiciona membros de grupos aninhados ao grupo selecionado. O Azure AD adiciona ao grupo somente nomes de grupos e membros imediatos, e não membros de subgrupos, durante o processo de sincronização.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. No aplicativo, vá para **Usuários e grupos** > clique em **+ Adicionar usuário/grupo**. A página Adicionar atribuição se abre.
3. Procure o usuário ou grupo no campo **Pesquisar**, clique em **Selecionar** e depois em **Atribuir**. A página Usuários e grupos se abre.
4. Marque a caixa de seleção do usuário ou grupo correspondente.
5. Clique em **Provisionamento** e, em seguida, clique em **Iniciar o provisionamento**. Os detalhes da configuração bem-sucedida são exibidos.

Provisionar todos os usuários e grupos

Apos a conexão ser estabelecida entre o Azure AD e o Ivanti Neurons for MDM, você pode provisionar usuários ou grupos.

Procedimento

1. Clique em **Provisionamento** e, em seguida, clique em **Iniciar o provisionamento**. A página se abre com os detalhes do provisionamento bem-sucedido, e o usuário será provisionado no Ivanti Neurons for MDM.

Verificar o provisionamento de um usuário atribuído

Após um usuário atribuído ser provisionado no portal do Azure AD, verifique o provisionamento no portal administrativo do Ivanti Neurons for MDM.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse a guia **Usuários** no menu principal. O usuário provisionado estará presente na lista de usuários nesta página.

   O processo de provisionamento pode levar até uma hora.

Verificar o provisionamento de um grupo

Após um grupo ser provisionado no portal do Azure AD, verifique o provisionamento no Ivanti Neurons for MDM.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse a guia **Usuários** > **Grupos de usuários**. O grupo provisionado estará presente na lista de grupos nesta página.

   O processo de provisionamento pode levar até uma hora.

Editar Configurações

Este tópico ajuda você a definir as configurações do Azure Active Directory.

Procedimento

1. Acesse **Administrador > Microsoft Azure > Provisionamento de Usuários Azure AD**.
2. Clique em **Gerar token** e copie o token.
3. Atualize a página. A página Editar Configurações é exibida.
4. Clique em **Editar configurações**.
5. Defina **Convidar automaticamente usuários importados do AAD**: gerencie se os usuários importados do AAD para o Ivanti Neurons for MDM serão automaticamente convidados a se registrar via e-mail.
6. Defina **ID Apple gerenciado**: escolha sincronizar o ID Apple Gerenciado para os usuários do AAD.
    - **Nenhum**
    - **Padrão:** endereço de e-mail do usuário.
        - (Opcional) Selecione a opção Incluir subdomínio "appleid" para evitar conflitos com os IDs Apple existentes.
7. (Opcional) Clique em **Adicionar atributos personalizados**: especifique atributos de usuário personalizados do serviço de diretório para aplicar ao gerenciamento de dispositivos. Cada atributo poderá então ser referenciado por ${attributeName} nos campos de configuração compatíveis com variáveis. O uso desta opção exibe uma implementação consistente de atributos personalizados em servidores AAD. Se um servidor AAD incluído em sua implementação não utilizar esse atributo, os recursos dependentes desse atributo poderão não funcionar conforme esperado. A coluna **Tipo de Atributo** exibe o atributo **IDP** na tabela **Atributos Personalizados** na seção **Editar Configurações**.
8. Clique em **Salvar alterações** após modificar as configurações do AAD.

Configurar atributos no provisionamento de usuários SCIM

Esta seção descreve como criar atributos personalizados e corporativos para o Azure AD durante o provisionamento de usuários.

Mapeando atributos

Após a conexão ser estabelecida, você pode mapear os atributos entre Azure AD e Ivanti Neurons for MDM. Ivanti Neurons for MDM oferece suporte aos seguintes atributos do Azure AD:

Atributos principais

- id(urn:ietf:params:scim:schemas:core:2.0:id)
- userName("urn:ietf:params:scim:schemas:core:2.0:User:userName")
- displayname("urn:ietf:params:scim:schemas:core:2.0:User:displayName")
- active("urn:ietf:params:scim:schemas:core:2.0:User:active")
- name("urn:ietf:params:scim:schemas:core:2.0:User:name")
- userType(urn:ietf:params:scim:schemas:core:2.0:User:userType)
- emails(urn:ietf:params:scim:schemas:core:2.0:User:emails)
- locale("urn:ietf:params:scim:schemas:core:2.0:User:locale")

Lista de atributos para os quais a operação de atualização é permitida

- displayName
- emails
- nome
- ativo
- id
- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User

Atributo personalizado

Esquema - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

Atributo empresarial

Atualmente, apenas o atributo Departamento é suportado.

Esquema - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Navegue até **Administrador** > **Identidade** > **Provisionamento de Usuários**.
3. Em **Editar configurações**, clique em **+Adicionar atributo personalizado**
4. Digite um nome no campo **Nome do atributo**.
5. Clique em **Salvar alterações**.
6. O atributo é listado e disponibilizado na página Administrador > Sistema > Atributo.
7. O atributo é indicado como tipo IDP, e você só pode executar a ação de exclusão.
8. Faça login no portal do Azure AD.
9. Acesse **Início** > **Aplicativo corporativo** > clique no aplicativo SCIM.
10. Clique em **Provisionar usuários do Azure Active Directory** na seção **Mapeamentos**.
11. Marque a caixa de seleção **Mostrar opções avançadas**.
12. Clique em **Editar lista de atributos para aplicativos personalizados**.
13. Insira uma nova entrada para o atributo personalizado que você criou na interface do usuário do Ivanti Neurons for MDM.
14. Adicione o esquema para o atributo Personalizado/Empresarial (Departamento) da seguinte forma:
    Atributo personalizado - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<atributo personalizado>**

    Atributo empresarial - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
15. Clique em **Salvar alterações**.

16. Clique em **Adicionar novo mapeamento** e selecione os atributos Origem e Destino no menu suspenso:
17. Clique em **Ok** e clique em **Salvar mapeamento**.
18. Acesse **Início** > **Aplicativo corporativo** > clique no aplicativo SCIM > **Usuários e grupos**.
19. Clique no nome do usuário. A página Perfil se abre.
20. Verifique se o valor associado ao atributo aparece na página Perfil.
21. (Opcional) Clique no aplicativo SCIM > **Provisionamento** > **Provisionar sob demanda**, procure o usuário específico e clique em **Provisionamento**. Para validar os novos mapeamentos de atributo realizados nas etapas anteriores.
22. Faça login no portal administrativo do Ivanti Neurons for MDM.
23. Acesse **Usuários** > **Usuários**.
24. Selecione o usuário, clique na guia **Atributos** e verifique o valor do atributo. O atributo é mapeado para o usuário específico.

Tópicos relacionados:

"Provisionamento de Usuários - Azure Active Directory " na página 1250

"Atributos" na página 1164

Administrador > Infraestrutura > LDAP

Licença: Silver

Configurar um servidor LDAP e um Connector permite que você importe usuários e grupos do seu diretório corporativo. Após instalar pelo menos um Connector, adicione um ou mais servidores LDAP.

Adicionar um servidor LDAP significa a configuração:

- a *conexão* ao servidor LDAP
- os *termos de pesquisa* necessários para visualizar os dados do diretório de destino
- a parte do diretório para *importar*
- se ou não *convidar usuários* automaticamente na parte selecionada do diretório

Depois de adicionar um servidor LDAP, você pode retornar a essa página para editar as informações do servidor LDAP ou alterar os usuários LDAP selecionados.

Os usuários LDAP devem ser importados após a configuração de um usuário LDAP. Veja Importação de usuários LDAP.
Nomes de usuário LDAP, como os nomes de usuário locais, devem ser globalmente exclusivos. Verifique se os usuários já não possuem uma conta local com o mesmo nome de usuário ou, para organizações com mais de um locatário, se os nomes de usuários já não foram associados a outro locatário.

Como adicionar um servidor LDAP

Procedimento

1. Clique em **+Adicionar servidor**.
2. Forneça as seguintes informações:

Configuração	O que fazer
Nome	Insira um nome que identifique esse servidor.
Descrição	Insira uma descrição que esclareça o propósito desse servidor.
URL do diretório	Insira a URL para o diretório. Use um dos seguintes formatos: ldap://endereço IP ou ldaps://endereço IP ou Por exemplo: ldap://meuservidor1.minhaempresa.com:389
ID do usuário	Insira a ID do usuário para uma conta com as seguintes características: • gerenciada pelo servidor LDAP • pode ser vinculada ao servidor LDAP e pesquisar subárvores para usuário, grupo e unidade organizacional Normalmente, esta é uma conta com Credenciais do Administrador do Diretório (DN ou nome distinto e senha).
Senha	Insira a senha para a conta.
Confirmar senha	Insira novamente a senha para a conta.
Tipo de diretório	Selecione o tipo de diretório da lista de diretórios suportados. • Microsoft Active Directory • Abrir LDAP • Outros (compatível com LDAP aberta)

3. Clique em **Testar conexão e continuar**.

   Essa etapa valida as informações já fornecidas.

- Se as informações forem válidas, o serviço recupera o contexto do nome LDAP, utilizado para preencher alguns dos campos da próxima página.
- Se a URL do LDAP não conseguir se conectar, siga as etapas a seguir. Entretanto, elas podem resultar em uma funcionalidade limitada até que o problema de conexão seja resolvido.

4. Conclua as configurações restantes:

Configuração	O que fazer
URL de failover do diretório	Insira a URL para o diretório secundário. Use o seguinte formato: ldap://endereço IP ou Por exemplo: ldap://meuservidor2.minhaempresa.com:389
Intervalo de sincronização	Insira o tempo entre cada tentativa de sincronização dos dados do LDAP do servidor LDAP. O tempo padrão é 15 minutos. Considere aumentar o intervalo depois de ter sincronizado com sucesso todos os dados do LDAP de destino e confirmado que sua configuração LDAP atende às suas necessidades.
Habilitar Descarte da sincronização	Selecione para descartar automaticamente os dados da sincronização do LDAP se o conjunto de dados recarregados cair significantemente. Essa opção garante que comportamentos anormais do sistema LDAP não resultem em atualizações inoportunas e desnecessárias no serviço e na remoção de configurações dos dispositivos registrados. Verifique se essa opção não está selecionada se você planeja fazer grandes mudanças na configuração LDAP ou no servidor LDAP.
Habilitar este servidor LDAP	Selecione para usar esse servidor LDAP com seu serviço. Exclua essa configuração caso deseje desativar esse servidor LDAP ou retirá-lo do serviço. Embora um failover configurado para um segundo servidor LDAP substitua automaticamente esse servidor, usar essa opção permite o planejamento com antecedência e evita uma breve falta de conectividade durante o failover.
Convide os usuários automaticamente sempre que forem importados	Selecione para enviar convites automaticamente aos usuários quando eles forem importados de um servidor LDAP.

Fazer upload do Certificado da CA	Clique em **Escolher arquivo** para carregar o certificado TLS emitido pela CA instalada neste servidor LDAP. Você pode carregar vários certificados CA.
Buscar indicações	Aplica-se somente se você estiver usando um domínio com várias florestas. Essa opção indica se você deseja usar controladores de domínio alternados quando o controlador de domínio de destino não tiver uma cópia do objeto solicitado. • Selecione **Seguir** se quiser usar indicações. • Selecione **Ignorar** se não quiser usar controladores de domínio alternativos. • **Lançar** possui o mesmo efeito que **Ignorar**. Selecionar **Seguir** atrasa a autenticação LDAP.
Tempo limite dos resultados da pesquisa	Aumente esse tempo limite se você perceber problemas de desempenho ou resultados incompletos ao pesquisar os dados sincronizados do servidor LDAP.
Contagem dos resultados da pesquisa	Configure para o número máximo de registros que devem ser retornados do servidor LDAP por vez. Cenários que podem exigir alterações nessa configuração para aprimorar o desempenho incluem: • O servidor LDAP está longe ou protegido por um link de latência alta. Nesse caso, resultados grandes de pesquisas demorarão mais para serem recuperados do que os resultados pequenos. Por isso, uma configuração menor permite que você veja subconjuntos de dados atualizados mais rapidamente. • O LDAP é muito grande, e cada pesquisa retorna um conjunto de resultados enorme. Nesse caso, se o desempenho não for um problema, uma configuração de resultados maior possibilitaria o retorno de todos os dados com uma quantidade menor de pesquisas.

5. Clique em **Avançar**.
6. Use as diretrizes a seguir para configurar a integração com o servidor LDAP:

Configuração	O que fazer
Formato do membro do grupo	Selecione **DN** ou **UID** para indicar se você deseja ou não utilizar o nome distinto ou a ID do usuário na pesquisa.
Atributos de pesquisa de OU	Especifique os critérios para pesquisar no nível da unidade organizacional.
DN de base	Insira o nome distinto para o nível inicial que você deseja que sua pesquisa seja iniciada. Suas seleções determinam os padrões para vários outros campos, que, se você quiser, podem ser alterados.
GUID do objeto	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP. Este é o atributo que identifica uma unidade organizacional de forma exclusiva em mudanças de nome de OU e horário.
Nome do atributo	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Descrição	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
DN do atributo	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Filtro de pesquisa	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Escopo da pesquisa	Selecione a parte da hierarquia LDAP para direcionar: • **Base** (somente o nível da entrada base da pesquisa) • **Um nível** (o nível abaixo da base da pesquisa) • **Subárvore** (a subárvore na árvore de informações do diretório abaixo da base de pesquisa DN)
Atributos da pesquisa de usuário	Especifique os critérios para pesquisar usuários em um nível de diretório especificado.

DN de base	Insira o nome distinto para o nível inicial que você deseja pesquisar.
UID do atributo	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
GUID do objeto	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP. Este é o atributo que identifica um usuário de forma exclusiva em mudanças de nome de usuário e horário.
DN do atributo	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Nome	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Sobrenome	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Nome de exibição	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Endereço de e-mail	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Nome principal	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Local	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Membro de	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Filtro de pesquisa	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.

Escopo da pesquisa	Selecione a parte da hierarquia LDAP para direcionar: • **Base** (somente o nível da entrada base da pesquisa) • **Um nível** (o nível abaixo da base da pesquisa) • **Subárvore** (a subárvore na árvore de informações do diretório abaixo da base de pesquisa DN)
ID Apple gerenciado	Escolha sincronizar o Apple ID gerenciado para os usuários LDAP. • **Nenhum** • **Padrão**: endereço de e-mail do usuário. Opcionalmente, selecione a opção **Incluir subdomínio "appleid"** para evitar conflitos com os Apple IDs existentes.
+Adicionar atributo personalizado	(Opcional) Especifique até 7 atributos personalizados de usuário do serviço de diretório aos quais você gostaria de aplicar o gerenciamento de dispositivos. Cada atributo poderá então ser referenciado por ${attributeName} nos campos de configuração que suportam variáveis. **Importante:** o uso desta opção requer a implementação consistente de atributos personalizados nos servidores LDAP. Se um servidor LDAP incluído em sua implementação não utilizar esse atributo, os recursos que dependem desse atributo podem não funcionar conforme esperado.
Atributos da pesquisa de grupo	
DN de base	Insira o nome distinto para o nível inicial que você deseja pesquisar.
GUID do objeto	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP. Este é o atributo que identifica um grupo de forma exclusiva em mudanças de nome de grupo e horário.

DN do atributo	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Nome do atributo	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Descrição	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Membro	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Filtro de pesquisa	Se necessário, altere o valor padrão para corresponder com seu ambiente LDAP.
Escopo da pesquisa	Selecione a parte da hierarquia LDAP para direcionar: • **Base** (somente o nível da entrada base da pesquisa) • **Um nível** (o nível abaixo da base da pesquisa) • **Subárvore** (a subárvore na árvore de informações do diretório abaixo da base de pesquisa DN)

7. Clique em **Navegar** ou em **Pesquisar**.
8. Confirme que a sua configuração retorna os dados esperados.

   Você pode fazer isso navegando ou pesquisando um item conhecido no diretório.
9. Clique em **Avançar**.

Excluir um atributo LDAP personalizado

Você pode excluir um atributo LDAP personalizado e remover seus valores dos usuários ou dispositivos associados.

Procedimento

1. Vá para **Administrador > Atributos**.
2. Na seção **Atributos personalizados** clique no link **Excluir** ao lado do atributo LDAP que deve ser excluído. Uma janela de confirmação é exibida.

3. Clique em **Excluir** para confirmar a exclusão.

> que o botão **Excluir** está desabilitado por padrão. Você deve selecionar a caixa de seleção na opção **Eu entendo que a exclusão de um atributo personalizado não poderá ser revertida** para habilitar o **botão** Excluir.

Editar as informações do servidor LDAP

Procedimento

1. Acesse **Administrador > LDAP**.
2. Na entrada do servidor LDAP, selecione o ícone **Editar** da coluna **Ações** para visualizar a página Conectar servidor LDAP.
3. Faça as alterações necessárias.
4. Clique em **Testar conexão e continuar**.
   Se o URL do LDAP não conseguir se conectar, siga as etapas a seguir. Entretanto, elas podem resultar em uma funcionalidade limitada até que o problema de conexão seja resolvido.
5. Clique em **Navegar** ou em **Pesquisar**.
6. Confirme que a sua configuração retorna os dados esperados.
   Você pode fazer isso navegando ou pesquisando um item conhecido no diretório.
7. Clique em **Concluído**.

Importar usuários LDAP

Procedimento

1. Acesse **Usuários**.
2. Clique em **+Adicionar > Convidar usuários do LDAP**.
3. Clique em **Selecionar usuários** na entrada do servidor LDAP.
4. Na página Adicionar usuários LDAP, insira o nome do usuário, grupo ou OU no campo de busca.
5. Para adicionar novos usuários ou grupos, clique em **+Adicionar** ao lado da entrada que deseja adicionar.

6. Clique em **Avançar**.
7. Escolha se deseja ou não enviar o convite:
   - Não convidar nenhum
     Para enviar os convites mais tarde, acesse **Usuários > Usuários** e selecione **Ações > Enviar convite** para enviar os convites.
   - Convidar todos
8. Clique em **Concluído**.

Atualizar usuários, grupos ou unidades organizacionais selecionadas

Procedimento

1. Acesse **Administrador > LDAP**.
2. Na entrada do servidor LDAP, selecione o ícone **Gerenciar usuários** da coluna **Ações** para visualizar a página Adicionar usuários LDAP.
3. Para adicionar novos usuários ou grupos, insira o nome do usuário ou grupo no campo de busca.
4. Clique em **Adicionar** ao lado da entrada que deseja adicionar.
5. Para remover um usuário, grupo ou OU, clique no ícone Remover ao lado da entrada que deseja excluir.
6. Clique em **Concluído**.

Habilitar a Notificação de descarte de sincronização do LDAP

Descartar a notificação de descarte de sincronização LDAP ajuda a evitar interrupções causadas por alterações acidentais em grande escala no ambiente LDAP.

Procedimento

1. Acesse **Administrador > LDAP**.
2. Na entrada do servidor LDAP, selecione o ícone **Editar** da coluna **Ações** para visualizar a página Conectar servidor LDAP.
3. Marque a caixa de seleção **Habilitar descarte da sincronização**.

4. Insira um valor para a porcentagem dos dados do LDAP recarregados para acionar o descarte da sincronização.

5. Clique em **Testar conexão e continuar**.
   Se a URL do LDAP não conseguir se conectar, siga as etapas a seguir. Entretanto, isso pode resultar em uma funcionalidade limitada até que o problema de conexão seja resolvido.

6. Clique em **Concluído**.

7. Clique no ícone **Sincronizar agora** na entrada do servidor LDAP.
   Quando a diferença de mudança a ser sincronizada do LDAP com o Ivanti Neurons for MDM superar a porcentagem de descarte estabelecida, uma notificação de ALERTA será gerada. Quando as alterações são revertidas para um valor abaixo da porcentagem estabelecida, a notificação é EXCLUÍDA.

Indicador	Severidade	Tipo de notificação	Tipo de componente	Componente
Descarte da sincronização LDAP	Aviso	Sincronização de dados	LDAP	Nome do servidor LDAP
Sincronização LDAP restaurada	Informações	Sincronização de dados	LDAP	Nome do servidor LDAP

A Notificação de descarte de sincronização parcial é gerada quando um ou mais registros de usuário não são sincronizados do LDAP. Neste caso, um arquivo CSV é incluso como anexo com uma lista de usuários que não fizeram a sincronização. Se um usuário foi descartado devido a atributos ausentes, a lista de atributos ausente também é inclusa no arquivo CSV exportado.

Sincronizar alterações do servidor LDAP

Na página do LDAP, clique no ícone **Sincronizar agora** na entrada do servidor LDAP.

Resolução de problemas de conectividade com o servidor LDAPS

Se estiver tendo dificuldades para se conectar ao servidor LDAPS (LDAP sobre SSL), você pode estar com problemas no seu certificado.

Para resolver o problema:

- Verifique se você não está usando um certificado autoassinado no Servidor LDAPS.
- Verifique se o certificado LDAPS ainda não expirou ou foi revogado. Também verifique se há problemas de correspondência com o nome do host.

Após a verificação, aguarde a sincronização automática do LDAP ou sincronize manualmente usando o ícone **Administrador > LDAP > Sincronizar agora** na entrada do servidor LDAP.

Se você não conseguir visualizar a página LDAP, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Sentry

O Sentry é um componente que atua como um gateway entre dispositivos móveis e seu sistema de e-mail do usuário habilitado para o ActiveSync. Use o Sentry para controlar quais dispositivos podem acessar o e-mail. Está disponível para download como um arquivo ISO que pode ser instalado em uma máquina virtual. As organizações devem as considerar o uso de um balanceador de carga para manter vários Sentrys (redundantes).

Licença: Silver

Documentação mais recente

Para obter as instruções mais recentes do Sentry, acesse Documentação do produto e clique em Sentry.

Para obter as instruções mais recentes de instalação do Sentry, selecione a versão adequada do *Guia de instalação presencial do Standalone Sentry*.

Para obter as instruções de upgrade do Sentry, selecione a versão adequada do *Guia do Sentry*. Veja as seguintes seções do Guia do Sentry:

- Para instruções de atualização usando a UI de gerenciador de sistema do Standalone Sentry, veja "Atualizações de software do Standalone Sentry".
- Para instruções de atualização usando a interface da linha de comando (CLI) do Standalone Sentry, veja "Atualização usando a CLI".

Antes de fazer a atualização, veja as notas de versão do Standalone Sentry para a nova versão que você vai instalar.

Configurações da Apple

Esta seção contém os seguintes tópicos:

Apple Configurator

Você pode usar esta página para preparar o Apple Configurator para configurar o gerenciamento de dispositivos do Ivanti Neurons for MDM em dispositivos iOS. O Apple Configurator facilita muito a implantação de dispositivos com iOS em grandes quantidades. Além disso, o Configurator permite que os administradores tornem os dispositivos com iOS supervisionados, o que permite níveis maiores de recursos de configuração e gerenciamento. Para obter mais informações sobre o Apple Configurator, consulte a Mac App Store.

As etapas básicas são:

1. Exporte o perfil MDM a partir de seu locatário do Ivanti Neurons for MDM.
2. Importe o perfil MDM no Configurator.
3. Use o Configurator para aplicar o perfil MDM em dispositivos presos.

Definição de um usuário padrão para dispositivos

Os dispositivos configurados por meio do Apple Configurator são atribuídos ao usuário Ninguém no Ivanti Neurons for MDM, a menos que você selecione um usuário diferente:

1. Clique no campo **Atribuir dispositivos configurados a**.
2. Comece a inserir o nome do usuário do Ivanti Neurons for MDM que você deseja selecionar.
3. Selecione o nome de usuário quando ele aparecer na lista suspensa.
4. Clique em **Salvar**.

Instalação de apps usando o Apple Configurator

Antes de usar o Apple Configurator para instalar apps:

- O acesso à app Store da Apple é restrito pela configuração do dispositivo.
- A instalação de apps é permitida pela configuração do dispositivo.
- O Apple Configurator deve ser instalado no computador usado para configurar os dispositivos.

Para instalar apps usando o Apple Configurator:

1. No Ivanti Neurons for MDM, acesse **Administrador > Apple Configurator**.
2. Alterne o switch de alternância dos dispositivos de registro para Ativado.
3. Clique em uma das opções a seguir:
   - **Plist do usuário padrão**.
   - **Plist do usuário específico** – Insira o nome de usuário ou ID de email do usuário específico.
4. No Apple Configurator, acesse **Preparar > Apps**.
5. Acesse **Preparar > Configurações e desative a opção Supervisão**.
6. Selecione a opção **Nunca atualizar o dispositivo** em Atualizar iOS.
7. Clique em **Preparar** (parte inferior do Apple Configurator).
   Os apps ficarão visíveis na lista de apps instalados no dispositivo após o registro do dispositivo.

Instalação de apps usando o servidor UEM

Para instalar apps usando o servidor UEM:

1. Faça upload de um aplicativo a partir da loja interna na guia Apps.
2. Selecione o aplicativo.
3. Clique na guia **Configurações de aplicativo**.
4. Selecione **Instalar no dispositivo**.
   Conclua as definições das configurações.
5. Selecione **Ações > Forçar registro**.

O que o usuário final precisa fazer

A Apple exige que o usuário final abra o Go pelo menos uma vez, caso contrário o recurso de local do Ivanti Neurons for MDM não funcionará corretamente. Isso serve para garantir que o usuário final esteja ciente que sua localização está sendo monitorada.

Cuidado: se os dispositivos forem implantados no modo de aplicativo único usando o Configurador, essa abordagem não será possível.

Se você não conseguir visualizar a página **Instalando o Apple Configurator**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Registro de dispositivos

O Registro de Dispositivos faz parte do Apple Business Manager, que permite que os clientes comprem dispositivos em massa e os registrem automaticamente no MDM durante a ativação. Se optar por participar, você poderá usar o Ivanti Neurons for MDM como o servidor de MDM para gerenciar esses dispositivos. Para obter mais informações, consulte https://business.apple.com/.

Como conectar o Ivanti Neurons for MDM ao Registro de dispositivos

Para utilizar o Ivanti Neurons for MDM como servidor MDM para Registro de dispositivos, configure o token do servidor do Apple Business Manager no Ivanti Neurons for MDM.

Para cada servidor do Apple Business Manager, o Ivanti Neurons for MDM disponibiliza as seguintes ações:

- Testar conexão
- Adicionar perfil do Registro de dispositivos
- Baixar chave pública
- Sincronização total de registro de dispositivo – Iniciar sincronização total. Pode demorar um pouco para concluir. Depois de concluída a sincronização, é possível visualizar as informações na coluna Última sincronização. Não é possível iniciar a sincronização total se ela já estiver em andamento.
- Fazer upload de novo token
- Excluir

As ações **Editar autenticação** e **Atribuir atributo de dispositivo de registro de dispositivo** agora estão disponíveis para perfis de registro de dispositivo em vez de registro de dispositivo (servidor MDM).

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Clique em **Baixar a chave**.
3. Salve sua chave do Ivanti Neurons for MDM.
4. Clique em **business.apple.com**.

5. Faça login usando suas credenciais Apple qualificadas para o Registro de dispositivos.
6. No site de Registro de dispositivos da Apple:
    a. Clique em **Começar**.
    b. Selecione o telefone de confiança para ser utilizado na autenticação do serviço da Apple.
    c. Insira o código de verificação enviado ao telefone selecionado.
    d. Clique em **Adicionar servidor MDM**.
    e. Insira um nome para identificar o servidor MDM virtual que será utilizado com o serviço.
    f. Clique em **Avançar**.
    g. Faça o upload da chave pública baixada anteriormente.
    h. Clique em **Avançar**
    i. Clique em **Seu token do servidor** para baixar o token.
    j. Clique em **Concluído**.
7. Em Ivanti Neurons for MDM, clique em **Carregar**.
8. Clique em **Avançar**.

9. Selecione uma opção de autenticação:

   - **Pedir que o usuário faça o registro/login**

     Será solicitado que os usuários forneçam nome de usuário e senha. Os usuários podem inserir uma senha ou um PIN no campo de senha. As preferências de senha e PIN podem ser configuradas em Usuários > **Configurações de usuário** relacionadas à autenticação.

   - **Ignorar login do usuário**.

     Os dispositivos designados a um usuário específico ou que não foram designados a ninguém (anônimos) podem ser redesignados a usuários específicos posteriormente na página **Dispositivos**.

     Selecione uma das opções a seguir:

     - **Definir um usuário para designar todos os dispositivos**
     - **Designar todos os dispositivos a um usuário anônimo**

   A opção selecionada substitui as seleções em Configurações do usuário.

10. Clique em **Upload** para instalar a chave recebida na Etapa 3.
11. Preencha o formulário exibido para definir o perfil para seus dispositivos no Registro de dispositivos:

Configuração	O que fazer
Nome	Insira um nome que identifique esse perfil de Registro de dispositivos.
Descrição	Insira uma descrição para o perfil.
Departamento	Insira o departamento na sua organização associado a este perfil.
Modo supervisionado	Permite o controle administrativo adicional das configurações e restrições. Para dispositivos iOS 13+ e macOS 10.15+, essa opção é ativada por padrão.
Baixar e instalar automaticamente as atualizações do iOS	(Somente iOS 9.0 ou superior) As atualizações do sistema operacional serão baixadas automaticamente (mas não instaladas), mesmo com a opção de perfil de Registro de dispositivos desativada, caso a opção Downloads Automáticos esteja selecionada no dispositivo em **Ajustes > iTunes e App Store**. Essa configuração terá preferência quando houver uma configuração de Atualizações de software do iOS aplicáveis aos dispositivos supervisionados registrados pelo Registro de dispositivos. Qualquer mudança nessa configuração será aplicável ao dispositivo supervisionado registrado pelo Registro de dispositivos, mesmo sem reiniciar o dispositivo.

Configuração	O que fazer
MDM removível	Define se o usuário poderá cancelar o registro do MDM após o registro do dispositivo. Esta configuração não é aplicável para iPads compartilhados.
MDM obrigatório	Define se o usuário poderá ignorar a instalação do MDM durante o processo de ativação. Para dispositivos iOS 13+ e macOS 10.15+, essa opção é ativada por padrão.
Permitir pareamento	(Não aplicável para iOS 13+ e macOS 10.15+) Permite funções de emparelhamento de host, como sincronização do iTunes. O pareamento é sempre permitido para hosts que têm certificados de pareamento válidos.
Certificado	Clique em **+ Adicionar** para carregar os certificados.
Número do telefone do suporte	Forneça um número de telefone que os usuários do dispositivo possam usar caso precisem de ajuda.
Endereço de E-mail do Suporte	Forneça um endereço de e-mail que os usuários do dispositivo possam usar caso precisem de ajuda.

Configuração	O que fazer
Registro personalizado	(iOS 13.0+ e macOS 10.15+) Crie páginas web de registro personalizadas. Especifique sua própria página web personalizada (web view) para autenticar usuários durante o Registro do dispositivo. Use esta página para exibir informações personalizadas, como tipo de autenticação, identidade visual, texto de consentimento e política de privacidade. Veja a seção "*Adicionando uma página web personalizada de Registro de dispositivos*" seguindo este procedimento para obter mais detalhes. • Selecione **Ativar registro personalizado** para ativar esse recurso. • Digite o **URL**, como https://mycustomweburl.com. Este URL define o valor do URL personalizado a ser apresentado ao usuário em uma web view.

Configuração	O que fazer
Vários usuários	(iOS 13.4+) iPad compartilhado para empresas Permite que as empresas compartilhem dispositivos entre vários funcionários, ao mesmo tempo em que proporciona uma experiência personalizada. Selecione o **Modo multiusuário** para habilitar o iPad compartilhado neste dispositivo. Para obter mais informações, consulte iPad compartilhado para empresas. • Esta configuração não é aplicável para Educação da Apple. • Selecione a configuração **Modo supervisionado** para modificar a configuração Multiusuário.
Tamanho da cota	(iOS 13.4+) iPad compartilhado para empresas. O valor em megabytes (MB) denota o armazenamento alocado para um usuário em um dispositivo. Se o valor for muito pequeno, um tamanho de cota padrão é alocado pelo dispositivo.

Configuração	O que fazer
Usuários residentes	(iOS 13.4+) iPad compartilhado para empresas O valor denota o número de usuários que podem permanecer ou residir no dispositivo. Se o valor for maior do que o número máximo de usuários que o dispositivo suporta, o servidor MDM usará esse valor (número máximo de usuários) como um padrão. Os administradores podem fornecer tanto o valor do tamanho da cota quanto dos usuários residentes. Se ambos os valores forem fornecidos, o servidor MDM usa o tamanho de cota como padrão.

Configuração	O que fazer
Tempo limite de sessão do usuário	(iOS 14.5+) iPad compartilhado para empresas Exibe o tempo limite em segundos para uma sessão de usuário. A sessão do usuário faz o logout automaticamente após o período de inatividade especificado. O valor mínimo de é 30 segundos. Definir este valor como 0 remove o tempo limite e define o tempo limite padrão do dispositivo. Valores entre 1 e 29 são inválidos. Quando configurado, o dispositivo é definido para o tempo limite padrão.

Configuração	O que fazer
Tempo limite de sessão temporária	(iOS 14.5+) iPad compartilhado para empresas Exibe o tempo limite em segundos para uma sessão temporária ou de convidado. A sessão temporária faz o logout automaticamente após o período de inatividade especificado. O valor mínimo de é 30 segundos. Definir este valor como 0 remove o tempo limite e define o tempo limite padrão do dispositivo. Valores entre 1 e 29 são inválidos. Quando configurado, o dispositivo é definido para o tempo limite padrão.
Somente sessão temporária	(iOS 14.5+) iPad compartilhado para empresas Se verdadeiro, o usuário visualiza apenas o painel de boas-vindas ao convidado e só pode fazer o login como usuário convidado. Se falso, o usuário pode fazer login com um ID Apple gerenciado (o comportamento existente). Padrão: falso

Configuração	O que fazer
Domínios Padrão de ID Apple Gerenciado	(iOS 16.0+) iPad compartilhado para empresas Especifique uma lista de domínios. Os usuários podem selecionar o domínio da conta a partir da lista de domínios no teclado QuickType.
Período de tolerância da autenticação on-line	(iOS 16.0+) iPad compartilhado para empresas Especifique quantos dias o usuário pode fazer login sem se conectar à rede. Definir esse valor como zero impõe sempre a autenticação on-line. **Padrão**: 0
Fuso horário	Especifique o fuso horário ao qual o dispositivo deve pertencer. **Exemplo**: Pacífico/Midway

Defina quais etapas podem ser ignoradas pelo usuário durante a ativação do dispositivo para as seguintes opções de configuração:

Opções de configuração

- Ignorar inserção de senha – selecionar essa opção habilitará automaticamente Ignorar configuração do Apple Pay e Ignorar configuração do Touch ID.
- Ignorar serviços de localização
- Ignorar restauração do backup
- Ignorar "Mover para iOS" do Android
- Ignorar termos de serviço
- Ignorar Entrar em Apple ID e iCloud – selecionar essa opção habilitará automaticamente a configuração Ignorar Apple Pay.
- Ignorar configuração de Touch ID (apenas iPhone 5s, 6, 6+, iPad Air 2, iPad Mini 3) – selecionar essa opção habilitará automaticamente a configuração Ignorar Apple Pay.
- Ignorar configuração do Apple Pay (apenas iPhone 6, 6+, iPad Air 2, iPad Mini 3)
- Ignorar configuração do zoom
- Ignorar Siri
- Ignorar o envio automático das informações de diagnóstico
- Ignorar armazenamento na Cloud (iOS 10.3+ e macOS 10.13.4+)
- Ignorar configuração de tom de exibição (iOS 9+ e macOS 10.14+)
- Ignorar sensibilidade do botão inicial
- Ignorar a tela de seleção do teclado
- Ignorar telas de informações de integração – essas informações são para instruir o usuário. Por exemplo: Folha de rosto, Centro de multitarefa e controle.

Opções de configuração
• Ignorar a tela para a migração do Apple Watch • Ignore a tela Escolher seu visual (iOS 13.0+ e macOS 10.14+) • Ignorar tempo de tela (iOS 12.0+ e macOS 10.15+) • Ignorar privacidade (macOS 10.13.4+ e tvOS 11.3+) • Ignorar Adicionar painel de plano de celular (iPhone XS, iPhone XS Max e iPhone XR) • Mostrar texto personalizado na página Login – Selecione esta opção para digitar uma mensagem personalizada na caixa de texto. Essa mensagem será exibida na página de login no dispositivo durante a configuração de Registro de dispositivos, para oferecer instruções adicionais que ajudem os usuários finais no processo. • Configuração de avanço automático – selecione esta opção para o assistente de configuração avançar automaticamente pelas telas de configuração do dispositivo. O padrão é definido como falso. Compatível com tvOS e macOS 11 e posterior. A configuração de avanço automático não funciona com uma conexão Wi-Fi, o dispositivo deve ser conectado por Ethernet. • Termos de Endereço - ignora o painel Termos de Endereço. (iOS 16+)
iOS
• Ignorar atualização do software (12.0+) • Ignorar o painel de introdução (13.0+) • Ignorar iMessage e FaceTime (12.0+) • Ignorar Restauração concluída (14.0+) • Ignorar Atualização concluída (14.0+)

Opções de configuração
macOS
• Ignorar tela de análise do iCloud • Tela Ignorar exibição de tom certo (macOS 10.13.6+) – (Opcional) Selecione essa opção para pular a janela Exibição de tom certo. • Ignorar acessibilidade (macOS 11.0+) • Ignorar desbloqueio com o Watch (macOS 12.0+)
tvOS
• Ignorar a tela de sincronização de layout da tela inicial da Apple TV • Ignorar a tela de login do provedor da Apple TV • Ignorar a opção Toque para configurar • Ignorar a configuração de proteção de tela Aerial
Opções do assistente de configuração de conta do macOS

Opções de configuração
• Ignorar criação da conta de administrador • Ignorar criação da conta de configuração principal • Criar contas principais como usuários regulares (como administrador, se desmarcado)
(iOS supervisionado) Aguarde a Configuração do dispositivo durante a configuração do Registro de dispositivos
• Aguarde até que todas as configurações e as políticas sejam enviadas aos dispositivos. Selecione para evitar que as configurações sejam enviadas ao dispositivo antes de continuar com as telas restantes de configuração de Registro de dispositivos. Essa configuração evitará que o usuário final use o dispositivo antes de as configurações obrigatórias serem enviadas ao dispositivo. • Limite de tempo – O limite de tempo padrão é de três minutos. O tempo máximo é de 10 minutos. Para ativar esse recurso, selecione a opção **Modo supervisionado** ao editar o perfil de Registro de dispositivos.

12. Clique em **Salvar**.
    A tabela a seguir é preenchida na página **Administrador** > **Apple** > **Registro de dispositivos**:

Configuração	O que fazer
Nome (Clique no cabeçalho da coluna para classificar de modo alfanumérico.) Use o campo Pesquisar para pesquisar itens desta coluna	Nome do servidor MDM
Nome da conta Apple (Clique no cabeçalho da coluna para classificar de modo alfanumérico.) Use o campo Pesquisar para pesquisar itens desta coluna	ID Apple gerenciado
Número de dispositivos	Contagem de dispositivos atribuídos
Perfis de registro	Contagem de perfis de registro de dispositivo atribuídos
Última sincronização (Clique no cabeçalho da coluna para classificar de modo alfanumérico.)	Hora do último contato
Token expira (Clique no cabeçalho da coluna para classificar de modo alfanumérico.)	Data de expiração do token

- Quando novos dispositivos são adicionados ao Registro de dispositivos da Apple, pode demorar até 15 minutos para o Ivanti Neurons for MDM identificar esses dispositivos novos. Em seguida, um perfil de cadastro é atribuído aos novos dispositivos. Caso não seja possível adicionar novos dispositivos ao Registro de dispositivos, vá até **Painel > Notificações** para verificar se há notificações da Apple sobre o Registro de dispositivos. Se houver atualizações ao EULA, você receberá uma notificação por e-mail com instruções para aceitar o novo EULA.
- É possível visualizar todos os atributos dos dispositivos personalizados existentes no seu locatário e designá-los aos dispositivos durante o registro por meio do Registro de dispositivos da Apple.
- Em dispositivos macOS compartilhados, o comando `ListUsers` mostra uma lista de todos os usuários locais no dispositivo e os detalhes do último check-in do usuário que registrou o dispositivo.

Como editar o perfil de Registro de dispositivos

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Encontre o nome do servidor do Apple Business Manager (que você criou no site da Apple) na coluna Nome da conta Apple.
3. Clique no link do número na coluna Perfis de registro.
4. Em um perfil específico, selecione **Ações** > **Editar perfil de registro de dispositivos**.
5. Atualize e salve o perfil.

- Quando um perfil de Registro de dispositivos é editado, a contagem de dispositivos do perfil modificado é atualizada logo em seguida.
- Se você atualizar o token do servidor no site da Apple, o token existente se tornará inválido. Entretanto, a exibição na página Registro de dispositivos, incluindo a data de expiração do token, permanecerá sem mudanças até que você faça o upload do novo token.

O perfil de registro do dispositivo contém os seguintes detalhes:

Configuração	O que fazer
Nome do perfil (Clique no cabeçalho da coluna para classificar de modo alfanumérico.)	Insira um nome que identifique esse perfil de Registro de dispositivos.
Descrição (Clique no cabeçalho da coluna para classificar de modo alfanumérico.)	Insira uma descrição para o perfil.
Departamento (Clique no cabeçalho da coluna para classificar de modo alfanumérico.)	Insira o departamento na sua organização associado a este perfil.
Número de telefone do suporte (Clique no cabeçalho da coluna para classificar de modo alfanumérico.)	Forneça um número de telefone que os usuários do dispositivo possam usar caso precisem de ajuda.
Número de dispositivos	Exibe o número de dispositivos do perfil
Ações	Gerenciar perfis

Como gerenciar múltiplos perfis de Registro de dispositivos

É possível criar vários perfis de Registro de dispositivos para cada servidor do Apple Business Manager. Dessa forma, diferentes conjuntos de dispositivos podem receber diferentes configurações. Os dispositivos também podem ser movidos de um perfil de Registro de dispositivos para outro.

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Encontre o nome do servidor do Apple Business Manager na coluna Nome da conta Apple.

3. Clique no link do número na coluna Perfis de registro.
4. Para criar um novo perfil de Registro de dispositivos que será associado ao servidor selecionado, clique em **Criar novo perfil**. Crie e salve o perfil.
5. Para gerenciar cada perfil, clique em **Ações** e selecione uma das seguintes opções:
   - **Definir como perfil padrão** – defina o perfil como padrão no mesmo servidor virtual. Os registros de novos dispositivos receberão este perfil padrão.
   - **Editar perfil** – atualize um perfil existente.
   - **Editar autenticação** – Edita a configuração de autenticação de Registro de dispositivos.
   - **Designar atributo de dispositivo de registro de dispositivos** – Os administradores usam atributos personalizados para dispositivos para associar propriedades adicionais a esses objetos. Essas propriedades podem ser usadas para criar grupos ou distribuir configurações.
   - **Excluir** – não é possível excluir o perfil padrão. Quando um perfil não padrão é excluído, todos os dispositivos associados serão reatribuídos ao perfil padrão.
6. Para mover um dispositivo registrado de um perfil para o outro dentro do mesmo servidor virtual (e não entre diferentes servidores do Apple Business Manager), clique no link de número na coluna Número de dispositivos. A reatribuição de perfis aplica-se a dispositivos que ainda serão registrados.
   a. Para mover um único dispositivo, clique na opção **Atribuir perfil de registro** para o dispositivo específico, selecione o perfil na lista suspensa e clique em **Atribuir**.
   b. Para mover vários dispositivos, selecione os dispositivos e clique em **Ações** > **Atribuir perfil de registro**, selecione o perfil na lista suspensa e clique em**Atribuir**.

- Quando um perfil de Registro de dispositivos é editado, a contagem de dispositivos do perfil modificado é atualizada logo em seguida.
- Se você atualizar o token do servidor no site da Apple, o token existente se tornará inválido. Entretanto, a exibição na página Registro de dispositivos, incluindo a data de expiração do token, permanecerá sem mudanças até que você faça o upload do novo token.

Adicionando uma página web personalizada de Registro de dispositivos

Aplicável a: iOS 13.0 e macOS 10.15 e versões mais recentes com suporte

Na seção Registro personalizado, você pode especificar sua própria página web personalizada (web view) para autenticar usuários durante o Registro do dispositivo. Use esta página para exibir informações personalizadas, como tipo de autenticação, identidade visual, texto de consentimento e política de privacidade.

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Encontre o nome do servidor criado no site da Apple.
3. Selecione **Ações** > **Editar perfil de registro de dispositivos**.
4. Na seção Registro personalizado, selecione **Ativar registro personalizado**.
5. Selecione uma das opções a seguir:

    - **Página da web hospedada do MobileIron** – redireciona para um Provedor de Identidade (IDP) se o registro estiver usando um provedor de identidade como Serviços de Federação do Microsoft Active Directory (ADFS) ou Okta. O redirecionamento também pode ser feito para o portal de autoatendimento, no caso de um Ivanti Neurons for MDM usuário com autenticação não baseada em IDP.
    - **URL personalizada** – insira uma URL como https://mycustomweburl.com. Esse URL define o valor do URL personalizado a ser apresentado ao usuário em uma web view carregada durante a configuração inicial de um novo dispositivo de Registro de dispositivo ou de um dispositivo apagado. Use este campo para definir sua própria interface do usuário de autenticação com o método de autenticação. Depois que o usuário é autenticado, o perfil de registro no MDM é baixado.

Fluxo de trabalho da página web personalizada de Registro de dispositivos

Esta seção elabora o comportamento da página web personalizada de Registro de dispositivos e o procedimento para criar a página web personalizada (web view).

Quando a página web personalizada especificada no campo **URL** é carregada inicialmente:

- O URL da web de configuração possui um esquema **https** e é uma solicitação **GET**. A página web deve usar um certificado publicamente confiável.

- Um cabeçalho personalizado **x-apple-aspen-deviceinfo** é anexado à solicitação GET pelo dispositivo Apple no qual o registro é iniciado. Ele contém uma codificação base64 de um envelope CMS (Cryptographic Message Syntax) que contém uma lista com atributos de dispositivo. Essas são as mesmas informações, no mesmo formato, conforme fornecidas na solicitação inicial do POST com registros de dispositivos baseados em token.

Quando a página web personalizada é carregada posteriormente:

- O usuário do dispositivo interage com a página da web (web view) até que o servidor host do administrador forneça um arquivo **custom.mobileconfig** ao cliente. O servidor Ivanti Neurons for MDM retorna o código de bytes do perfil MDM. No servidor host do administrador, o arquivo custom.mobileconfig deve ser definido com o tipo MIME **deapplication/x-apple-aspen-config** para que o perfil MDM do dispositivo seja baixado e instalado no dispositivo.
- Para autenticação com Ivanti Neurons for MDM, a página web deve conter as credenciais de nome de usuário e senha de autenticação. Recomenda-se criar um usuário separado no Ivanti Neurons for MDM e atribuir a função de registro personalizado ao usuário que busca o perfil do MDM com o URL do servidor Ivanti Neurons for MDM (por exemplo, https://micloudDomain.com/c/i/dep/custom.mobileconfig).

- Para registro do dispositivo e para obter o perfil MDM de Ivanti Neurons for MDM, o servidor do web host do administrador deve fazer uma chamada POST para o URL do servidor Ivanti Neurons for MDM. Ele também deve passar o cabeçalho x-apple-aspen-deviceinfo com o valor fornecido pelo dispositivo quando o dispositivo atingir o GET URL para carregar a página web personalizada. Se o ID do usuário de registro não for fornecido, o dispositivo será registrado para o usuário ninguém. Aqui estão os detalhes adicionais:
    - Quando um dispositivo atinge o URL da web personalizada configurada no perfil de Registro do dispositivo, o servidor do web host do administrador deve capturar o cabeçalho "x-apple-aspen-deviceinfo" apresentado pelo dispositivo.
    - Para obter o perfil MDM para esse dispositivo e seu usuário relacionado, o servidor do web host do administrador deve fazer uma chamada POST para o URL do servidor Ivanti Neurons for MDM com o cabeçalho x-apple-aspen-deviceinfo. Ele deve conter a autenticação básica usando um ID do usuário Ivanti Neurons for MDM como um parâmetro de solicitação (por exemplo, https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com). O usuário deve receber a atribuição da função Registro personalizado.
    - Depois que o servidor web do host do administrador receber o código de bytes, ele deverá fazer o download do código de bytes para o dispositivo, definindo os cabeçalhos de resposta, Content-Disposition=attachment;filename="profile.mobileconfig" e Content-Type=application/x-apple-aspen-config.
- A web view é fechada e o sistema operacional tenta instalar o perfil, que deve ser um perfil de registro no MDM.

Ivanti Neurons for MDM não autentica o ID do usuário para o qual o perfil MDM é retornado. Portanto, os administradores devem realizar a autenticação necessária para o ID do usuário antes de solicitar o perfil do MDM.

Para o iOS, esse fluxo de trabalho é compatível durante a configuração inicial de um dispositivo apagado. Para o macOS, esse fluxo de trabalho é compatível no Assistente de instalação e também no painel de preferências de Perfis, caso o Registro do dispositivo seja ignorado durante o Assistente de instalação.

Para obter informações do desenvolvedor relacionadas à criação de uma página web personalizada, consulte as seguintes referências de documentação da Apple:

- Web views
- Autenticando através de web views

- Exemplo de código para implementar um navegador web simples para iPad que pode exibir a versão de um site para computador ou para celular

Como editar a configuração de autenticação de Registro de dispositivos

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Encontre o nome do servidor criado no site da Apple.
3. Selecione **Ações** > **Editar autenticação**.

Gerenciamento de token de inicialização para contas móveis

Aplicável a: dispositivos macOS 10.15 e versões compatíveis mais recentes que sejam registrados no MDM usando o Apple School Manager ou o Apple Business Manager.

Ivanti Neurons for MDM é compatível com gerenciamento de token de inicialização para contas móveis. Os tokens de inicialização permitem que contas móveis façam login em dispositivos macOS que utilizem o FileVault. Com esse recurso, todas as contas móveis que fazem login recebem automaticamente um SecureToken. Esse recurso é útil quando vários usuários fazem login em uma máquina criptografada.

Quando uma conta de administrador gerenciada tenta fazer login em um dispositivo:

- No primeiro login, o token de inicialização é solicitado do servidor de MDM.
- Se o servidor de MDM fornecer o token de inicialização, o dispositivo automaticamente criará um SecureToken para a conta.
- O dispositivo habilita o FileVault para o usuário.

O campo Token de inicialização disponível é habilitado na página de detalhes do dispositivo e na forma de um atributo de filtro, durante a criação de um novo grupo de dispositivos ou de uma política personalizada.

Para fins de solução de problemas e verificação, acesse a página de detalhes do dispositivo. Use a página Logs para restringir os logs do dispositivo usando filtros baseados nos nomes de ação Definir token de inicialização e Obter token de inicialização.

Configurações de conta de administrador do macOS gerenciada usando o Registro de dispositivos

O Ivanti Neurons for MDM oferece suporte ao Registro de dispositivos em dispositivos que foram restaurados ao padrão de fábrica ou estão sendo ativados pela primeira vez.Usando o Registro de dispositivos, é possível criar uma conta de administrador em dispositivos macOS. Ivanti Neurons for MDM oferece suporte apenas ao registro opcional no macOS e, portanto, ignora o campo **MDM obrigatório** no perfil de Registro de dispositivos, pois ele se aplica apenas a dispositivos iOS.

Procedimento

1. Acesse **Administrador > Apple > Registro de dispositivos**.
2. Encontre o nome do servidor criado no site da Apple.
3. Selecione **Ações > Editar perfil de registro de dispositivos**.
4. Selecione uma das opções a seguir nas opções do assistente de configuração de conta do macOS:
    - **Ignorar criação de conta de administrador** – selecione essa opção para desativar a criação de uma conta de administrador, visível ou oculta. Desmarque essa opção para permitir que uma conta de administrador seja criada na seção **Configurar conta de administrador do macOS gerenciada** (descrita abaixo).
    - **Ignorar criação de conta de configuração primária** – selecione essa opção para ignorar a configuração da conta primária no dispositivo macOS. Não é criada nenhuma conta de usuário além da conta de administrador. Outra seção, **Configurar conta de administrador do macOS gerenciada**, será exibida (descrita abaixo) para criar a conta de administrador do macOS gerenciada. A conta
 também pode ser oculta a partir de Usuários e Grupos.
    - **Criar contas primárias como usuários regulares (como administrador se não estiverem marcadas)** – selecione essa opção para criar uma conta padrão que não seja de administrador como parte do registro. O Administrador ainda pode criar uma conta de administrador e enviá-la por push para o dispositivo. Outra seção, **Configurar conta de administrador do macOS gerenciada**, será exibida (descrita abaixo) para criar a conta de administrador do macOS gerenciada. A conta
 também pode ser oculta a partir de Usuários e Grupos.
5. Depois de selecionar uma das opções acima, insira os seguintes detalhes na seção **Configurar conta de administrador do macOS gerenciada** se desejar criar uma conta de administrador do macOS gerenciada:

- Nome Completo
- Nome da conta
- Senha
- Confirmar senha
- (Opcional) Ocultar conta de administrador gerenciada em Usuários e grupos

6. Se você não selecionar a opção **Ignorar criação da conta de configuração primária**, informe os seguintes detalhes na seção **Configurar conta primária**. Essa ação adiciona o suporte do canal do usuário à conta de administrador gerenciada, graças à configuração do nome abreviado do usuário local gerenciado para o nome abreviado de um administrador.
   - **Nome completo**
   - **Nome abreviado**
   - (Opcional) **Impedir a modificação pelo usuário final** – Esta configuração será substituída se o Nome completo e/ou o Nome abreviado tiverem variáveis de substituição e forem avaliados como vazios. Se você selecionar esta opção, esteja ciente de que a configuração desta conta primária do administrador só será aplicável se uma das seguintes opções for definida apropriadamente:
     a. A opção Solicitar registro/login do usuário está selecionada na visualização de configuração de autenticação.
     b. A página da Web hospedada no MobileIron está selecionada para Personalização do registro.
7. Selecione **Ignorar criação de conta de configuração principal** para permitir o suporte do canal do usuário para a conta de administrador gerenciada. Você pode definir o nome abreviado do usuário local gerenciado como o nome abreviado de um administrador.
8. Clique em **Salvar**.

Alteração da senha da conta de administrador local do macOS

O administrador pode alterar a senha local de uma conta local de administrador do macOS que foi criada pelo Assistente de configuração durante o Registro de dispositivos.

Aplicável a: macOS 10.11 ou a versões mais recentes com suporte.

Procedimento

1. Acesse **Dispositivos**.
2. Clique no nome do usuário ao qual o dispositivo está associado para visualizar a página de detalhes do dispositivo.
3. No menu Ações, clique em**Configurar senha do administrador do macOS**. Essa ação também pode ser executada na página Lista de dispositivos selecionando um ou mais dispositivos.
4. Insira a senha.
5. Clique em **Salvar**.

Exportar para CSV

Ivanti Neurons for MDM permite exportar os dispositivos inscritos pelo dispositivo para um arquivo CSV.

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Clique no link de contagem de dispositivos específicos na coluna **Número de dispositivos**.
3. Clique na opção **Exportar para CSV** para exportar a lista de dispositivos e os detalhes relacionados para um arquivo CSV. Quando o relatório estiver pronto, você receberá uma mensagem para Baixar ou Excluir o relatório. Você também receberá um e-mail contendo um link para baixar o relatório.
4. Clique em **Baixar**.
5. (Opcional) Clique em **Excluir** para excluir o relatório.

Configurando o Assistente de Configuração

O Assistente de Configuração permite selecionar as telas que você deseja ignorar ou incluir durante a configuração dos dispositivos iOS e macOS.

Procedimento

1. Faça login no console administrativo do Ivanti Neurons for MDM.
2. Vá até **Configurações**.
3. Selecione **Assistente de Configuração**.
4. Clique no ícone de lápis (editar).
5. Marque as caixas de seleção para ignorar as telas de configuração específicas do dispositivo.
6. Clique em **Concluído**.
7. Selecione **Canal do dispositivo**.
8. Selecione **Todos os dispositivos**. A configuração do Assistente de Configuração é enviada aos dispositivos, e a guia Configuração na página Detalhes do Dispositivo exibe o estado Instalado.
9. Faça login no dispositivo. Todas as telas da configuração inicial são ignoradas

Instalar certificado de MDM

Você deve solicitar e instalar um certificado de MDM da Apple para gerenciar os dispositivos iOS instalados. Também será necessário renovar esse certificado uma vez por ano. (A conta Apple usada para criar o certificado recebe uma notificação do site da Apple quando a data de expiração se aproxima.) Use a página Certificado MDM para adicionar ou renovar este certificado.

Aquisição e instalação do certificado de MDM

Procedimento

1. Use a página **Certificado MDM** para baixar uma solicitação de assinatura de certificado (CSR) do seu locatário do Ivanti Neurons for MDM.
2. Faça o upload do CSR para Apple para criar um novo certificado.

   No site da Apple, adicione uma observação indicando o propósito do certificado. Essa observação ajudará na hora de renovar o certificado.
3. Salve o certificado.
4. Instale o certificado para seu locatário do Ivanti Neurons for MDM.

Renovação do certificado de MDM

Procedimento

1. Clique em **Renovar certificado**.
2. Baixe uma solicitação de assinatura de certificado (CSR) do seu locatário do Ivanti Neurons for MDM.
3. Faça o upload do CSR para Apple para renovar o certificado correspondente.

   No site da Apple, certifique-se de estar renovando o certificado certo. O upload de um certificado diferente no Ivanti Neurons for MDM desativa automaticamente todos os dispositivos iOS registrados.
4. Instale o certificado para seu locatário do Ivanti Neurons for MDM.

   Você receberá um aviso se tentar fazer o upload do certificado errado.

Se você não conseguir visualizar a página **Instalando o certificado MDM**, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Dispositivos iPad compartilhados para empresas

Os dispositivos iPad compartilhados para empresas estão disponíveis para os IDs Apple Gerenciados criados no Apple Business Manager com iOS 13.4 ou versões compatíveis mais recentes.

- Dispositivos iPad compartilhados permitem que as empresas compartilhem dispositivos entre vários funcionários, ao mesmo tempo em que proporcionam uma experiência personalizada.
- Os funcionários podem fazer login com um ID Apple Gerenciado para começar a carregar seus dados, incluindo contas de e-mail, arquivos, Biblioteca de Fotos do iCloud, dados de aplicativos e muito mais.
- Os dados são armazenados no iCloud, para que os funcionários possam fazer login em qualquer dispositivo iPad compartilhado que pertença à organização.

Os dispositivos iPad compartilhados podem ser usados em aplicações nas áreas de saúde, varejo e industrial. Por exemplo, médicos e enfermeiros podem compartilhar um dispositivo iPad, pois cada um acessa com segurança o perfil de usuário elaborado exclusivamente para si. Em lojas de varejo, os funcionários da linha de frente podem ter acesso a informações sobre produtos, recursos, experiência para encantar os clientes e fornecer melhores experiências de compra.

Funcionamento

- Os dispositivos iPad são adicionados ao Apple Business Manager e registrados usando um perfil de registro automatizado com o modo compartilhado ativado.
- Os funcionários fazem login no dispositivo iPad compartilhado com um ID Apple Gerenciado e uma senha fornecidos pela empresa. O administrador do Apple Business Manager pode criar manualmente as contas para os usuários ou federar a criação da conta a um provedor de identidade como o Azure Active Directory.
- Cada usuário pode ter seu perfil personalizado quando estiver logado no dispositivo iPad compartilhado. Os administradores podem distribuir aplicativos segundo a função, as responsabilidades e o departamento dos usuários.
- Os usuários podem fazer login como convidados em um dispositivo iPad compartilhado. O login do usuário convidado é habilitado por padrão. Um usuário convidado não precisa fazer login com ID Apple Gerenciado e senha. O login de usuário convidado pode ser desabilitado configurando-se a opção **Permitir sessão de convidado para iPad compartilhado** como **Falso** na configuração Restrições do iOS.

- Acesse Ivanti Neurons for MDM **>** **Dispositivos**, clique no nome de um dispositivo iPad compartilhado e clique na guia **Usuários** para ver a lista de usuários no dispositivo com seus respectivos detalhes (tais como ID Apple Gerenciado, Dados Disponíveis em bytes, Dados Usados em bytes e Tem Dados para Sincronizar com o Ivanti Neurons for MDM).
- Acesse a guia **Logs** e selecione nos filtros a ação **Relatar Lista de Usuários** para exibir detalhes adicionais dos usuários.
- O login de usuário convidado em um dispositivo iPad compartilhado difere do gerenciamento de usuário convidado feito pelo Ivanti Neurons for MDM. Por padrão, a conta de usuário convidado está desabilitada no Ivanti Neurons for MDM. Para gerenciar um usuário convidado em um dispositivo iPad compartilhado, habilite a conta de usuário convidado.
- A gravação de tela está disponível na Central de Controle em dispositivos iPad compartilhados.
- Ivanti Neurons for MDM é compatível com uma variável de substituição para o ID Apple gerenciado, `${managedAppleID}`. Esta variável do sistema é exibida na seção de atributos do sistema e na seção de atributos do dispositivo.
- Ivanti Neurons for MDM impede que um administrador altere o ID Apple Gerenciado de usuários residentes que estavam conectados ao dispositivo iPad compartilhado no passado, juntamente com os usuários atualmente conectados. Se você tentar alterar o ID Apple Gerenciado, uma mensagem de erro indicará que o ID Apple Gerenciado do usuário não pode ser alterado, pois o usuário está usando um dispositivo iPad compartilhado.
- No caso de Apps e Livros Apple, Apps e Livros são instalados nos dispositivos iPad compartilhados segundo licenças baseadas em dispositivo, independentemente de tais licenças estarem ou não selecionadas.

Pré-requisitos

Assegure que os pré-requisitos a seguir sejam atendidos:

- Um dispositivo iPad compartilhado requer um ID Apple Gerenciado. Os administradores podem criar manualmente as contas ou federar a um provedor de identidade como o Azure Active Directory.
- Os dispositivos iPad compartilhados devem conter iOS 13.4 ou versões compatíveis mais recentes.
- Os dispositivos devem estar associados a contas do Apple Business Manager.
- Os dispositivos devem conter armazenamento de 32 GB ou mais.

Observe os seguintes pontos:

- Ivanti Neurons for MDM impede determinadas configurações, tais como Senha, em dispositivos iPad compartilhados, pois a Apple não oferece suporte a elas. Essas configurações não são transmitidas para os dispositivos (Dispositivos > clique no link de nome de um dispositivo > guia Configurações).
- A configuração Senha não se aplica a dispositivos iPad compartilhados, pois eles exigem IDs Apple Gerenciados, que estão associados a senhas alfanuméricas, e não a códigos de acesso. A ação Desbloquear no portal administrativo do Ivanti Neurons for MDM não limpará a senha em um dispositivo iPad compartilhado.
- Selecione Canal do Dispositivo ou Canal do Usuário durante a distribuição da configuração Restrições do iOS aos dispositivos iPad compartilhados. É possível distribuir configurações separadas e aplicar restrições que sejam aplicáveis apenas ao canal do dispositivo ou do usuário.
- Ivanti Neurons for MDM verifica as contas expiradas e desativa os dispositivos pertencentes a elas. No entanto, para um dispositivo iPad compartilhado, o proprietário do dispositivo é o último usuário logado e pode não ser o proprietário legal. Se uma conta de proprietário expira, o Ivanti Neurons for MDM exclui os dispositivos iPad compartilhados da desativação.
- O cliente Go para iOS não é compatível com dispositivos iPad compartilhados.
- Usuários não podem realizar ações como desativar e apagar em dispositivos iPad compartilhados. Somente administradores podem executar ações de desativação e apagamento pelo portal administrativo do Ivanti Neurons for MDM.
- Os administradores não podem alterar o proprietário do dispositivo iPad compartilhado no portal administrativo do Ivanti Neurons for MDM.
- O login zero não é compatível com dispositivos iPad compartilhados.
- Quando o comando `ListUsers` está habilitado, todos os IDs de usuário gerenciados e seus horários de check-in são exibidos em Registro de Dispositivo (parte do Apple Business Manager) na guia **Administrador**.

Configurando um dispositivo iPad compartilhado

Você pode estabelecer um dispositivo iPad compartilhado e definir as configurações.

Procedimento

1. Acesse **Administrador** > **Apple** > **Registro de dispositivos**.
2. Adicione o dispositivo ao Apple Business Manager registrando o dispositivo com um perfil de registro de dispositivo automatizado. Para obter informações sobre este procedimento, consulte Registro de dispositivos.
3. Nas configurações de registro de dispositivos, habilite:
   - **Modo Supervisionado**.
   - **Modo Multiusuário** em **Dispositivo iPad compartilhado para empresa**.
4. (Opcional) Criar uma conta de usuário local. O dispositivo será registrado para este usuário. A autenticação deste usuário ocorre apenas uma vez durante o registro.
5. Redefina o iPad compartilhado.

   O processo de registro começa somente após a reinicialização. Leva alguns minutos para o dispositivo ser registrado e configurado como um iPad compartilhado.
6. O proprietário legal é atribuído à conta de usuário que registrou o dispositivo. O administrador pode alterar o proprietário legal na página **Dispositivos**.

7. Na tela de login do dispositivo, insira as credenciais do ID Apple Gerenciado do usuário.

    - Semelhante aos dispositivos macOS, você pode enviar configurações em dispositivos iPad compartilhados por meio dos canais de dispositivo e de usuário.
    - As variáveis de substituição do usuário não substituem as configurações (incluindo a configuração Aplicativo Gerenciado) enviadas no canal do dispositivo.
    - Se o usuário logado em um dispositivo iPad compartilhado não for um usuário gerenciado - o ID Apple gerenciado não pertence a nenhum usuário no portal administrativo Ivanti Neurons for MDM, o dispositivo não é atribuído a ninguém. Os usuários não serão gerenciados - o administrador não pode enviar configurações de canal de usuário a partir do Ivanti Neurons for MDM.
    - Por padrão, o usuário convidado padrão criado pelo Ivanti Neurons for MDM está desabilitado. Quando um usuário convidado faz login, o dispositivo não é atribuído a nenhum usuário, e o usuário não é gerenciado. Se o usuário convidado tiver que ser gerenciado, o usuário convidado padrão criado pelo Ivanti Neurons for MDM deverá ser habilitado, e o dispositivo será atribuído ao usuário convidado padrão após o login do usuário convidado. O usuário pode então ser gerenciado.
    - As informações do proprietário do dispositivo são exibidas na página Ivanti Neurons for MDM > **Dispositivos** e nos logs de dispositivo (página de detalhes do dispositivo > **Logs**).

Gerenciamento de proprietários legais para iPads compartilhados

Você pesquisa e visualiza os proprietários legais dos dispositivos iPad compartilhados usando seus IDs de e-mail na página de listagem de dispositivos. Você pode alterar os proprietários legais dos dispositivos iPad compartilhados reatribuindo os proprietários legais existentes aos novos proprietários legais. Se o proprietário legal de um dispositivo iPad não compartilhado for reatribuído, o Ivanti Neurons for MDM ignorará a atribuição.

Procedimento

1. Acesse **Dispositivos**.
2. Clique no ícone de engrenagem para selecionar e adicionar a coluna **Proprietário Legal** à página da lista de dispositivos.
3. Selecione os dispositivos iPad compartilhados.
4. Clique em **Ações > Atribuir ao proprietário legal**.

Enviando um e-mail para o proprietário legal de um dispositivo iPad compartilhado

Você pode enviar e-mails para o proprietário legal de um dispositivo iPad compartilhado.

Procedimento

1. Acesse **Dispositivos**.
2. Clique no nome do dispositivo iPad compartilhado.
3. Clique no ícone **e-mail**.
4. Redija o e-mail.
5. Clique em **Enviar**.

Usando o atributo Modo multiusuário

Você pode usar o atributo Modo Multiusuário dos dispositivos iPad compartilhados no Ivanti Neurons for MDM.

Procedimento

1. Na página **Dispositivos**, use o atributo **Modo multiusuário**.
2. Clique em **Pesquisa avançada** e crie uma regra para encontrar os dispositivos usando o atributo **Modo multiusuário**.
3. Na página **Dispositivos > Grupos de dispositivos**, crie um grupo dinâmico para os dispositivos iPad compartilhados usando o atributo **Modo multiusuário**. Por exemplo, você pode usar este grupo como um filtro de distribuição para distribuir configurações.
4. Na página **Políticas**, crie uma política personalizada para os dispositivos iPad compartilhados usando o atributo **Modo multiusuário**.
5. Em **Aplicativos > Filtro de distribuição**, use o atributo **Modo multiusuário** para limitar o número de aplicativos disponíveis para instalação.

- O Ivanti Neurons for MDM não suporta o modo multiusuário para dispositivos Apple School Manager. Não é recomendável ativar a configuração e transferir o perfil Registro de dispositivos para dispositivos Apple School Manager.
- A configuração Entrada Segura Multiusuário para iOS não se aplica a dispositivos iPad compartilhados.

Excluindo usuários de um dispositivo iPad compartilhado

Você pode excluir um usuário ou várias contas de usuário dos dispositivos iPad compartilhados. Na guia Lista de usuários, o rótulo **Ativo** indica o usuário conectado no momento. A opção Excluir não se aplica ao usuário atualmente conectado no dispositivo iPad compartilhado. Os usuários podem ser excluídos pelas guias **Dispositivos** ou **Usuários**.

Excluindo usuários da guia Dispositivos

Procedimento

1. Vá para a guia **Dispositivos** > **Detalhes do dispositivo**.
2. Vá para a guia **Usuários**. A lista de usuários é exibida.
3. Clique em **Excluir todos os usuários**.
4. Clique no sinal de menos "**-**" para excluir usuários específicos.
   - (Opcional) Na janela **Excluir usuário**, selecione a opção **Forçar exclusão do usuário mesmo se a sincronização de dados com o Ivanti Neurons for MDM estiver pendente** e clique em **Sim**.

     Selecionar **Forçar exclusão do usuário mesmo se a sincronização de dados com o Ivanti Neurons for MDM estiver pendente** forçará a exclusão do usuário, mesmo que os dados ainda não estejam sincronizados com o portal administrativo do Ivanti Neurons for MDM.

Excluindo usuários da guia Usuários

Procedimento

1. Vá para a guia **Usuários**.
2. Selecione um ou vários usuários, vá para o menu suspenso **Ações**, clique em **Excluir**. Uma mensagem de confirmação é exibida. Após você confirmar, o comando excluir usuário é emitido para os dispositivos.
3. Vá para **Logs do dispositivo** nos detalhes do dispositivo e verifique se o comando Excluir usuário foi enviado aos usuários selecionados do dispositivo iPad compartilhado.

Desconectando usuários de um dispositivo iPad compartilhado

O administrador pode fazer o logout de usuários de um dispositivo iPad compartilhado.

Procedimento

1. Na página **Dispositivos**, selecione um dispositivo iPad compartilhado.
2. Selecione **Forçar logout** no menu **Ações**. Ao fazer logout de usuários do dispositivo iPad compartilhado, um pop-up solicitará confirmação.
3. Clique em **OK** para aprovar o logout forçado.

School Manager

Licença: Gold

Aplicável para: iOS 9.3+ supervisionado

O Apple School Manager é um serviço em nuvem da Apple dedicado a instituições de ensino para fornecer serviços que incluem a compra de aplicativos no Apps and Books da Apple, o registro de iPads por meio do Registro de Dispositivos Apple e a criação de IDs Apple gerenciados. Com integração total com o Apple School Manager, a solução Ivanti Neurons for MDM UEM oferece uma maneira perfeita de gerenciar totalmente os iPads designados para professores e alunos para aproveitar o ecossistema do School Manager e aplicativos como o Classroom.

Apple Books não é compatível.

Configurando o School Manager

1. Acesse **Administrador > School Manager**.
2. Clique na opção **Configurar Educação**, caso ela esteja desativada.
3. Selecione uma das opções a seguir:

- **Sincronize com a conta do Apple School Manager para importar as informações da instituição de ensino**:

  a. Acesse **Administrador > Apple > Registro de dispositivos** para fazer download dos arquivos de chave da sua organização.

  b. Transfira os arquivos de chave para sua conta do Apple School Manager para gerar chaves de criptografia.

  Faça o download das chaves de criptografia do Apple School Manager e o upload das chaves para o Ivanti Neurons for MDM (**Administrador > Apple > Registro de dispositivos**).

  > As contas existentes de Registro de dispositivos da Apple podem ser reutilizadas para a Educação da Apple. A Apple oferecerá a opção de atualizar sua conta do Registro de dispositivos para incluir recursos da Educação ao acessar o Apple School Manager. Para obter instruções de atualização, acesse https://support.apple.com/en-in/HT206960.

  c. Quando as chaves de criptografia forem aceitas, o botão **Sincronizar agora** será exibido.

  d. Clique em **Sincronizar agora** para iniciar a sincronização dos dados com o Apple School Manager.

- **Importar dados de arquivos CSV**:

  a. (Opcional) Clique em **Fazer download do arquivo ZIP de modelos de CSV** para fazer download de um arquivo zip que contém modelos de todos os tipos de dados.

  b. Clique em **Selecionar arquivos**...

  c. Adicione os seis arquivos CSV a seguir:

  - Arquivo de dados dos alunos (students.csv)
  - Arquivo de dados de registro (roster.csv)
  - Arquivo de dados da equipe (staff.csv)
  - Arquivo de dados das classes (classes.csv)
  - Arquivo de dados dos cursos (courses.csv)
  - Arquivo de dados das localidades (locations.csv)

  > Sempre selecione os seis arquivos CSV juntos antes de fazer o upload.

  d. Clique em **Upload**.

  e. (Opcional) Se os arquivos CSV precisarem ser modificados, mantenha todos os dados necessários nos seis arquivos carregados anteriormente. Faça as edições necessárias e o upload de todos juntos.

4. Pesquise dados nas guias **Turmas** e **Indivíduos**.

> Os indivíduos (alunos e funcionários) também aparecem na página **Usuários** do Ivanti Neurons for MDM.

5. Crie dois grupos para os dispositivos que serão usados para educação por alunos e funcionários, da seguinte forma:
   a. Acesse **Administrador > Atributos personalizados**.
   b. Crie atributos personalizados para os alunos e para a equipe que serão usados para criar grupos de dispositivos gerenciados de forma dinâmica.
   c. Acesse **Dispositivos > Grupos de dispositivos**.
   d. Clique em **Adicionar+**.
   e. Crie um grupo de dispositivos gerenciados de forma dinâmica para o alunos e para a equipe usando os atributos personalizados criados anteriormente como filtros.
6. Atribua os dispositivos registrados aos alunos e à equipe a partir da página **Dispositivos** usando a opção **Ações > Atribuir a usuário**.
7. Crie uma configuração de Líder (equipe) e uma configuração de Membro (alunos) ao adicionar as cargas úteis **Configurações > Educação**.
8. Distribua as configurações de Líder (equipe) e Membro (alunos) aos grupos de dispositivos de equipe e alunos.
   A distribuição aplicará essas configurações e instalará certificados nos respectivos dispositivos.

Na página **Administrador > School Manager**, se não constar nenhum valor para o Nome da classe, o valor será derivado dos campos identificador de origem do sistema de classes e identificador de curso. Esses campos são opcionais no Apple School Manager ou no arquivo CSV. Entretanto, é recomendado sempre inserir um valor como a combinação usada como o identificador padrão na ausência de um Nome da classe.

Aplicando o aplicativo Classroom a professores

Com o aplicativo Classroom, os professores (Líder) podem gerenciar os seguintes cenários:

- Capacidade de gerenciamento do Classroom para controlar iPads e apps remotamente.
- Capacidade de criar um grupo de classe.
- Capacidade de o professor visualizar os alunos desse grupo.

- Capacidade de o professor enviar conteúdo aos alunos desse grupo.
- Restrinja os apps e o conteúdo que podem ser visualizados pelos alunos.

Você pode enviar o aplicativo Classroom a partir da Apple App Store.

Procedimento

1. Acesse a página **Apps > App Catalog**.
2. Clique no botão **+Adicionar**.
3. Pesquise e selecione o aplicativo Classroom da Apple.
4. Clique em **Avançar**.
5. Insira a categoria e a descrição.
6. Clique em **Avançar**.
7. Distribua o aplicativo no grupo de dispositivos de professores criado anteriormente.
8. Defina as configurações do aplicativo na página Configurações do aplicativo.
9. Clique em **Concluído**.

Desativando o School Manager

Desativar o School Manager limpará todos os dados atuais. Tome cuidado ao fazer isso.

1. Acesse **Administrador > School Manager**.
2. Clique na opção **Configurar Educação**, caso ela esteja ativada.
3. Clique em **Sim**.

Configuração (Apple)

Os administradores podem configurar, habilitar e desabilitar diversas configurações para os dispositivos Apple.

Registro silencioso (apenas para macOS)

O registro silencioso para dispositivos macOS está bloqueado como Ativado. Isso se aplica a todos os novos registros de dispositivos no locatário e é compatível com o Mobile@Work 1.4 ou versões mais recentes com suporte.

Configurações do perfil

Os administradores podem ativar ou desativar o envio de e-mails para os usuários finais e notificações para os clientes macOS e Go para iOS se o perfil MDM não estiver instalado. O recurso de notificações de perfil do MDM é ativado por padrão.

Procedimento

1. Acesse **Administrador** > **Configurações**.
2. Marque ou desmarque a opção **Enviar email para o usuário e notificar o cliente se o perfil MDM não estiver instalado**.
3. Selecione o número máximo de notificações/emails entre 1 e 4.
4. Clique em **Salvar**.

Atualizações do SO para o registro automatizado de dispositivos (apenas iOS)

Os administradores podem ativar as atualizações do sistema operacional iOS para o registro automatizado de dispositivos. Se essa opção estiver ativada, os dispositivos de Registro do dispositivo usarão a configuração Atualizações de software em vez da configuração de atualização do SO agendada no Perfil de registro de dispositivos.

Essa opção está desativada por padrão. Nesse caso, é usada a configuração de atualização do SO agendada no Perfil de registro do dispositivo. A ativação dessa configuração é permanente e não pode ser desativada. Essa configuração removerá a configuração de atualização do SO agendada em todos os perfis de Registro de dispositivos disponíveis.

Os dispositivos de registro de não dispositivo supervisionados usam a configuração Atualizações de software.

Procedimento

1. Acesse **Administrador > Configurações**.
2. Marque ou desmarque a opção **Usar configuração de atualização de software para registro automatizado de dispositivos**.
3. Clique em **Sim** para confirmar.
4. Clique em **Salvar**.

Entrada segura multiusuário

Os administradores podem apagar a senha do dispositivo quando o usuário fizer logout do clipe da Web de Entrada segura multiusuário em dispositivos compartilhados iOS selecionando a opção "**Limpar senha após o logout do usuário**" na seção "**Entrada segura multiusuário**" em Administrador > Apple > Configurações.

Definições de prioridade para configuração de restrições

O administrador pode ativar prioridades para diversas restrições de configuração para iOS e macOS selecionando as opções **Configuração de restrições de iOS** ou **Configurações de restrições de macOS** na seção **Definições de prioridade para configuração de restrições** em **Administrador > Apple > Configurações**. Essa opção está desativada por padrão. Para obter mais informações sobre o funcionamento das prioridades, consulte "Priorização de configurações" na página 478.

Procedimento

1. Acesse **Administrador > Apple > Configurações**.
2. Na seção **Definições de prioridade para configuração de restrições**, selecione a opção **Configuração de restrições de iOS** ou **Configuração de restrições de macOS**.

3. Clique em **Salvar** para ativar a prioridade. O banner "**Definições de prioridade para configuração de restrições (iOS ou macOS) foi ativado**" é exibido. Antes de a prioridade ser **Aprovada**:

   - **Editar resumo da distribuição (se aplicável)**: quando a configuração de prioridade estiver ativada, o resumo de distribuição para a configuração de restrição selecionada é alterado de "**Aplicar a dispositivos em outros espaços**" para "**Aplicar a todos os dispositivos em outros espaços com a prioridade mais alta**" por padrão.
   - **A prioridade padrão é atribuída na ordem de criação**: para configurações de tipo de restrição selecionada, uma prioridade padrão existente é atribuída na ordem em que foi criada.
   - **Suspensão do gerenciamento da configuração**: o gerenciamento da configuração de restrições selecionadas (por exemplo, Configuração de restrições de iOS) é suspenso até que a prioridade seja aprovada por você.

   > Após a prioridade ser ativada, todas as alterações nas restrições não serão processadas até que sejam aprovadas. Antes de aprovar, o administrador pode editar a distribuição, o resumo da distribuição ou a prioridade para configurações de restrições na seção **Configurações**.

4. Marque a opção **Aprovar** para colocar a prioridade em vigor.
5. Clique em **Salvar**.

   > A opção **Aprovação** não estará disponível ao desmarcar uma opção de configuração Restrições de iOS ou macOS, as alterações serão aplicadas instantaneamente.

Quando a configuração de prioridade é desativada, não há nenhuma prioridade associada às configurações. Todas as configurações de restrição são enviadas por push ao dispositivo, se aplicável (na próxima sincronização do dispositivo).

- **Resumo de distribuições (se aplicável):** quando a configuração de prioridade é desativada para a configuração de restrições, o resumo de distribuições é alterado de **Aplicar a todos os dispositivos em outros espaços de dispositivos como a prioridade mais alta** ou **Aplicar a todos os dispositivos em outros espaços de dispositivos como a prioridade mais baixa** para "**Aplicar a dispositivos em outros espaços**".
- **Nenhuma prioridade é atribuída**: a prioridade atribuída é removida da configuração de restrições selecionadas

Trabalhe com dispositivos com Windows

Esta seção contém os seguintes tópicos:

Configuração de perfis do Windows Autopilot

O Windows Autopilot é um recurso da Microsoft que ajuda os administradores a configurar e pré-configurar novos dispositivos para deixá-los prontos para uso. O recurso Autopilot ajuda com um provisionamento rápido, confiável e contínuo de dispositivos Windows Desktop ou HoloLens 2. Além disso, o recurso Autopilot ajuda a executar as seguintes tarefas:

- Unir dispositivos automaticamente ao Azure Active Directory (AAD)
- Registrar automaticamente dispositivos em serviços MDM
- Criar e atribuir automaticamente dispositivos para grupos de configuração com base no perfil do dispositivo
- Personalizar a experiência de registro
- Aplicar configurações e políticas
- Instalar aplicativos essenciais

Pré-requisitos

Os administradores podem criar perfis de usuário na página do Windows Autopilot no portal administrativo Ivanti Neurons for MDM. Assegure que os pré-requisitos a seguir sejam atendidos para que o recurso do Autopilot funcione conforme esperado:

- O recurso Autopilot (feature.autopilot) está ativado
- O locatário do Ivanti Neurons for MDM é integrado ao locatário do AAD
- Um usuário fictício é criado e sincronizado - fooUser@<aad-domain>

Modos de registro do Autopilot

Depois que você associar os dispositivos a um grupo específico de perfil de usuário, com base no uso do dispositivo, você pode configurar o modo de registro do Autopilot para permitir que os usuários comecem a trabalhar rapidamente com os dispositivos. O Ivanti Neurons for MDM oferece os seguintes modos de registro do Autopilot:

- Modo de autoimplementação
- Orientado pelo usuário (modo pré-provisionado)

- Orientado pelo usuário

Modo de autoimplementação do Autopilot – O modo de registro de dispositivos de autoimplementação do Autopilot garante uma implementação perfeita de um dispositivo corporativo para um usuário, dispensando a configuração inicial do dispositivo e inserindo todos os arquivos de configuração necessários para que o dispositivo seja iniciado de forma segura. Este modo protege o hardware, conecta o dispositivo à rede corporativa, registra o dispositivo no Azure Active Directory (AAD), no serviço MDM e no portal de administrador do Ivanti Neurons for MDM usando um ID de usuário fictício, e todos os arquivos de configuração necessários são inseridos no dispositivo antes que o usuário faça login. Assim que os arquivos obrigatórios de configuração forem inseridos, o dispositivo é reiniciado e exibe a tela de login para que o usuário corporativo possa começar a trabalhar. Você pode usar o modo de autoimplementação para um dispositivo que pode ser usado como um quiosque ou um dispositivo assinado digitalmente.

Modo de perfil pré-provisionado orientado pelo usuário – Assim que o administrador criar um perfil pré-provisionado movido pelo usuário, ele atribuirá o perfil a um grupo de usuários, e o ID de hardware do dispositivo será carregado e atribuído ao grupo do AAD. O dispositivo será associado ao perfil pré-provisionado orientado pelo usuário. Este modo é usado pelo administrador para configurar um dispositivo antes que ele seja entregue ao usuário corporativo. O processo envolvido é o seguinte:

Procedimento

1. Conecte o novo dispositivo de hardware ao LAN e pressione o botão do Windows cinco vezes.
2. O dispositivo vai exibir uma pergunta. Selecione a opção Provisionamento do Windows Autopilot e clique em Continuar. O Intune detecta o modo de perfil de pré-provisionamento orientado pelo usuário, e todas as configurações básicas são implementadas no dispositivo. A tela Configuração do Windows Autopilot é exibida.
3. Clique em Continuar. O dispositivo segue adiante e protege o hardware, conecta o dispositivo à rede corporativa, registra o dispositivo no Azure Active Directory (AAD), no serviço MDM e no portal de administrador do Ivanti Neurons for MDM usando um ID de usuário fictício, todos os arquivos de configuração necessários são inseridos no dispositivo e uma mensagem de confirmação aparece.
4. Agora você já pode entregar o dispositivo para o usuário. Quando o usuário fizer login no dispositivo, o ID do usuário será registrado no portal de administrador do Ivanti Neurons for MDM com os detalhes do dispositivo.

As configurações a seguir são inseridas automaticamente antes que o usuário faça login no dispositivo:

- Certificado de identidade
- Wi-Fi
- Windows Hello para Empresas
- Restrições do Windows

O restante das configurações fica em estado Pendente, sendo enviado assim que o usuário fizer login no dispositivo usando um endereço de e-mail.

Durante o processo de registro no Autopilot nos modos de implantação automática e orientado ao usuário (pré-provisionamento), os aplicativos .MSI e .EXE atribuídos serão instalados no dispositivo para concluir o processo de registro. Ao instalar os aplicativos .MSI e .EXE durante o processo de registro no Autopilot, se os aplicativos relatarem ou deixarem de relatar durante a instalação, o processo do Autopilot será concluído, e o botão Redefinir será habilitado.

Criação de perfis de usuários do Windows Autopilot

Assim que você configurar a Fonte de usuário do Azure Active Directory (AAD) e sincronizar os usuários e os grupos de usuários do AAD com o locatário do Ivanti Neurons for MDM, pode criar os perfis do Autopilot.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Administrador > Microsoft Azure > Gerenciamento de Dispositivos Windows**.

   Se a Fonte de usuário ADD não estiver configurada, o botão **Adicionar** será desativado. Você deve configurar a Fonte de Usuário usando a opção **Gerenciamento de Dispositivos Windows** presente na seção **Microsoft Azure**.

3. Clique em **Adicionar**.

   A página **Adicionar perfil do Windows Autopilot** aparece na tela.

4. Insira um nome de perfil na caixa **Nome**.
5. Conclua as **Configurações de perfil** usando a tabela embaixo deste procedimento.

6. Clique em **Avançar**.

   Uma nova página com todos os Grupos de Dispositivos AAD aparece na tela.

7. Selecione um ou mais Grupos de Dispositivos AAD aos quais o perfil do Autopilot deve ser atribuído.

   Você também pode criar um Grupo de Dispositivos AAD e atribuir o perfil do Autopilot a esse grupo recém-criado. Consulte "Criar Grupos de Dispositivos AAD" na página 1329 para obter mais informações.

8. Caso você queira atribuir o perfil do Autopilot para todos os Grupos AAD, selecione a opção **Atribuir a todos os Grupos AAD**.

   Você não pode atribuir mais de um perfil a "Todos os grupos" devido a uma limitação da Microsoft.

9. Clique em **Concluído**.

Configuração	Descrição
Tipo de dispositivo	Selecione uma das duas opções a seguir, dependendo do dispositivo: • **Windows PC**. • **HoloLens** – Quando essa opção é selecionada, o modo padrão de implementação deve ser definido como modo de **Autoimplementação**. Em casos raros, ao registrar dispositivos HoloLens 2 usando o Autopilot, o registro pode ficar parado na tela 'Configurando seu dispositivo para o trabalho'. Neste caso raro, o usuário deve desligar e ligar o dispositivo apertando o botão Liga/Desliga. Em seguida, o dispositivo mostra a tela de Login, na qual o usuário deve inserir as credenciais AAD para concluir o registro.
Modo de implementação	• **Autoimplementação**: neste modo, a implementação do dispositivo ocorre com pouco ou nenhum envolvimento manual. • **Orientado pelo usuário**: os administradores podem usar essa opção para selecionar o modo de registro para configurar um novo dispositivo para o usuário antes de entregar o dispositivo para o usuário.

Configuração	Descrição
Tipo de conta do usuário	• **Administrador**: selecione esta opção se o usuário precisar de controle total assim que o dispositivo for implementado. • **Padrão**: selecione esta opção se o usuário precisar de autorização para as opções básicas assim que o dispositivo for implementado.
Idioma	Por padrão, o idioma será específico do sistema operacional. Você pode alterá-lo para um idioma diferente na lista.
Converter todos os dispositivos direcionados para o Autopilot	Selecione esta opção para converter todos os dispositivos no grupo atribuído para o Autopilot.
Permitir pré-provisionamento	Selecione esta opção para registrar dispositivos para o Autopilot usando o processo normal de registro. Esta opção não ficará disponível quando a opção **Autoimplementação** estiver selecionada.
Configurar teclado automaticamente	Selecione **Sim** para pular a seleção de teclado caso a opção **Idioma** esteja definida em um valor diferente do valor padrão.
Modelo do nome do dispositivo	Insira um nome de modelo para ser utilizado durante o processo de registro do dispositivo.
Termos de licença do software Microsoft	Você pode exibir ou ocultar apenas no modo de Implementação movida pelo usuário.
Configurações de privacidade	Você pode exibir ou ocultar apenas no modo de Implementação movida pelo usuário.
Alterar opções de conta	Você pode exibir ou ocultar apenas no modo de Implementação orientada pelo usuário e quando o tipo de conta do usuário for do tipo Padrão.

Gerenciamento de Dispositivos Windows

O administrador pode configurar o recurso Autopilot em um locatário usando a nova opção Gerenciamento de Dispositivos Windows. Essa opção facilita a integração com o Ivanti Neurons for MDM caso o usuário tenha um ambiente AAD.

Para acessar essa opção, **Administrador** > **Microsoft Azure** > **Gerenciamento de Dispositivos Windows**.

Essa integração concede permissões ao Ivanti Neurons for MDM para gerenciar dispositivos, perfis do Autopilot, verificar a conformidade de dispositivos Windows e validar o locatário do Azure.

Tópicos relacionados

- TenantLockdown CSP

Criar Grupos de Dispositivos AAD

O administrador pode criar grupos de dispositivos AAD, conforme necessário, na seção Grupos de Dispositivos AAD. A validação do locatário do AAD deve ter sido configurada na seção Conformidade do Dispositivo para criar grupos de dispositivos do AAD.

Procedimento

1. Acesse **Administrador** > **Microsoft Azure** > **Grupos de Dispositivos AAD**.

   A página **Grupo de Dispositivos do Azure Active Directory** aparece na tela.

2. Clique em **ADICIONAR**.

   A página **Configurações do grupo** aparece na tela.

3. Forneça os seguintes detalhes:

   - Nome do grupo
   - Descrição do grupo
   - Tipo de participação
     - Dispositivo estático - o administrador obterá a lista de dispositivos estáticos disponíveis na janela **Atribuir Membros ao Grupo**. Selecione os dispositivos necessários e clique em **Salvar**.
     - Dispositivo dinâmico - o administrador deve fornecer determinados critérios da janela **Consulta dinâmica**.

O novo grupo de dispositivos AAD será criado, e o administrador poderá adicionar dispositivos ao grupo recém-criado.

Após a criação de um grupo dinâmico, os dispositivos serão, depois de algum tempo, listados na guia Dispositivos do grupo de dispositivos específico.

Editando dispositivos Autopilot

Os usuários podem editar dispositivos Autopilot no portal administrativo do Ivanti Neurons for MDM.

Pré-requisitos

Assegure que os pré-requisitos a seguir sejam atendidos:

- O usuário precisa ter uma licença do Microsoft Intune atribuída a ele
- Um nome amigável de usuário poderá ser definido somente se o usuário estiver definido
- O nome do dispositivo não poderá ter a definição removida após ser definido

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Administrador** > **Windows** > **Autopilot**. Os dispositivos Autopilot são listados na guia Autopilot Devices.
3. Clique em **Editar** (ícone do lápis). A página de edição aparece.
4. Edite os detalhes a seguir:
   - **Usuário**
   - **Nome legível para o usuário**
   - **Nome do dispositivo**
   - **Tag de grupo**
5. Clique em **Salvar**. Os detalhes do dispositivo são atualizados.

Excluindo dispositivos Autopilot

Os usuários podem excluir os dispositivos Autopilot no portal administrativo do Ivanti Neurons for MDM.

1. Faça login no portal administrativo do Ivanti Neurons for MDM.
2. Acesse **Administrador** > **Windows** > **Autopilot**. Os dispositivos Autopilot são listados na guia Autopilot Devices.
3. Clique em **Excluir**. Os detalhes do dispositivo são excluídos.

Trilhas de auditoria em perfis do Windows Autopilot

O recurso Trilhas de Auditoria monitora todas as atividades realizadas em todas as entidades dentro do Ivanti Neurons for MDM. Essas atividades incluem adicionar, excluir, atualizar novos dispositivos, etc.

Para obter mais informações, consulte Trilhas de auditoria.

Usando trilhas de auditoria, o administrador pode realizar as seguintes atividades em todos os dispositivos Windows registrados no modo Autopilot:

Perfis do Autopilot

- Criar
- Editar
- Excluir
- Atribuir o perfil a grupos

Dispositivos do Autopilot

- Carregar CSV
- Editar
- Excluir

TenantLockdown CSP

O administrador pode bloquear todos os dispositivos Windows para locatários usando o recurso TenantLockdown CSP. Para usar este recurso, os dispositivos devem ser registrados utilizando a opção Autopilot. Essa configuração pode ser feita no nível do dispositivo.

Nos modos Autopilot autoimplantado e orientado pelo usuário, o administrador pode bloquear os dispositivos diretamente para os locatários. Isso é útil quando os dispositivos são perdidos ou roubados. Nesses casos, mesmo se o dispositivo for reiniciado, o usuário será obrigado a se conectar ao locatário, e a criação da conta local não é compatível com o modo Autoimplantado. Mas se a criação da conta tiver de ser evitada no modo Orientado pelo usuário, o administrador deve ativar a opção **Ocultar** na configuração **Opções de alterar conta** durante a configuração Perfil do Autopilot.

O administrador pode ativar o TenantLockdown CSP criando uma Configuração de restrição do Windows e selecionando a opção **Exigir que os usuários se conectem à rede durante a configuração do dispositivo (é necessário o perfil do Autopilot)** em **Outras restrições**.

Para remover um dispositivo do TenantLockdown CSP, o administrador deve remover o dispositivo manualmente do grupo ou alterar as restrições.

Navegador ADMX (GPO)

Com o Navegador ADMX (GPO), você pode visualizar as configurações de GPO organizadas com base nos objetos ADMX que existem no locatário. É possível pesquisar e visualizar os objetos ADMX padrão, além de adicionar (carregar) os arquivos ADMX personalizados que fornecem uma estrutura baseada em XML para definir a exibição das configurações de GPO

Para carregar um objeto ADMX personalizado:

1. Selecione **Admin > Navegador ADMX (GPO)**. A página do **Navegador ADMX (GPO)** é exibida.
2. Clique em **Anexar**. A janela **Anexar Objetos ADMX (GPO) personalizados** é exibida.
3. Clique em **Escolher arquivo** para selecionar o arquivo ADMX a ser carregado.
4. Clique em **Anexar**. Uma mensagem de confirmação será exibida se o carregamento for concluído com êxito.

Pesquisando configurações de GPO

No navegador ADMX (GPO), você pode pesquisar e selecionar um GPO clicando no componente relevante da árvore hierárquica de GPO no painel esquerdo. A árvore hierárquica de GPO representa o caminho das configurações de política. Como alternativa, busque uma configuração de GPO específica digitando o nome do GPO ou o arquivo ADMX no campo Pesquisar. Os detalhes da configuração de GPO selecionada são exibidos no painel direito.

Configurando intervalos de inventário de aplicativos

Você pode definir intervalos de coleta de inventário de aplicativos do Windows 10 para vários inventários de tipos de fontes de aplicativos. Os intervalos são usados quando a configuração Privacidade é definida para coletar todos os aplicativos do dispositivo.

1. Navegue até Administrador > **Intervalos de inventário de aplicativos**.
2. Selecione o intervalo (em horas) para coletar o inventário de aplicativos da lista suspensa dos seguintes tipos de fontes de aplicativos.
   - **Intervalo de inventário que não é da App Store**
   - **Intervalo de inventário da App Store**
   - **Intervalo de inventário do sistema**
   - **Intervalo de inventário do Win32**
     As opções de intervalo para coletar o inventário de aplicativos Windows variam de **24** a **48** horas. O valor padrão é **24** horas.

Inventário de hardware

É possível ativar a coleta de informações de hardware em dispositivos Windows 10. Os detalhes do inventário de hardware são obtidos usando o Bridge.

1. Navegue até **Administrador > Inventário de hardware**.
2. Ative a opção **Ativar a coleta do inventário de hardware**.
3. Em **Intervalo do inventário**, selecione a frequência da coleta do inventário de hardware. Estas são as opções disponíveis:
    - **Uma vez por dia**(padrão)
    - **Uma vez por semana**
    - **A cada 30 dias**

Quando a opção de inventário de hardware está ativada, os detalhes do hardware do dispositivo são exibidos na guia **Hardware**, na página de detalhes do dispositivo.

Configuração com o Microsoft Azure

Esta seção contém os seguintes tópicos:

Usando o Microsoft Azure

Ivanti Neurons for MDM pode ser configurado com o Microsoft Azure para inscrição de seus usuários em desktops Windows e tablets que rodem Windows 10. Siga as etapas abaixo para configurar e conectar suas instâncias.

Esta seção contém os seguintes tópicos:

Configurando a conta AAD

Para configurar o Azure AD:

1. Acesse https://azure.microsoft.com/en-in/pricing/purchase-options/ para adquirir uma conta do Azure.
2. Use sua conta Hotmail ou Outlook.com existente ou crie uma nova conta e registre-se como um novo usuário.
3. Adquira uma conta do Azure usando uma das opções de pagamento e seguindo as etapas de verificação.
4. Peça para a Microsoft incluir o locatário do Ivanti Neurons for MDM na lista de permitidos.
5. Use a mesma conta do Hotmail ou Outlook.com usada na etapa 2 para efetuar login no AAD em https://manage.windowsazure.com/ como administrador.
6. Acesse a guia **Domínio**.

   Um domínio padrão, TestMiBGLRoutlook.onmicrosoft.com, será criado para sua conta, e todos os usuários criados pertencerão a esse domínio. Se necessário, é possível recriar um domínio customizado.

Criando usuários no Azure AD

Para criar usuários no Azure AD:

1. Acesse Active Directory - > **Diretório Padrão -> Usuários**.
2. Ao selecionar a opção Adicionar usuário -> Selecionar novo usuário em sua organização.
3. Insira o nome de usuário. Clique em avançar **(->)**.

   A página **Perfil do Usuário** será exibida.
4. Inclua as informações do usuário, tais como nome, sobrenome e o nome de exibição.
5. Use o menu suspenso para designar a função apropriada para o usuário.
6. Gere a senha temporária.

   Será solicitado que o usuário altere essa senha no primeiro login.

Conectando o AAD ao UEM para dispositivos Windows 10

Para conectar o AAD ao UEM:

1. **Acesse Administrador > Microsoft Azure > Registro e conformidade do Windows usando o AAD.**
2. Conclua as etapas de configuração do UEM descritas na seção "Configuração do gerenciamento de terminal unificado para Windows 10 com Azure Active Directory" na página 1342
3. Conclua a configuração "Atribuindo o aplicativo AAD UEM" na página 1344 no portal do Azure.
4. No Portal de administradores do Ivanti Neurons for MDM, digite o nome de domínio da sua conta AAD, clique no portal Connect Azure e marque a caixa de seleção.
5. Depois de fazer login, aceite o consentimento para que o aplicativo de validação de locatário do MobileIron AD verifique se o seu aplicativo Ivanti Neurons for MDM UEM está configurado. É exibida uma mensagem que indica que a conexão foi realizada com êxito.

Microsoft Passport for Work para dispositivos Windows 10

O Microsoft Passport for Work é pelo Windows Hello para Empresas. Para mais informações, consulte a "Configuração do Windows Hello para Empresas" na página 780.

Registro no AAD do dispositivo Windows

Pré-requisitos

Os usuários devem estar registrados no Ivanti Neurons for MDM.

Conecte seu domínio para registrar o usuário nos dispositivos Windows 10 Mobile.

1. Clique em **Entrar no Azure AD**.
2. Insira seu nome de usuário e senha.
3. Clique em **Entrar**.
4. Aceite o EULA
5. Clique em **Criar PIN**.
    - Se você tiver habilitado a complexidade de PIN do Microsoft Passport for Work, você será solicitado a configurar um PIN complexo de acordo com a política configurada.
    - O Azure AD autentica o usuário e faz download de um JWT (Token Web JSON) no dispositivo.
    - O dispositivo agora está registrado.
    - O usuário é contatado por meio do dispositivo para verificação.
6. Insira e confirme um PIN.
7. Clique em **OK**.

Suporte multiusuário para dispositivos Windows

Ivanti Neurons for MDM oferece suporte a recursos multiusuário para dispositivos Windows 10 inscritos no Azure AD. Esse recurso inclui enviar alguns perfis por push, como VPN, Wi-Fi, perfis de e-mail padrão do cliente e certificados, a um único usuário e não um dispositivo. Ele também suporta a distribuição de aplicativos internos e públicos para o usuário logado. Cada vez que um novo usuário Azure AD faz login em um dispositivo, o Ivanti Neurons for MDM avalia não apenas o dispositivo, mas também o usuário. Se o usuário for novo, o Ivanti Neurons for MDM atualizará o dispositivo para esse usuário. Se o usuário for um usuário existente no dispositivo, serão avaliadas quaisquer alterações no dispositivo e nas configurações de usuário que precisem ser atualizadas desde o último login.

Os detalhes do usuário do Azure AD que está logado no dispositivo são relatados no portal administrativo do Ivanti Neurons for MDM. Quando o usuário sai do dispositivo e o segundo usuário faz login no dispositivo, os detalhes do segundo usuário são atualizados na página de detalhes do dispositivo.

Como configurar o Microsoft Store for Business com UEM

O Microsoft Store for Business é um portal fornecida pela Microsoft como parte do Azure. Os administradores podem fazer login no portal e comprar apps e distribuí-los a todos os dispositivos gerenciados. Ivanti Neurons for MDM pode ser configurado com o Microsoft Store for Business para gerenciar aplicativos do portal do administrador do Ivanti Neurons for MDM configurando-se as seguintes etapas.

Etapa 1: registrar o aplicativo AAD no portal do Microsoft Azure

1. Abra o primeiro navegador e efetue login no portal do Microsoft Azure (https://portal.azure.com/).
2. Clique em **Registros de aplicativos** no painel esquerdo.
3. Clique em **+Novo registro de aplicativo**
4. Insira as informações a seguir para registrar o MobileIron como um aplicativo Azure:
    1. **Nome**: insira um nome para o aplicativo MobileIron. (Este campo é obrigatório e deve ter no mínimo 4 caracteres.)
    2. **Tipo de aplicativo**: selecione Aplicativo da Web/API.
    3. **URL de sign-on**: insira a URL que os usuários de dispositivos acessam para efetuar login no MobileIron (obrigatório).
5. Clique em **Criar** para adicionar o aplicativo e retornar à página inicial do Azure.
6. Vá para Configurações e crie uma nova chave.

Etapa 2: adicionar o aplicativo como uma ferramenta de gerenciamento

1. Em Configurações da Microsoft Store for Business, clique em Gerenciar
2. Configurações de distribuição
3. Na ferramenta Adicionar gerenciamento, ative o aplicativo criado.

Conectar a conta no portal do administrador

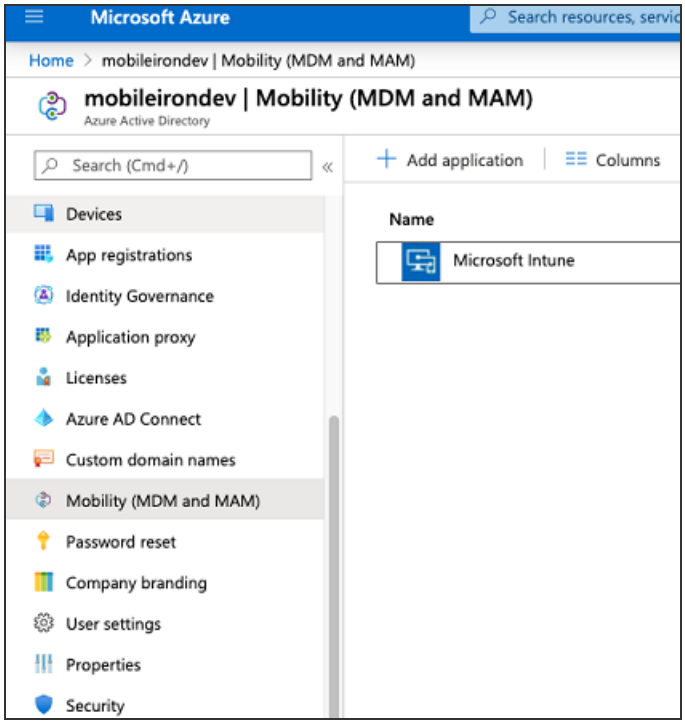
1. Acesse **Administrador > Microsoft Azure > Microsoft Store for Business**.
2. Na Etapa 1, **Registrar aplicativo AAD**, marque a caixa de seleção **Sim, conclui esta etapa**.
3. Na Etapa 2, **Adicionar ferramenta de gerenciamento**, marque a caixa de seleção **Sim, conclui esta etapa**.
4. Na Etapa 3, Conectar conta, atualize os seguintes campos:
    1. Domínio do Azure AD
    2. Identificador do aplicativo
    3. Chave de aplicativo
    4. Intervalo de sincronização (horas)
5. Clique em **Conectar**. Você verá uma mensagem de confirmação de que o MobileIron Store for Business foi configurado com êxito.
6. Clique em **Sincronizar aplicativo**. Quando sincronizado com êxito, o status é exibido como **Aplicativos sincronizados com êxito**.

Quando o Microsoft Store para aplicativos é enviado ao dispositivo, os detalhes do aplicativo são disponibilizados na guia **Apps instalados** nos detalhes do dispositivo. Cada aplicativo do Microsoft Store for Business reportado do dispositivo pode ser identificado como **Microsoft Store for Business** na coluna **Origem**.

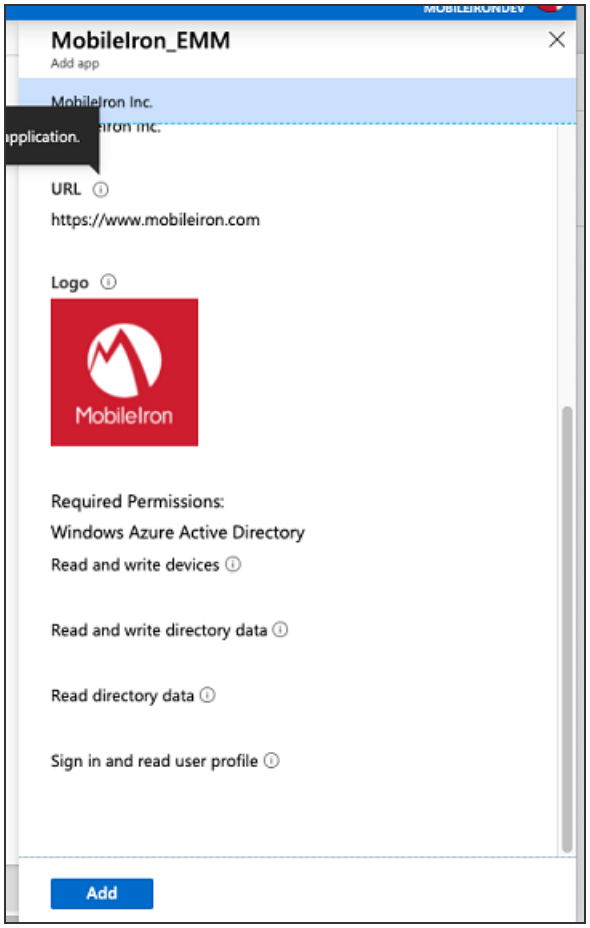
Configuração do gerenciamento de terminal unificado para Windows 10 com Azure Active Directory

Para configurar o Gerenciamento de terminal unificado (UEM) para Windows 10:

1. Faça login em https://portal.azure.com/ como usuário administrador e selecione Azure Active Directory.
2. Selecione "Mobilidade (MDM e MAM)" no painel do lado esquerdo e clique em **+Adicionar aplicativo**.



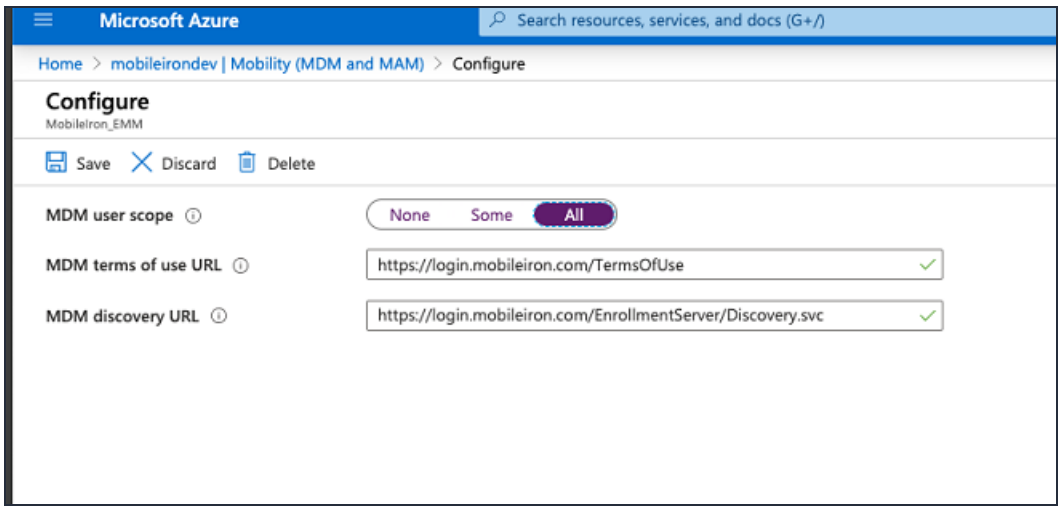
3. Selecione o aplicativo MobileIron_UEM na galeria de aplicativos e clique em **Adicionar**.



Atribuindo o aplicativo AAD UEM

Para concluir a configuração de atribuição de usuário:

1. Clique no aplicativo MobileIron UEM que você criou na Etapa 2 em "Configuração do gerenciamento de terminal unificado para Windows 10 com Azure Active Directory" na página 1342
2. No escopo do usuário do MDM, atribua o aplicativo aos seus grupos de usuários personalizados ou selecione **Todos**.



Conectar o Ivanti Neurons for MDM com o Azure Active Directory

Para trabalhar com o Azure Active Directory (AAD), você deve configurar o Ivanti Neurons for MDM com os detalhes da sua conta do Microsoft AAD. É necessário ter uma conta configurada do Microsoft AAD. Esta solução não requer conector presencial ou LDAP.

Esta seção contém os seguintes tópicos:

Casos de uso

Você pode conectar o Ivanti Neurons for MDM ao AAD para um dos seguintes casos de uso:

- Trabalhar com o Microsoft Office 365
- Configurar o Microsoft AAD, o Microsoft ADFS ou outro provedor de identidade (IdP) SAML 2.0 para autenticação de usuário
- Configurar o Microsoft AAD como sua origem de usuário
- Sincronize usuários do Microsoft AAD e comece. Todos os usuários e grupos em seu domínio do AAD serão sincronizados com sua instância do Ivanti Neurons for MDM

  Uma notificação é exibida na página **Notificações** se ocorrer um erro na sincronização AAD devido a um dos seguintes motivos:

  - O serviço AAD não pôde ser localizado
  - Todos os atributos de usuários não estão sincronizados com o AAD
  - Alguns atributos de usuário não estão sincronizados com o AAD

- Atualmente não há suporte para os ambientes com vários IdPs.
- Se você não estiver usando o Microsoft AAD como a sua origem do usuário, você poderá usar contas locais ou usuários de origem do LDAP. Isso requer a configuração do conector do Ivanti Neurons for MDM para acessar recursos LDAP no local.
- Atualmente não é possível usar o Microsoft AAD apenas para autenticação do usuário e usar um LDAP presencial para diretório de usuários.

Usando o Azure Active Directory

Para usar o AAD, configure seu provedor de identidade para autenticação de usuário em um dos seguintes métodos:

- Para usar o Microsoft AAD para origem de usuário e autenticação de usuário, configure o AAD como seu IdP. Acesse **Administrador > Identidade > Configuração de IdP do Ivanti Neurons for MDM** e selecione **AAD** no menu.
- Para usar o Microsoft AAD para origem de usuário e usar o ADFS para autenticação de usuário, configure o ADFS como seu IdP. Acesse **Administrador > Identidade > Configuração de IdP local** e selecione ADFS no menu.
- Para usar um IdP SAML 2.0 que não seja o AAD nem o ADFS para a autenticação de usuário, acesse **Administrador > Identidade> Configuração de IdP genérico** e siga as instruções na página.

Para mais informações, consulte "Configuração de provedor de identidade" na página 1244.

Configurações do Azure Active Directory

Este tópico ajuda você a definir as configurações do Azure Active Directory.

Procedimento

1. Acesse **Administrador > Microsoft Azure > Origem do Usuário AAD**.
2. Especifique os seguintes detalhes:

a. **Nome do AAD**.

b. **Intervalo de sincronização**: modifique a frequência com que o Ivanti Neurons for MDM sincroniza os dados de usuário do seu AAD.

c. **Ativar este AAD**: use esta opção para ativar ou desativar a instância do AAD.

d. Selecione **Convidar automaticamente usuários importados do AAD**: gerencie se os usuários importados do AAD para o Ivanti Neurons for MDM serão automaticamente convidados a se registrar via e-mail.

e. Selecione **ID Apple gerenciado**: escolha sincronizar o ID Apple Gerenciado para os usuários do AAD.

   - **Nenhum**
   - **Padrão:** endereço de e-mail do usuário.
     - (Opcional) Selecione a opção Incluir subdomínio "appleid" para evitar conflitos com os IDs Apple existentes.

f. (Opcional) Clique em **Adicionar atributos personalizados**: especifique atributos de usuário personalizados do serviço de diretório para aplicar ao gerenciamento de dispositivos. Cada atributo poderá então ser referenciado por ${attributeName} nos campos de configuração compatíveis com variáveis. O uso desta opção exibe uma implementação consistente de atributos personalizados em servidores AAD. Se um servidor AAD incluído em sua implementação não utilizar esse atributo, os recursos que dependem desse atributo poderão não funcionar conforme esperado.

3. Clique em **Salvar** depois de modificar as configurações do AAD.

Locatário do Azure

Esta seção contém os seguintes tópicos:

Esta seção descreve como configurar o Ivanti Neurons for MDM com locatário do Microsoft Azure.

Requisitos

Microsoft

Os clientes do Ivanti Neurons for MDM devem ter uma assinatura válida do Microsoft Intune e atribuir uma licença do Microsoft Intune aos usuários do dispositivo.

MobileIron

- Ivanti Neurons for MDM - o Ivanti Neurons for MDM, da versão 75 até a versão mais recente, é compatível com MobileIron.
- Licença adicional - A Conformidade de dispositivo do Azure é uma oferta Premium e está disponível para clientes de UEM seguro Premium e Platinum. Uma licença Platinum é suficiente para clientes existentes.
- Go para iOS (cliente) ou Go para Android (cliente) versão 75.0 até a versão mais recente com suporte do MobileIron.

Suporte a vários Ivanti Neurons for MDM

Se você tiver diversos Ivanti Neurons for MDM conectados ao mesmo locatário do Azure, desconecte-se de todos os Ivanti Neurons for MDM ou desative a política de conformidade para integração de conformidade do AAD, a partir de um Ivanti Neurons for MDM (único) específico, para que ele não carregue dados de dispositivo no Azure

Lembre-se de desativar a política de conformidade antes de desconectar o Ivanti Neurons for MDM.

Processo do administrador do Ivanti Neurons for MDM

O processo pela perspectiva do administrador do Ivanti Neurons for MDM:

1. O administrador aplica as licenças do Intune a usuários do dispositivo. Consulte "Aplicar a licença do Intune a usuários de dispositivos" na página 1351.
2. O administrador faz login no Portal do Azure.

3. O administrador adiciona MobileIron como um parceiro de conformidade do Azure. Consulte "Adicionar MobileIron como parceiro de conformidade" na página 1352.
4. O administrador cria a política de Acesso condicional para os aplicativos. Consulte "Criar uma política de acesso condicional no Microsoft Endpoint Manager" na página 1356.
5. O administrador configura a conexão entre o MobileIron e o Azure. Consulte "Conectando o Microsoft Azure ao Ivanti Neurons for MDM" na página 1361.
6. O administrador cria a política de conformidade de dispositivo no Ivanti Neurons for MDM. Consulte "Criar uma política de conformidade de dispositivo de parceiro" na página 1363.
7. A política de Acesso condicional entra em vigor. Dependendo da conformidade ou não do dispositivo, o acesso ao(s) aplicativo(s) é concedido ou negado.

A Ivanti recomenda que o administrador execute testes em cada aplicativo Microsoft.

Aplicar a licença do Intune a usuários de dispositivos

- Não utilize esse recurso se:
  - você estiver alterando usuários ou administrando situações em que os usuários provavelmente mudarão
  - o dispositivo for de propriedade de diversos usuários
- A Ivanti recomenda que você não realize **Atribuir ao usuário** e que não distribua a configuração de conformidade a dispositivos de diversos usuários como:
  - dispositivos com Login seguro WebClip
  - dispositivos iPad compartilhados
  - dispositivos Android no modo de quiosque

Ivanti Neurons for MDM requisitos de licença

A Conformidade de dispositivo é uma oferta Premium e está disponível para clientes de UEM seguro Premium e Platinum. Para clientes existentes, uma licença Platinum é suficiente.

Atribuir licenças em massa a usuários de dispositivos

Para atribuir licenças em massa a usuários de dispositivos existentes:

Atribuição com base em grupo

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

Atribuição baseada em PowerShell

https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

Adicionar MobileIron como parceiro de conformidade

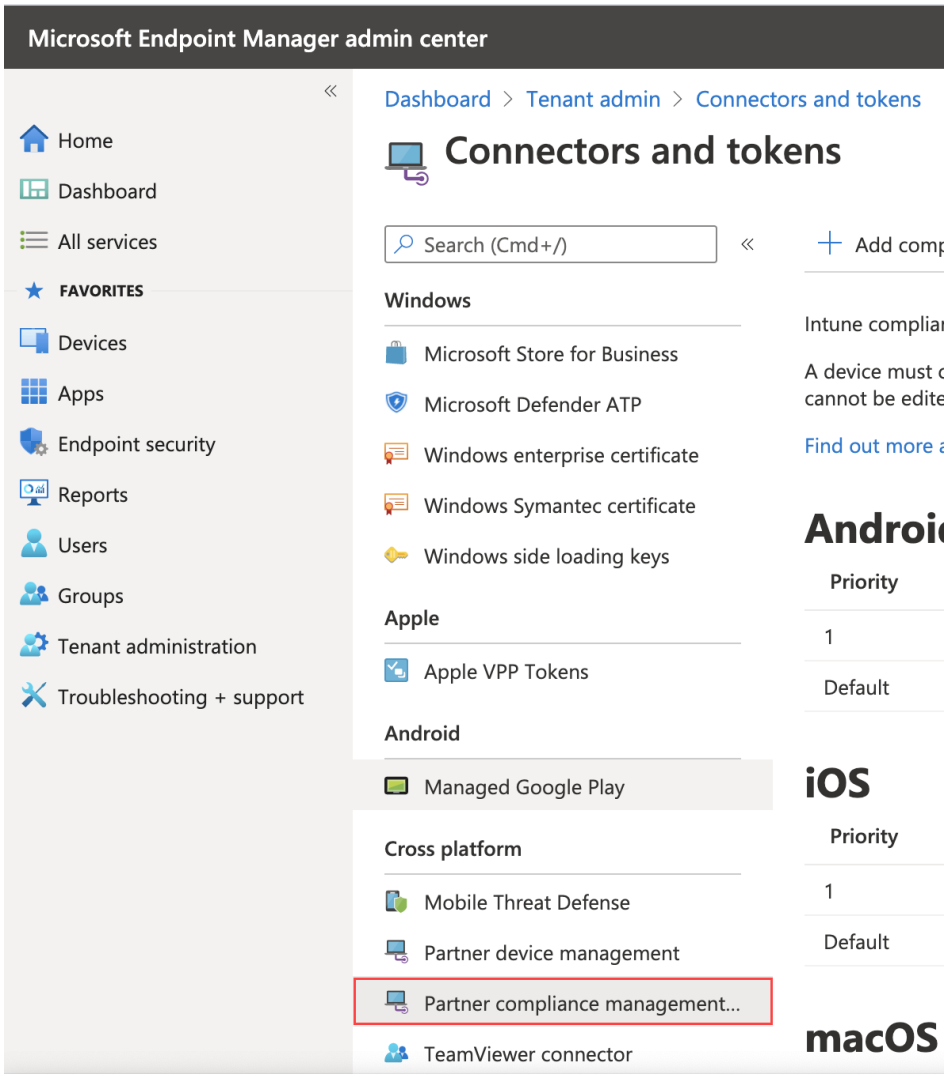
Pré-requisitos

- instalar uma licença do Microsoft Intune. Consulte "Aplicar a licença do Intune a usuários de dispositivos" na página 1351.
- ter usuários criados no Microsoft Azure
- ter grupos criados no Microsoft Azure

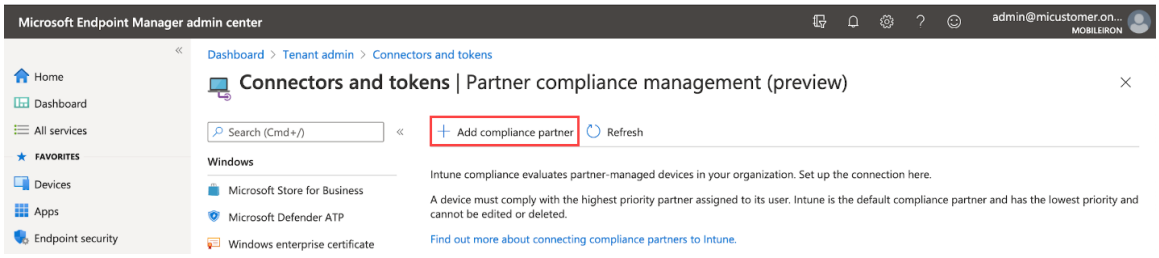
Procedimento

1. Faça login em: https://endpoint.microsoft.com.

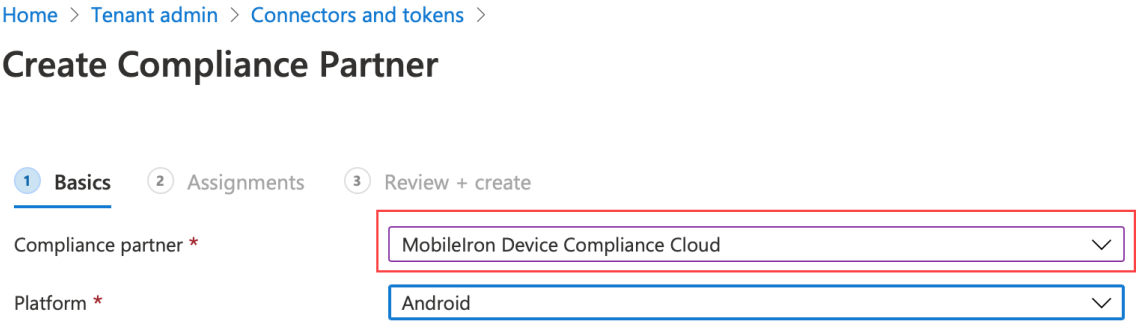
2. No painel esquerdo da página do centro de administração do Microsoft Endpoint Manager, clique em **Administrador de locatário**. Clique em **Connectors e tokens > Gerenciamento de conformidade do parceiro**.



3. À direita do campo Pesquisar, clique em **+ Adicionar parceiro de conformidade**.

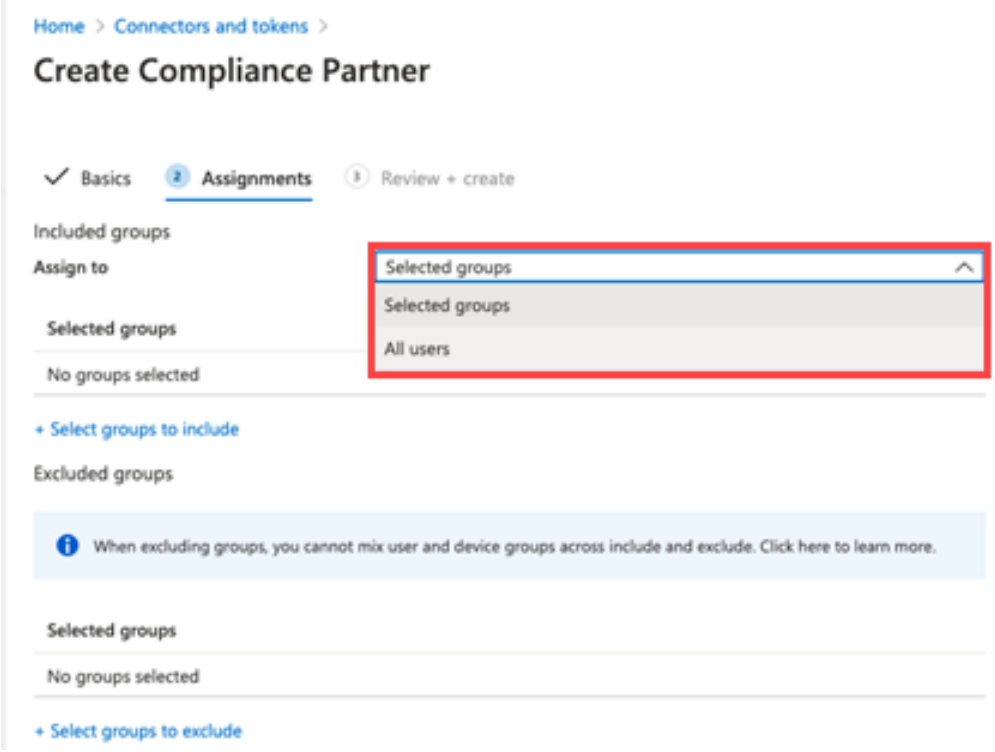


4. Na guia Noções básicas, selecione **Cloud de conformidade de dispositivo MobileIron** na lista suspensa do campo Parceiro de conformidade.



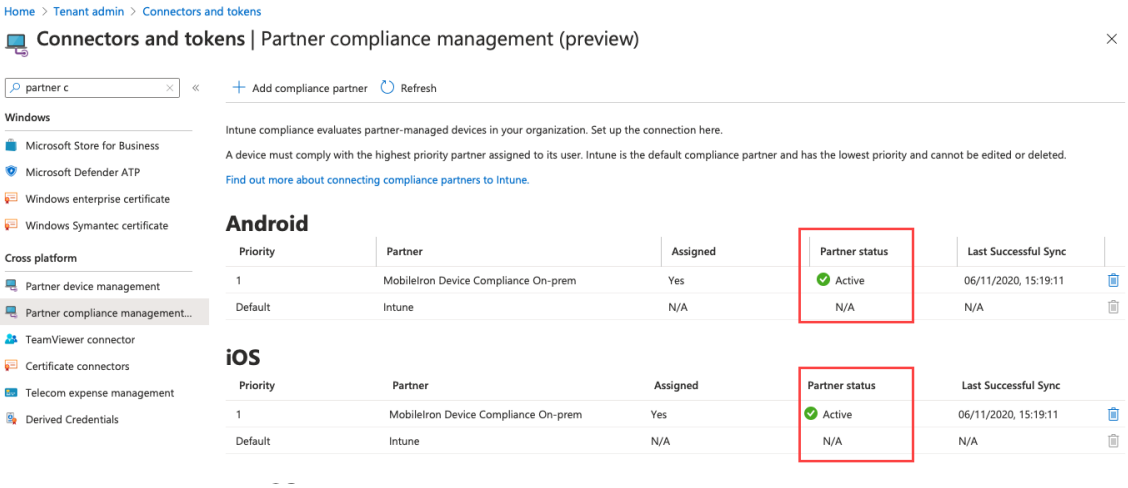
5. No campo Plataforma, selecione iOS ou Android e, em seguida, clique em **Avançar**.

6. Clique na guia **Atribuições**. Na lista suspensa Atribuir a, selecione o usuário/grupo de usuários de dispositivos que receberá o status de conformidade. Selecione o usuário/grupo que possui a licença.



7. Selecione **Avançar**.

8. Clique em **Criar**. O novo parceiro de conformidade aparecerá na página de Gerenciamento de conformidade do parceiro.



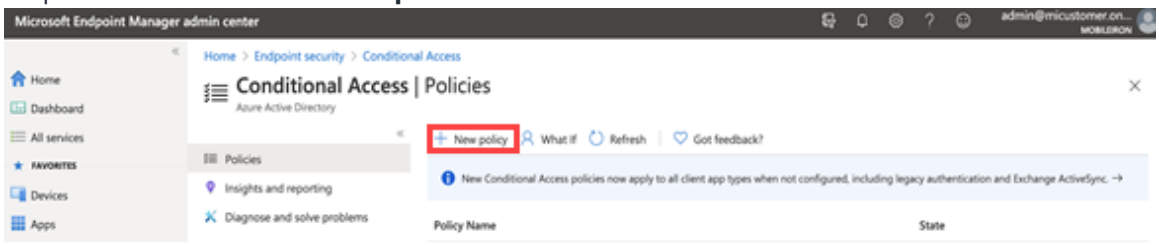
Criar uma política de acesso condicional no Microsoft Endpoint Manager

Procedimento

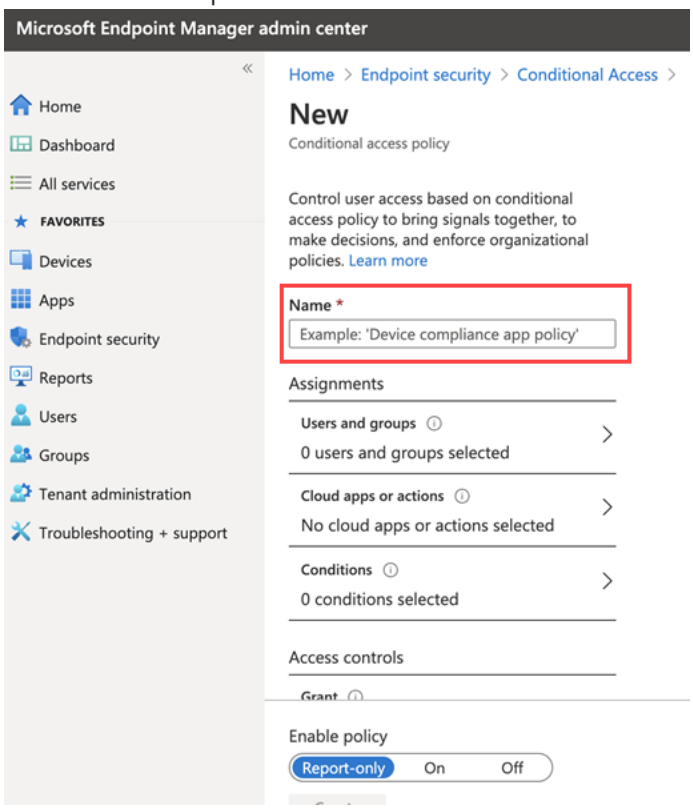
1. Faça login no Microsoft Endpoint Manager https://endpoint.microsoft.com.

2. Na página do centro de administração do Microsoft Endpoint Manager, vá até **Início > Segurança de ponto de extremidade > Acesso condicional**.

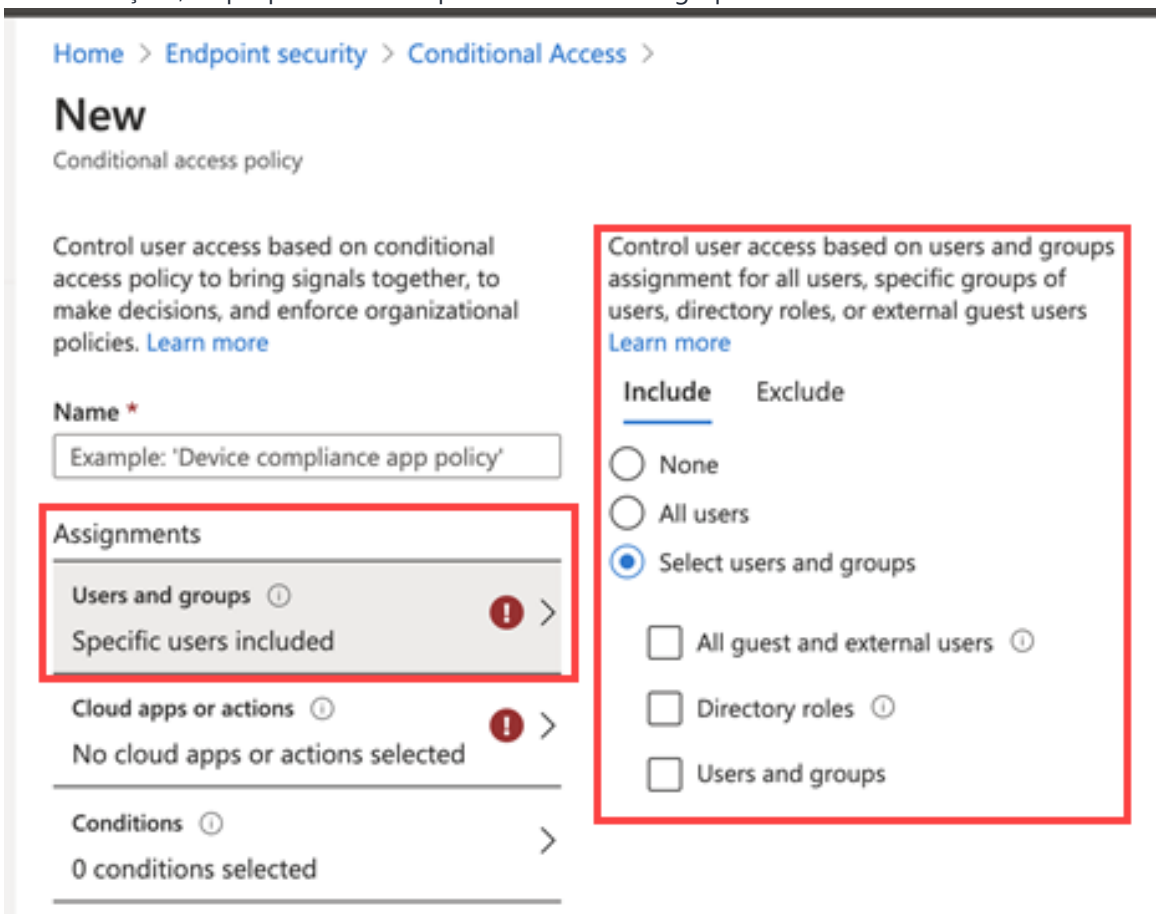
3. Clique em Políticas e em **+ Nova política**.



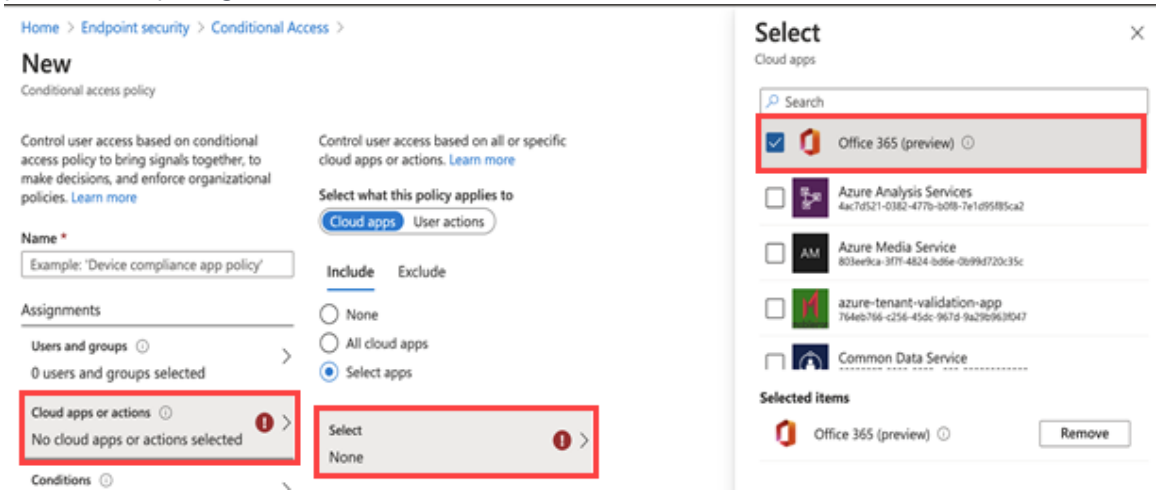
4. Insira o Nome da política de acesso condicional.



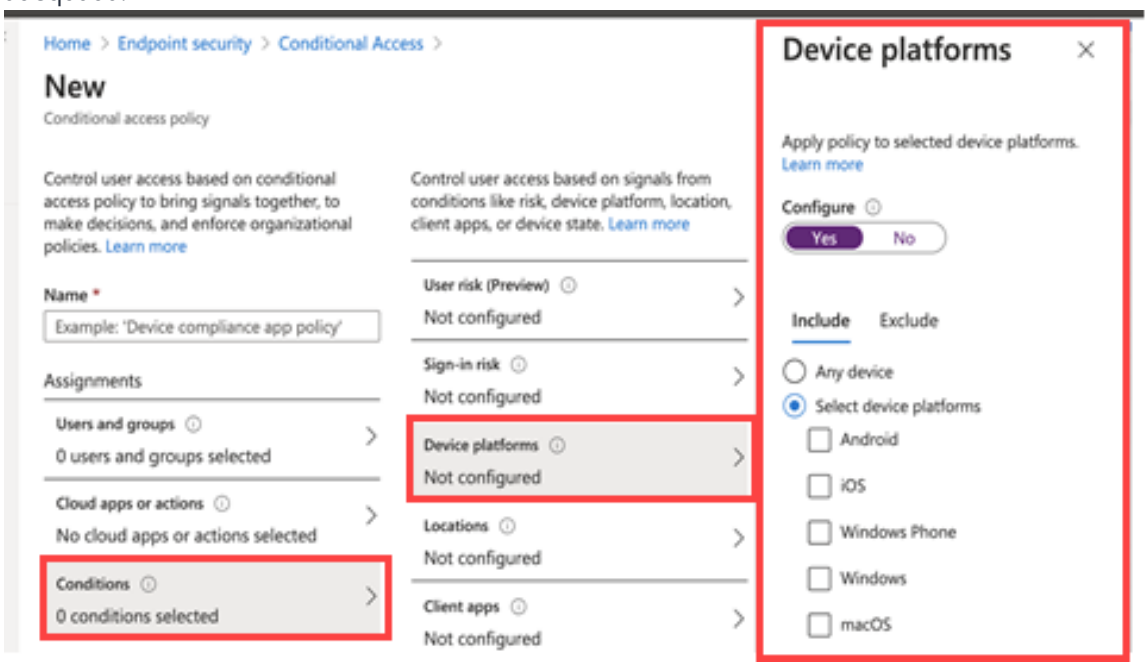
5. Em Atribuições, clique para atribuir a política a usuários e grupos.



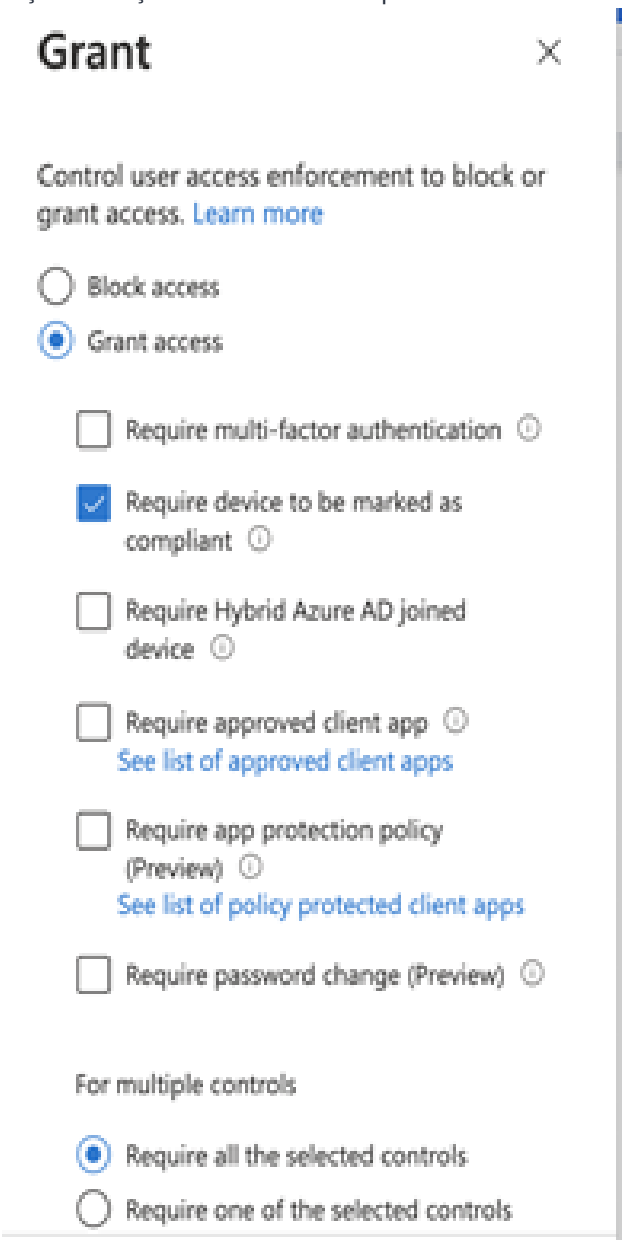
6. Clique em **Aplicativos na nuvem ou ações** e em **Selecionar**. Pesquise e selecione os aplicativos que precisam ser protegidos.



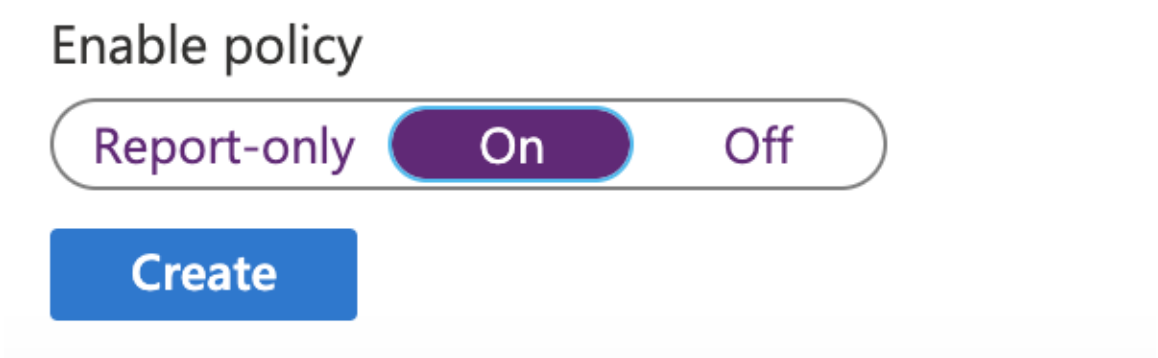
7. Clique em Condições e em **Plataforma do dispositivo**. Selecione a plataforma do dispositivo adequada.



8. Na **página Nova política de acesso condicional > Controles de acesso**, clique em **Conceder** e faça as seleções de acesso e bloqueio.



9. Para ativar a nova política, clique em **Ativar**.

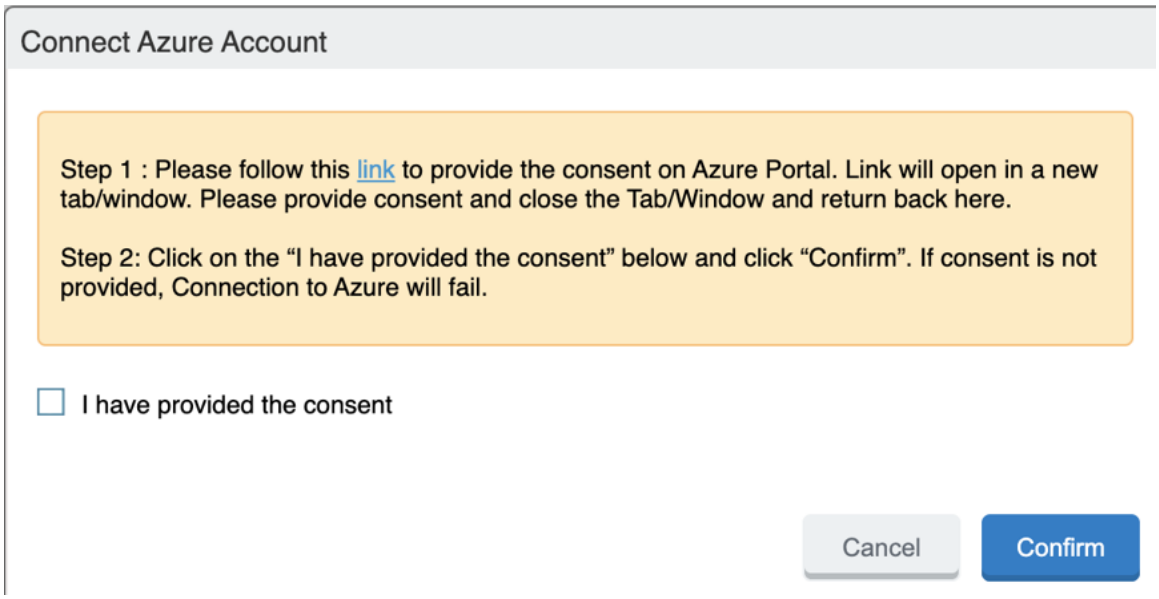


10. Clique em **Criar**.

Conectando o Microsoft Azure ao Ivanti Neurons for MDM

Procedimento

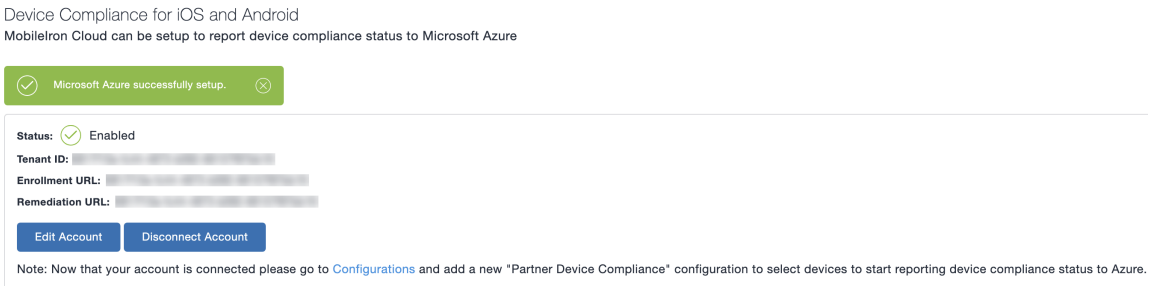
1. Faça login no Ivanti Neurons for MDM e acesse **Administrador** > **Microsoft Azure**.
2. No painel de navegação esquerdo, clique em **Microsoft Azure** > **Conformidade de dispositivos**.
3. Role até a seção **Conformidade de dispositivos para iOS e Android**. Clique em **Configurar conta**.
4. Na seção Conectar Conta, forneça os seguintes detalhes:
   - **ID de locatário do Azure** - Encontre em sua instância do Microsoft Azure.
   - **URL de registro** - (Opcional) Se o dispositivo não estiver registrado no MDM, os usuários serão direcionados para esse URL de registro. Ao configurar, use o formato HTTPS. Se você hospedar uma página em sua organização para redirecionar seus usuários de dispositivos para Informações de registro, adicione esse link aqui.
   - **URL de reparo** - (Opcional) Se o dispositivo não estiver em conformidade, os usuários do dispositivo serão direcionados para esse URL de reparo. Ao configurar, use o formato HTTPS. Se você hospedar uma página em sua organização para redirecionar seus usuários de dispositivos para Informações de reparo, adicione o link aqui.
5. Clique em **Conectar-se à conta**. A caixa de diálogo Conectar conta do Azure é exibida.



6. Na caixa de diálogo Conectar Conta do Azure, clique no **link**. presente na Etapa 1.
7. **Faça login**.
8. Revise as permissões e clique em **Aceitar**.

> Se você fizer login e a página solicitar que você faça login novamente, feche a guia/janela do navegador.

9. Volte ao Ivanti Neurons for MDM. Na caixa de diálogo Conectar conta do Azure, selecione a caixa **Eu forneci o consentimento**. Clique em **Confirmar**.



- Para editar a conta, clique em **Editar conta**.
- Para desconectar a conta, clique em **Desconectar conta**. Para instruções adicionais, consulte "Remoção do locatário do Azure" na página 1370.
- Todas as atividades de adição, edição e desativação de uma conta são registradas nos logs.

Criar uma política de conformidade de dispositivo de parceiro

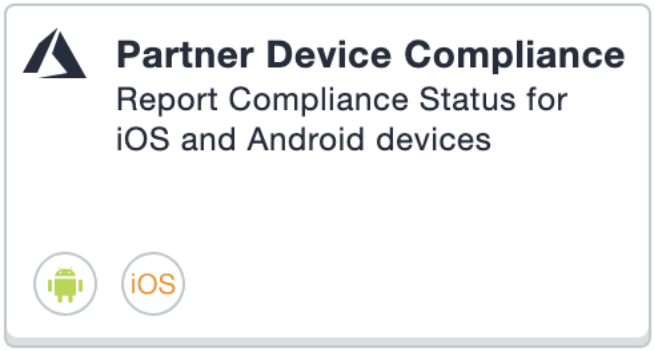
Crie uma política de conformidade de dispositivo parceiro no Ivanti Neurons for MDM e aplique o rótulo desejado. A política de conformidade de parceiro reporta o status de conformidade do dispositivo ao Azure para acesso condicional.

Pré-requisitos

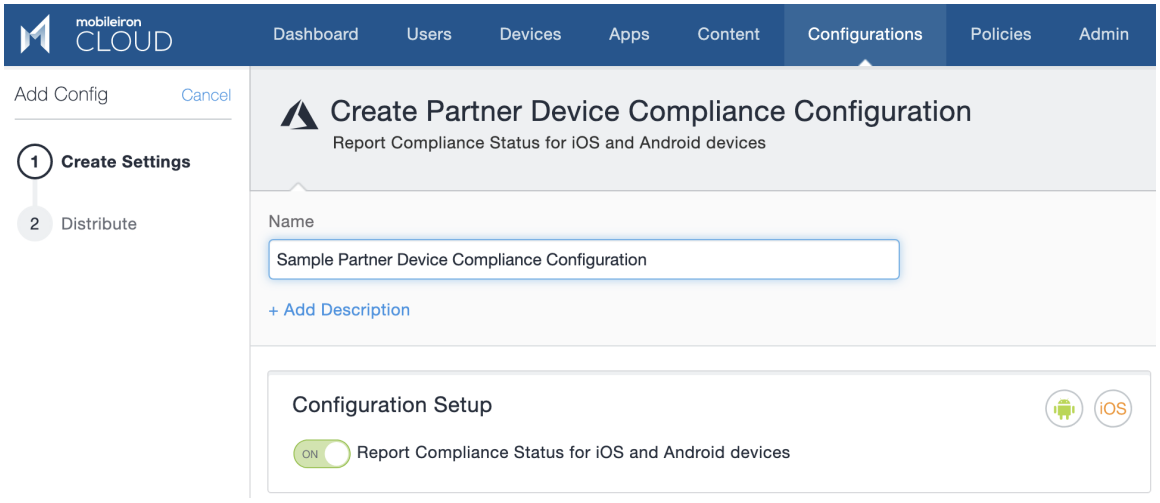
Você deve ter um ID de locatário do Azure configurado. Consulte "Conectando o Microsoft Azure ao Ivanti Neurons for MDM" na página 1361.

Procedimento

1. Faça login no portal administrativo do Ivanti Neurons for MDM, acesse **Configurações**.
2. Clique em **Adicionar novo > Conformidade de dispositivo do parceiro**. Como alternativa, na página **Configurações**, clique no bloco **Conformidade de dispositivo do parceiro**.

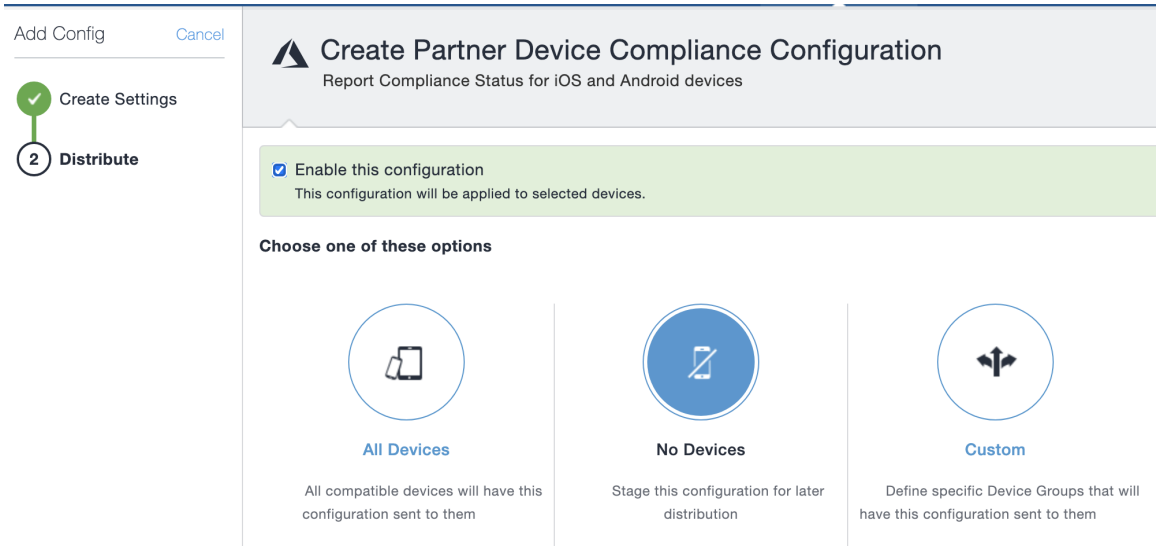


3. Na página **Criar configuração de conformidade de dispositivo parceiro**, use o formulário abaixo para inserir suas configurações.



Item	Descrição
Nome	Insira um nome.
+ Adicionar descrição	Insira uma explicação.
Relatar status de conformidade do dispositivo para o Azure em dispositivos iOS e Android	Ativado por padrão. Se não visualizar esse campo, será necessário antes configurar seu ID de locatário do Azure. Consulte "Conectando o Microsoft Azure ao Ivanti Neurons for MDM" na página 1361. Se a caixa de seleção Relatar status de conformidade do dispositivo para o Azure em dispositivos iOS e Android estiver ativada e a política de conformidade estiver aplicada ao cliente, o cliente exibirá "Acesso ao Microsoft 365" nos dispositivos em Configurações. O status de conformidade do dispositivo é relatado quando: • o dispositivo não estiver em conformidade • o dispositivo estiver em conformidade • o dispositivo retorna para em conformidade • 24 horas tiverem se passado. Se não houver alteração no status, um relatório será enviado uma vez por semana/a cada sete dias.

4. Clique em **Avançar**.



5. **Ativar essa configuração** está habilitado por padrão. Selecione um nível de distribuição para a configuração. Consulte "Adicionando uma configuração" na página 447.

> O Locatário do Azure não funciona em dispositivos macOS ou tvOS.

6. Clique em **Concluído**.

Relatório de status de dispositivo do Ivanti Neurons for MDM para o Azure

Para os casos a seguir, o Ivanti Neurons for MDM reporta o status de conformidade e inventário do dispositivo.

- Alteração de estado de conformidade do dispositivo
- Alteração de inventário do dispositivo
- Uma vez por semana, o Ivanti Neurons for MDM reporta o status de conformidade e do inventário

Dependendo da ação selecionada na política de conformidade, o seguinte status do dispositivo será enviado:

TABLE 2. AÇÕES NA POLÍTICA DE CONFORMIDADE

Ação **(a mais restritiva se aplica)**	**O que o Ivanti Neurons for MDM envia**
Bloquear e-mail, Aplicativos de AppConnect, Quarentena	Dispositivo não em conformidade
Enviar alerta	Conformidade com o Azure
Desativar dispositivo	Dados do dispositivo removidos da plataforma do Azure

Página de Detalhes do dispositivo

Para exibir as informações do Azure sobre o dispositivo, vá até a página de Detalhes do dispositivo. A descrição dos campos e seus possíveis valores:

TABLE 3. DETALHES DE DISPOSITIVO DO AZURE

Campo	Descrição
Identificador de dispositivo do Azure	O ID do dispositivo reportado pela Microsoft ao dispositivo iOS ou Android. Por exemplo: 007c8232-9489-4074-9b35-345b16f0a72d. O Ivanti Neurons for MDM recebe esse ID de dispositivo quando os usuários do dispositivo precisam se registrar no aplicativo Microsoft Authenticator para usar esse recurso. Se não for possível recuperar o ID de dispositivo, esse campo será deixado em branco.
Status de conformidade do dispositivo do Azure	Lista o status de conformidade do dispositivo no Azure. Valores possíveis: • Em andamento • Bem-sucedido • Falha

TABLE 3. DETALHES DE DISPOSITIVO DO AZURE (CONT.)

Campo	Descrição
Código de status do cliente Azure	Indica se o dispositivo está conectado ao Azure. Valores possíveis: • Success - Pode recuperar o ID do dispositivo. • Internal_Error - Ocorreu um erro irrecuperável no cliente ou no lado do servidor. • Workplace_Join_Required - Registro do dispositivo necessário. O usuário do dispositivo pode mitigar esse status. • Interaction_Required - Um login interativo é necessário. O usuário do dispositivo pode mitigar esse status. • Server_Declined_Scopes - Não foi concedido o acesso a alguns escopos. • Server_Protection_Policies_Required - O recurso solicitado é protegido por uma política de Acesso condicional do Intune. • User_Canceled - O usuário do dispositivo cancelou a sessão de autenticação da Web tocando no botão "Concluído" ou em "Cancelar" no navegador da Web. • Account_logged_out - Conta desconectada.
Hora do relatório de conformidade do dispositivo do Azure	A hora em que o Ivanti Neurons for MDM reportou o status de conformidade do dispositivo ao Microsoft Intune. Um campo em branco indica uma das opções a seguir: • esse recurso está desativado • O Ivanti Neurons for MDM recebeu os dados e ainda precisa chamar a API da Microsoft • há um erro como user_Cancelled ou Erro interno

Remoção do locatário do Azure

Se diversos Ivanti Neurons for MDM estiverem habilitados para usar o mesmo locatário do Azure, remova-o de todos os Ivanti Neurons for MDM. Se um único Ivanti Neurons for MDM precisar parar de usar o Azure, é possível desativar a política de conformidade de parceiro apenas desse Ivanti Neurons for MDM.

Se o administrador realizar uma desconexão no Ivanti Neurons for MDM, então, o Ivanti Neurons for MDM parará de reportar o inventário do dispositivo e o status de conformidade ao Azure.

Pré-requisitos

- garantir todos os dispositivos como não gerenciados
- garantir todos os dispositivos como em não conformidade

Procedimento

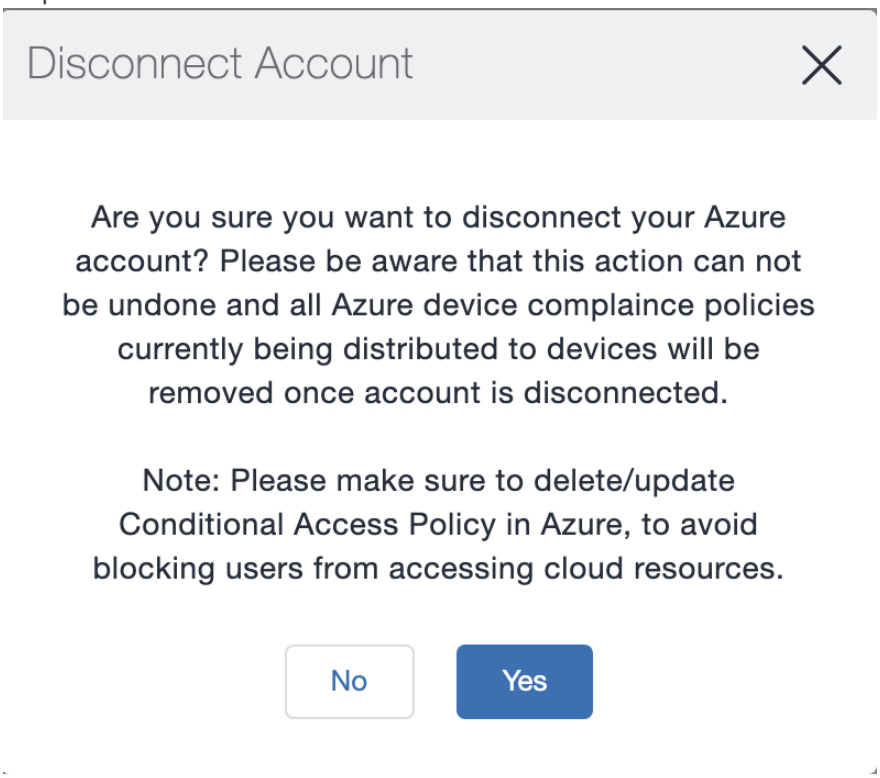
Microsoft

1. Faça login no Microsoft Azure.
2. Vá até **Intune > Acesso condicional**. Certifique-se de que a política de acesso condicional esteja desativada.

Ivanti Neurons for MDM

1. Faça login no Ivanti Neurons for MDM e vá até **Administrador**.
2. No painel de navegação esquerdo, clique em **Microsoft Azure > Conformidade de dispositivos para iOS e Android**.

3. Clique em **Desconectar conta**.



4. Clique em **Sim**.

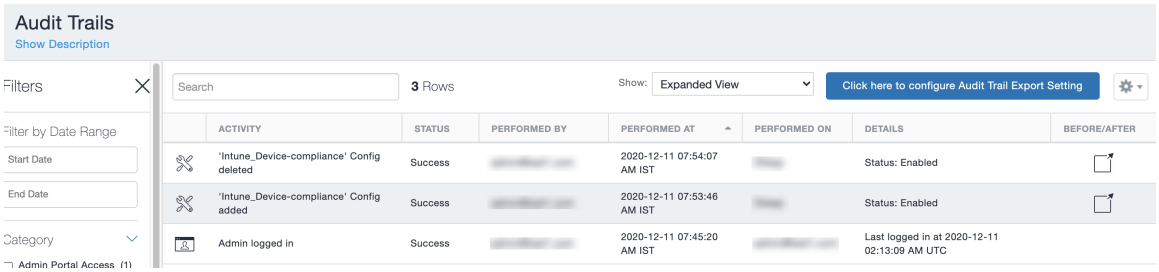
Remover um dispositivo do Azure

Depois de remover o dispositivo, o Ivanti Neurons for MDM reporta ao Azure que o dispositivo não está mais em gerenciamento e não está em conformidade.

O Azure exclui a entrada do dispositivo desativado após 90 dias.

Atividade da conta do Azure registrada nos logs

Toda a atividade é registrada nos logs.



Administrador > Microsoft Azure > Proteção de aplicativo do Office 365

Licença: Gold

Você pode configurar as políticas de proteção de aplicativo do Office 365 para ajudar a proteger os dados da sua empresa. As políticas impõem os controles de prevenção de perda de dados (DLP) aos apps do Microsoft Office 365 usando APIs do Microsoft Graph. Algumas destas APIs de gráfico permitem que os administradores reforcem a proteção de aplicativo para apps iOS e Android nativos que utilizam o SDK gráfico.

Use este recurso para aplicar políticas como:

- Impedir os usuários de imprimir de apps do Office 365.
- Impedir o compartilhamento de dados de saída de apps do Office 365.
- Forçar o PIN para apps do Office 365.
- Desativar a sincronização de contatos de apps do Office 365.

Pré-requisitos da proteção de aplicativos do Office 365

Antes de usar a proteção de aplicativos do Office 365, é necessário:

- Uma licença válida do MobileIron.
- Recurso de Proteção de aplicativos do Office 365 ativado no Ivanti Neurons for MDM
- Uma assinatura do Intune ou uma assinatura EMS da Microsoft que inclua o Intune.
    - Cada uso ao qual a política se aplica requer uma licença, no entanto a ativação e o teste da integração requerem apenas uma única licença.
- Uma assinatura válida do Office Enterprise ou Business com acesso ao apps do Office 365 em um dispositivo móvel.
- Um ou mais apps do Office 365.
- Sincronizar os usuários do seu Active Directory com o Azure Active Directory.

- One Drive for Business instalado nos dispositivos para proteger os dados no Word, Excel e PowerPoint. Isto não é obrigatório.
- Acesso ao portal Microsoft Azure (https://portal.azure.com/) para configurar as políticas de proteção do aplicativo Intune.
- O aplicativo Intune Company Portal instalado em dispositivos Android.
  Os usuários dos dispositivos não precisam efetuar login, mas o aplicativo precisa estar instalado no dispositivo para proteger os dados. A proteção se aplicará quando o usuário se registrar no aplicativo.

Registro do MobileIron como um aplicativo do Azure

Este tópico descreve como registrar e armazenar suas credenciais de locatário do Azure no software Ivanti Neurons for MDM e gerenciar remotamente as políticas de proteção para aplicativos Android e iOS do Office 365 na nuvem do Microsoft Azure. Embora não seja necessário, você poderá abrir dois navegadores para executar as etapas nos procedimentos a seguir. Use o primeiro navegador para efetuar login no portal do Microsoft Azure. Use o segundo navegador para efetuar login no portal administrativo do Ivanti Neurons for MDM.

Procedimento para o portal do Microsoft Azure

Ocasionalmente, a Microsoft pode alterar a interface do usuário do portal do Azure. Estas instruções pressupõem que você tenha familiaridade com o Portal do Microsoft Azure e possa fazer os ajustes necessários ao registrar o MobileIron como um aplicativo Azure.

1. Abra o primeiro navegador e efetue login no portal do Microsoft Azure (https://portal.azure.com/).
2. Clique em **Registros de aplicativos** no painel esquerdo.
3. Clique em **+Novo registro de aplicativo**.
4. Insira as informações a seguir para registrar o MobileIron como um Azure.
   - **Nome:** insira um nome para o aplicativo MobileIron. (Este campo é obrigatório e deve ter no mínimo 4 caracteres.)
   - **Tipo de aplicativo:** Selecione Aplicativo da Web/API.

- **URL de sign-on:** insira a URL que os usuários de dispositivos acessam para efetuar login no MobileIron (obrigatório).

5. Clique em **Criar** na parte inferior do painel para adicionar o aplicativo e retornar à página inicial do Azure.
6. Clique no aplicativo MobileIron recém-criado na página inicial do Azure.
7. Retorne à página inicial do Azure para atribuir as permissões ao aplicativo MobileIron Azure.
8. Para definir as permissões de API necessárias para o aplicativo MobileIron recém-criado, clique no nome do aplicativo em Registros de aplicativos.
9. Clique em **Permissões de API** > **Adicionar uma permissão**.
10. Na seção **Microsoft Graph > Permissões delegadas > Apps de gestão do dispositivo**, selecione a permissão **DeviceManagementApps.Read.All** e clique em **Salvar**. Por padrão, a permissão user.Read é ativada para o aplicativo.
11. Para conceder acesso, clique em **Conceder consentimento de administrador para o MobileIron**.
12. Realize o seguinte procedimento para o portal de administrador do Ivanti Neurons for MDM.

Procedimento para Portal Administrativo do Ivanti Neurons for MDM

1. Abra o segundo navegador e efetue login no portal de administrador do Ivanti Neurons for MDM.
2. Acesse **Administrador > Microsoft Azure > Proteção de aplicativo do Office 365**.
3. Cole o **ID do Aplicativo** no portal administrativo do Ivanti Neurons for MDM.

   Procedimento

   a. Acesse o portal do Azure.

   b. Selecione o aplicativo MobileIron > **Propriedades**.

   c. Copie o **ID do aplicativo**.

   d. Volte para **Administrador > Microsoft Azure > Proteção de aplicativo Office 365** no Portal do administrador.

   e. Cole-o no campo **ID do aplicativo**.

4. Cole o **Segredo do Aplicativo** (Segredo do Cliente) no portal administrativo do Ivanti Neurons for MDM.

   Procedimento

   a. Acesse o portal do Azure.

   b. Selecione o aplicativo MobileIron.

   c. Clique em **Chaves**, digite um nome em **Descrição da chave** e selecione um período de expiração em **Duração**.

   d. Clique em **Salvar** e copie o valor **Chave**.

   e. Volte para **Administrador > Microsoft Azure > Proteção de aplicativo Office 365** no Portal do administrador.

   f. Cole-o no campo **Segredo do aplicativo** (Segredo do cliente).

5. Cole o **ID do Locatário** no portal administrativo do Ivanti Neurons for MDM.

   Procedimento

   a. Acesse o portal do Azure.

   b. Clique em Azure Active Directory no painel esquerdo e clique em Propriedades.

   c. Copie o ID do diretório.

   d. Volte para **Administrador > Microsoft Azure > Proteção de aplicativo Office 365** no Portal do administrador.

   e. Cole-o no campo **ID do locatário**.

6. Insira seu **Nome de usuário** e sua **Senha** de administrador do Intune.

   - A conta do Azure deve ter direitos administrativos globais ou direitos administrativos limitados + direitos de administração do serviço Intune.

- A Ivanti recomenda a criação de uma conta local do Azure apenas com os direitos de administração do serviço Intune. Contas do usuário que são federadas para um provedor de identidade não têm suporte da Microsoft para autenticação com as APIs do Microsoft Graph.
- A conta não pode ter nenhum requisito de MFA. Caso contrário, a autenticação falharia.

7. Clique em **Autenticar e salvar**.

   Se a data enviada estiver incorreta, uma mensagem de erro será exibida.

Políticas para a Proteção de aplicativos do Office 365

Depois de configurar as credenciais do Microsoft Graph, acesse **Apps > Proteção do aplicativo Office 365** para adicionar novas políticas de proteção de aplicativos do Office 365 para dispositivos iOS ou Android em diferentes grupos de usuários.

As políticas são listadas na página **Apps > Proteção de aplicativo do Office 365**, na aba **Políticas de aplicativo**. A lista de política fornece detalhes tabulares tais como o carimbo de data e hora atualizado, plataforma, apps atribuídos e grupos de usuário implementados.

Adição de política de proteção de aplicativos do Office 365 para dispositivos iOS

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Políticas do aplicativo > +Adicionar**.
3. Insira um **Nome** e uma **Descrição** opcional para a política.
4. Em Escolher SO, clique em **iOS**.

5. Em **Realocação de dados**, selecione uma das seguintes configurações e opções:
    - Impedir backup de iTunes e iCloud
    - Permitir que aplicativo transfira dados para outros apps - Todos os apps (padrão), Apps gerenciados por política, Nenhum
    - Permitir que aplicativo receba dados de outros apps - Todos os apps (padrão), Apps gerenciados por política, Nenhum
    - Impedir "Salvar como"
    - Restringir ações recortar, copiar e colar em outros apps - Todos os apps (padrão), Bloqueado, Apps gerenciados por política, Aplicativo gerenciado por política com ação colar
    - Restringir conteúdo da Web a ser exibido no navegador gerenciado
    - Criptografar dados de aplicativo - Quando o dispositivo estiver bloqueado (padrão), Quando o dispositivo estiver bloqueado e houver arquivos abertos, Após a reinicialização do dispositivo, Usar configurações do dispositivo
    - Desativar sincronização de contatos
    - Desativar impressão
6. Em **Acessar**, selecione entre as seguintes configurações e opções:
    - Exigir PIN para acesso
    - Número de tentativas antes da redefinição do PIN (padrão de 5)
    - Permitir PIN simples
    - Tamanho do PIN (padrão de 4)
    - Permitir impressão digital em vez do PIN (iOS 8+)
    - Desativar PIN do aplicativo quando PIN do dispositivo for gerenciado
    - Exigir credenciais corporativas para acesso

- Bloquear aplicativos gerenciados de serem executados em dispositivos com desbloqueio ou com raiz
- Verificar novamente os requisitos de acesso após (minutos)
  - Tempo limite - Deve ser um valor entre 1 e 65535 (padrão de 30)
  - Off-line - Período de carência - Deve ser um valor entre 1 e 65535 (padrão de 720)
  - Intervalo off-line (dias) antes do apagamento dos dados de aplicativo - deve ser um valor entre 1 e 65535 (padrão é 90)
- Exigir sistema operacional iOS mínimo
- Exigir sistema operacional iOS mínimo (somente aviso)
- Exigir versão mínima do aplicativo
- Exigir versão mínima do aplicativo (somente aviso)
- Exigir versão mínima do SDK da política de proteção do aplicativo Intune

7. Clique em **Avançar**.
8. Selecione e atribua os apps que serão afetados pela política.
9. Clique em **Avançar**.
10. Selecione os grupos de usuários aos quais esta política será aplicada.
11. Clique em **Concluído**.

Adição de política de proteção de aplicativos do Office 365 para dispositivos Android

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Políticas do aplicativo > +Adicionar**.
3. Insira um **Nome** e uma **Descrição** opcional para a política.
4. Em Escolher SO, clique em **Android**.

5. Em **Realocação de dados**, selecione uma das seguintes configurações e opções:

    - Impedir backup de Android
    - Permitir que aplicativo transfira dados para outros apps - Todos os apps (padrão), Apps gerenciados por política, Nenhum
    - Permitir que aplicativo receba dados de outros apps - Todos os apps (padrão), Apps gerenciados por política, Nenhum
    - Impedir "Salvar como"
    - Restringir ações recortar, copiar e colar em outros apps - Todos os apps (padrão), Bloqueado, Apps gerenciados por política, Aplicativo gerenciado por política com ação colar
    - Restringir conteúdo da Web a ser exibido no navegador gerenciado
    - Criptografar dados de aplicativo
    - Desativar criptografia de aplicativo quando a criptografia do dispositivo estiver ativada
    - Desativar sincronização de contatos
    - Desativar impressão

6. Em **Acessar**, selecione entre as seguintes configurações e opções:
    - Exigir PIN para acesso
    - Número de tentativas antes da redefinição do PIN (padrão de 5)
    - Permitir PIN simples
    - Tamanho do PIN (padrão de 4)
    - Permitir impressão digital em vez do PIN (Android 6+)
    - Desativar PIN do aplicativo quando PIN do dispositivo for gerenciado
    - Exigir credenciais corporativas para acesso
    - Bloquear aplicativos gerenciados de serem executados em dispositivos com desbloqueio ou com raiz
    - Verificar novamente os requisitos de acesso após (minutos)
        - Tempo limite - Deve ser um valor entre 1 e 65535 (padrão de 30)
        - Off-line - Período de carência - Deve ser um valor entre 1 e 65535 (padrão de 720)
        - Intervalo off-line (dias) antes do apagamento dos dados de aplicativo - deve ser um valor entre 1 e 65535 (padrão é 90)
    - Bloquear captura de tela e assistente do Android
    - Exigir sistema operacional Android mínimo
    - Exigir sistema operacional Android mínimo (somente aviso)
    - Exigir versão mínima do aplicativo
    - Exigir versão mínima do aplicativo (somente aviso)
    - Exigir versão mínima do SDK da política de proteção do aplicativo Intune
7. Clique em **Avançar**.
8. Selecione os apps que serão afetados pela política.
9. Clique em **Avançar**.

10. Selecione os grupos de usuários aos quais esta política será aplicada.
11. Clique em **Concluído**.

Modificação de uma política de proteção de aplicativos do Office 365

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Políticas de aplicativos**.
3. Clique no nome da política que deseja modificar.
4. Na página de detalhes da política, clique em **Editar**.
5. Modifique as configurações da política.
6. Clique em **Avançar**.
7. Modifique a lista de apps aos quais esta política será aplicada.
8. Clique em **Avançar**.
9. Modifique os grupos de usuários aos quais esta política será aplicada.
10. Clique em **Concluído**.

Exclusão de uma política de proteção de aplicativos do Office 365

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Políticas de aplicativos**.
3. Na coluna **Ações**, clique no ícone de remoção no nome da política que deseja excluir.
4. Clique em **Sim** para confirmar.

Configurações de aplicativos do Office 365

Acesse a página **Apps > Proteção de aplicativos do Office 365** na aba **Configurações de aplicativo** para adicionar, modificar ou excluir as Configurações de aplicativo do Office 365 para grupos de usuários diferentes. Nessas configurações do aplicativo, os administradores podem adicionar uma lista de pares de valor-chave. e atribua as configurações para um ou mais apps do Office 365. A aba Configuração do aplicativo lista as configurações com detalhes tabulares como o carimbo de data e hora atualizado, apps atribuídos e status de implementação.

Como adicionar uma configuração aos aplicativos do Office 365

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Configurações do aplicativo > +Adicionar**.
3. Insira um **Nome** e uma **Descrição** opcional para a configuração.
4. Insira os pares de valor-chave.
5. Clique em **Avançar**.
6. Selecione os apps aos quais esta configuração será aplicada.
7. Clique em **Avançar**.
8. Selecione os grupos de usuário aos quais esta configuração será aplicada.
9. Clique em **Concluído**.

Como modificar a configuração dos aplicativos do Office 365

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Configuração do aplicativo**.
3. Clique no nome da configuração que deseja modificar.
4. Na página de detalhes da configuração, clique em **Editar.**

5. Outra opção é clicar nas abas **Distribuição de aplicativos** ou **Distribuição de grupos de usuário**. Clique em **Editar** para modificar apenas essas configurações e clique em **Salvar**.

6. Modifique as configurações.

7. Clique em **Avançar**.

8. Modifique a lista de apps aos quais esta configuração será aplicada.

9. Clique em **Avançar**.

10. Modifique os grupos de usuário aos quais esta configuração será aplicada.

11. Clique em **Concluído**.

Como excluir a configuração dos aplicativos do Office 365

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.

2. Clique em **Configuração do aplicativo**.

3. Na coluna **Ações**, clique no ícone de remoção do nome da configuração que deseja excluir.

4. Clique em **Sim** para confirmar.

Usuários que não estão em conformidade com os apps do Office 365

Os administradores podem rever a lista de usuários e seus dispositivos devido a não conformidade. Use esta página para apagar qualquer aplicativo do Office 365 em dispositivos sinalizados.

Como apagar apps do Office 365

Procedimento

1. Acesse **Apps > Proteção de aplicativos do Office 365**.
2. Clique em **Usuários que não estão em conformidade**.

3. Execute uma das seguintes ações:
    - Selecione os usuários da lista e clique em **Apagar apps do Office 365**.
    - Clique no nome do usuário para exibir a lista de dispositivos que possuem apps que não estão em conformidade. Na coluna **Ação**, clique no ícone **Apagar apps do Office 365** em relação a um dispositivo específico.
    - Clique no nome do usuário para exibir a lista de dispositivos que possuem apps que não estão em conformidade. Clique no nome de um dispositivo específico para visualizar os aplicativos listados com nomes de pacote e ver os motivos sinalizados. Clique em **Apagar apps do Office 365**.
4. Clique em **Sim** para confirmar a ação.

Como alternativa, siga as seguintes etapas:

1. Acesse **Usuários**.
2. Clique no nome do usuário para exibir a página de detalhes do usuário.
3. Clique em **Ação > Apagar apps do Office 365**.
4. Selecione os dispositivos dos quais os apps do Office 365 precisa ser apagados.
5. Clique em **OK** para confirmar a ação.

Como cancelar solicitações para apagar apps do Office 365

Procedimento

1. Acesse **Usuários**.
2. Clique no nome do usuário para exibir a página de detalhes do usuário.
3. Clique na aba **Proteção do Office 365**.
4. Na caixa suspensa **Selecionar tipo de relatório**, selecione o relatório **Apagar solicitações** para exibir as informações correspondentes.
5. Selecione os dispositivos dos quais as solicitações para pagar precisam ser canceladas. Apenas dispositivos com o status Apagamento pendente podem ser selecionados.
6. Clique em **Cancelar apagamento**.
7. Clique em **OK** para confirmar a ação.

Relatórios de aplicativos para usuários com Proteção de aplicativos do Office 365

Os administradores podem selecionar um dos seguintes relatórios para revisar a lista de usuários com proteção de aplicativos do Office 365 e informações relacionadas:

- Relatório de política de aplicativo
- Relatório de configurações do aplicativo
- Solicitações de apagamento

As informações nos Relatórios do aplicativo incluem ID do pacote, Nome do dispositivo, Tipo de dispositivo, Políticas ou configurações (implementadas no dispositivo), Status (Sincronizado, Sincronizado mas desatualizado ou Não sincronizado) e o horário do Último registro. Informações dos Relatórios de aplicativos podem ser exportadas para um arquivo CSV para referência ou análise posterior.

Informações no relatório Apagar solicitações incluem Nome de exibição, Nome do usuário, Nome do dispositivo, Tipo de dispositivo e Status de apagamento (Apagamento pendente ou Apagamento concluído).

Execute as seguintes etapas a seguir para visualizar um dos relatórios:

1. Acesse **Usuários**.
2. Clique no nome do usuário para exibir a página de detalhes do usuário.
3. Clique na aba **Proteção do Office 365**.
4. Na caixa suspensa **Selecionar tipo de relatório**, selecione um dos relatórios para exibir as informações correspondentes.
5. (Opcional) Na página de relatórios Solicitações de apagamento, selecione os dispositivos para os quais as solicitações de apagamento precisam ser canceladas e clique em **Cancelar apagamento**. Apenas dispositivos com o status Apagamento pendente podem ser selecionados.
6. (Opcional) Clique em **Exportar para o CSV** para fazer download do conteúdo reportado em um arquivo CSV para referência ou análise posterior.

Conexão com o Google Apps

Esta seção contém os seguintes tópicos:

Contas gerenciadas do Google Play (Contas com Android Enterprise)

Licença: Silver

Contas gerenciadas do Google Play devem permitir uso e configuração de dispositivos Android Enterprise. Não é mais necessário usar o Google Apps Directory Sync (GADS) ou contas do Google para registrar dispositivos.

Importante: se você já tiver configurado o Android Enterprise, será necessário primeiramente desativar esses dispositivos para poder usar esse recurso.

Configurar o Android Enterprise

Procedimento

1. Faça login no portal Ivanti Neurons for MDM.
2. Acesse **Administrador** > **Google** > **Android Enterprise**.
3. Em **Conta gerenciada do Google Play**, clique em **Autorizar Google** para exibir a página Google Play for Work.
4. Clique em **Começar**.
    - Insira o nome da empresa.
    - Aceite o contrato do Android Enterprise.
5. Clique em **Confirmar**.
6. Clique em **Concluir registro**.

Quando o Android Enterprise for configurado usando Contas gerenciadas do Google Play, há um limite no número de dispositivos cadastrados por usuário. Para superar esse limite, selecione a opção **Conta de dispositivo Android Enterprise** ao criar um novo usuário para permitir que os registros de dispositivos gerenciados de trabalho com Android Enterprise anexados à conta sejam atribuídos automaticamente à conta do dispositivo Google.

Contas de dispositivos são destinadas a implementações COSU (uso único de propriedade corporativa) (por exemplo, com o modo Quiosque). Usuários com contas de dispositivos podem ter acesso limitado ao Google Play.

Ocasionalmente, uma conta gerenciada do Google Play ou seu token expira por várias razões, como expiração do token de autenticação ou exclusão da conta/empresa. Em tais situações, os serviços do Google Play notificarão o cliente com uma ação de transmissão que acionará o reprovisionamento do dispositivo ao excluir a conta existente e adicionar uma conta com um token novo obtido do servidor UEM.

Em caso de falha no reprovisionamento da conta, seja porque a conta antiga não pôde ser removida ou porque houve muitas tentativas de reprovisionamento, o usuário será notificado para começar de novo desativando o cliente ou retornando o dispositivo à definição de fábrica, pois o caso pode depender de o dispositivo estar no modo Perfil de trabalho ou Dispositivo gerenciado, respectivamente.

Registro do dispositivo Android

Durante o registro do dispositivo Android, se for necessário obter permissão de usuários que devem informar o IMEI, o número do telefone e outros identificadores do telefone para concluir o registro, configure esta opção. Quando configurada, os usuários do dispositivo serão solicitados a conceder permissão para permitir que o Go client acesse os identificadores do dispositivo.

Esta configuração se aplica somente a novos registros de dispositivos Android com versão do Android superior à versão 6.0.

1. Selecione **Administrador > Google > Registro**.
2. Marque a caixa de seleção **Exigir identificadores de dispositivo Android durante o registro (perfil de trabalho e administrador do dispositivo)**
3. Clique em **Salvar**.

API de gerenciamento do Android

A API de gerenciamento do Android (AMAPI) é a API da plataforma Cloud do Google que integra as funções Android UEM do Google ao Ivanti Neurons for MDM. Na configuração do Android Enterprise, você pode habilitar a estrutura da API de gerenciamento do Android para gerenciar dispositivos Android Enterprise sem a necessidade de ter um aplicativo cliente instalado nos dispositivos para o seu gerenciamento. No momento, não há suporte para que o Go app seja inserido no dispositivo para outros recursos como MTD, etc.

Quando você tiver uma conta do Android Enterprise definida em sua configuração, poderá habilitar e usar a estrutura de API de gerenciamento do Android. Após a ativação, você pode:

- Adicionar um perfil de registro para usar o código QR para registro do dispositivo.
- Criar uma configuração de dispositivos dedicados (de uso único de propriedade da empresa ou COSU) para o dispositivo registrado para servir a um propósito específico.

A API de gerenciamento do Android é, no momento, compatível apenas com dispositivos que executam a versão 9 do Android ou superior e nos quais o Google Play esteja instalado e provisionado no modo Dedicado. O modo Dedicado à empresa também é referido como modo de Uso único de propriedade da empresa (COSU), e é uma amostra do modo proprietário do dispositivo. Este recurso também oferece suporte às seguintes ações do dispositivo:

- Bloquear
- Reiniciar
- Sincronizar com o servidor
- Apagar

Os check-ins do dispositivo são agendados para ocorrer em intervalos regulares (a cada hora). No entanto, para ação imediata, use a ação do dispositivo "Sincronizar com o servidor" na página de detalhes do dispositivo. Dispositivos AMAPI não enviam check-ins obrigatórios ao Ivanti Neurons for MDM. As atualizações de inventário ocorrem à medida e quando há atividade no dispositivo.

Ativação da API de gerenciamento do Android

Para habilitar a API de Gerenciamento do Android, vá para **Administrador > Android Enterprise > Autorizar Google (exige um endereço do Google válido) > Android Enterprise habilitado**.

O status de ativado da API de gerenciamento do Android (**Sim** para ativado e **Não** para desativado) também é mostrado na página Detalhes do dispositivo.

No momento, as contas do GSuite não são compatíveis com COSU.

Adicionar um perfil de registro

O perfil de registro deve ser criado para registrar o dispositivo Android usando a leitura do código QR ou a sequência alfanumérica do token. Os perfis de registro só podem ser criados quando a API de gerenciamento do Android estiver habilitada. Também é possível criar atributos personalizados do dispositivo a serem associados ao perfil de registro.

1. Selecione **Administrador > Android Enterprise > Perfis de registro**.
2. Configure as seguintes definições na janela **Perfil de registro – Dispositivo dedicado de propriedade da empresa**.

Configuração	Descrição
Nome	Insira um nome que identifique esse perfil de registro.
Descrição	Insira uma descrição que esclareça o objetivo deste perfil de registro.
Nome de usuário	Insira as primeiras letras de um nome de usuário válido e selecione um dos resultados correspondentes que são exibidos. Um nome de usuário válido pode vir de um usuário local ou de um usuário do LDAP. Os perfis de registro marcam os dispositivos inscritos usando o código QR no perfil para serem exibidos como um dispositivo pertencente ao usuário para o qual o perfil de registro foi criado.
Validade do token	Insira o número de dias para a validade da leitura do código QR do token de autenticação. O número inserido deve ser entre 1 e 30. O dispositivo é redefinido se você usar o token ou perfil de registro após o período de expiração.
Atributos personalizados do dispositivo	Na coluna Ações, clique em **+Adicionar novo** para adicionar atributos personalizados do dispositivo a serem associados ao perfil de registro.

Configuração	Descrição
	a. Selecione o atributo personalizado do dispositivo na lista suspensa na coluna **Nome do atributo**. b. Na coluna **Valor**, informe o valor do atributo personalizado. c. Clique em **Salvar**. O atributo personalizado do dispositivo adicionado é exibido na tabela. Para excluir, clique na opção **Excluir** na coluna Ações. Os atributos personalizados podem ser adicionados a um perfil de registro apenas durante a criação do perfil. Não é possível editar os campos de atributos após a criação do perfil.

3. Clique em **Salvar**. A janela **Resumo do perfil** mostra os seguintes detalhes do token:
   - Nome
   - Descrição
   - Nome de Usuário
   - Data de criação do token
   - Data de expiração do token
   - Valor do token
   - Código QR
   - Atributos personalizados do dispositivo.

Os dispositivos são redefinidos se a configuração adequada para o dispositivo não for adquirida dentro do intervalo de 10 minutos após o registro. Nesses casos, você deve se registrar novamente usando o token de registro/código QR

Quando um perfil de registro é criado, ele é listado na página **Perfis de registro**. É possível realizar qualquer das seguintes ações na coluna **Ações**.

- Clique no ícone Visualizar para visualizar os detalhes do perfil de registro na janela Resumo do perfil. O código QR também é exibido nesta janela.
- Clique no ícone Editar para editar os detalhes do perfil de registro.

  Você pode editar apenas a validade do token. Outros atributos não podem ser editados.

- Clique no ícone Excluir para excluir o perfil de registro.

Criação da configuração COSU

Os administradores podem configurar dispositivos dedicados que podem ser usados para uma finalidade específica com o Android Enterprise usando a configuração de dispositivos dedicados (uso único de propriedade da empresa, ou COSU). A configuração COSU é distribuída para dispositivos gerenciados de trabalho (modo proprietário do dispositivo) para fornecer apenas um aplicativo disponível para os usuários no modo quiosque. Dispositivos que estejam no Perfil de trabalho em Dispositivos de propriedade da empresa não são suportados.

Usando essa configuração, o administrador pode configurar os dispositivos para ter o aplicativo fixado na tela, de modo que o usuário do modo quiosque não possa desafixar este aplicativo e navegar para fora dele para outras telas do dispositivo, ou usar qualquer outro aplicativo no dispositivo.

Para forçar a instalação de outros aplicativos no dispositivo AMA, selecione a opção "Instalar no dispositivo" em Opções avançadas e configurações do aplicativo. No entanto, não será possível interagir com eles enquanto o aplicativo quiosque estiver fixado na tela pela configuração. Para o Quiosque multiaplicativo, é recomendado usar a funcionalidade de Quiosque do Dispositivo gerenciado de trabalho (modo proprietário do dispositivo). Ela oferece mais controle em configurações de aplicativos e dispositivos, e também pode ser expandida para um modo multiusuários.

Os administradores podem fazer alterações na configuração, como permitir a navegação do sistema e a capacidade de usar outros apps enviados ao dispositivo para o usuário final por meio do Google DPC, revisando as várias opções com base nas necessidades.

As configurações COSU são determinadas pela prioridade atribuída a eles. A configuração de maior prioridade é usada para enviar a configuração da política ao Google. As configurações COSU são aplicadas a dispositivos dentro do espaço definido. Pode ser delegado a outros espaços, se definido no espaço padrão.

Para configurar:

1. Acesse **Configuração > +Adicionar**.
2. Na configuração **Bloqueio e quiosque: Android Enterprise**, clique em **Dispositivos dedicados (uso único de propriedade da empresa ou COSU)**.
3. Insira um nome para a configuração.
4. Insira uma descrição.

5. Você pode definir as seguintes configurações clicando nas respectivas guias:

   - **Configurações do aplicativo**
   - **Bloqueios gerais**
   - **Personalização de quiosques**
   - **Configurações do sistema**

   A tabela a seguir fornece os detalhes dos campos configuráveis:

Configuração	Descrição
Configuração do aplicativo	
Nome do aplicativo	Selecione o aplicativo a ser fixado no dispositivo inserindo o nome do aplicativo, digitando a letra inicial do nome até ver o aplicativo desejado no menu suspenso. Se você não encontrar o aplicativo desejado no menu suspenso, certifique-se de que o aplicativo que deseja implantar é um aplicativo Público/Privado disponível na Play Store e adicionado ao App Catalog. Este campo é obrigatório. Você não terá permissão para criar a configuração se não selecionar um aplicativo a ser adicionado neste campo. Você pode adicionar apenas apps públicos e privados. Não é possível adicionar aplicativos internos e aplicativos da Web (privados).
Bloqueios gerais	
Manter tela ligada	Configure a bateria conectada nos modos para os quais o dispositivo permanece ligado. Selecione qualquer uma das opções a seguir:

Configuração	Descrição
	• **CA** – A fonte de alimentação é um carregador de CA • **Sem fio** • **USB** – A fonte de alimentação é uma porta USB • **Qualquer um** – A fonte de alimentação é um carregador de CA, a porta USB ou um carregador sem fio.
Personalização de quiosques	
Personalizar barra de status	Selecione qualquer uma das seguintes opções para personalizar a barra de status nos dispositivos de destino: • **Notificação e informações do sistema ativadas** – Para mostrar as informações do sistema e as notificações na barra de status. • **Somente informações do sistema ativadas**– Para mostrar somente as informações do sistema na barra de status.
Personalizar navegação no sistema	Selecione qualquer uma das opções a seguir para especificar o acesso aos recursos de navegação (botões Início e Visão geral) no modo quiosque. • **Ativado** – Ativa a navegação dos botões Início e Visão geral. Os usuários podem navegar para fora do aplicativo especificado se esta opção for selecionada. • **Desativado** – Desativa a navegação dos botões Início e Visão geral.

Configuração	Descrição
	• **Apenas botão Início** – Permite apenas a navegação do botão Início. O botão Voltar está disponível com todas essas opções.
Ativar ações globais	Selecione para ativar as ações globais no modo quiosque. A funcionalidade de reinicialização e desligamento associada aos botões liga/desliga é controlada por meio desta opção.
Ativar diálogos de erro do sistema	Selecione para ativar as caixas de diálogo de erro para apps travados ou que não respondem no modo quiosque.
Configurações do sistema	

Configurações de atualizações do sistema	Defina as seguintes configurações para gerenciar as atualizações do sistema:
	
	• **Atualização do sistema** – Selecione o tipo de atualização do sistema exigida.
	
	  • **Automática** – Instala automaticamente assim que uma atualização estiver disponível
	
	  • **Adiar** – Adia a instalação automática por um máximo de 30 dias.
	
	  • **Agendada** – Instala automaticamente dentro de uma janela de manutenção diária. Defina as horas de início e encerramento para o período da janela de manutenção.

Configuração	Descrição
	As atualizações instaladas nos dispositivos podem variar dependendo do conjunto de recursos compatíveis, da versão do Android e da versão do Google DPC instalada no dispositivo. • **Período de congelamento** – Quando o dispositivo está definido como dentro do período de congelamento, todas as atualizações de sistema são bloqueadas e não instaladas. Clique em **Adicionar período de congelamento** para definir a **Data de início** e a **Data de encerramento** do período de congelamento. Quando um dispositivo está fora do período de congelamento, é aplicado o comportamento normal de atualizações. Se a data final for anterior à data inicial, o período de congelamento abrangerá o ano atual e o ano seguinte. O período de congelamento pode ser definido para um máximo de 90 dias. Dois períodos de congelamento consecutivos devem ser separados por um mínimo de 60 dias.

6. Clique em **Avançar**.

7. Selecione uma das opções de distribuição a seguir:
    - **Todos os dispositivos**
    - **Nenhum dispositivo** (padrão)
    - **Personalizada**
8. Clique em **Concluído**.

Gerenciamento de aplicativos em dispositivos AMAPI

Quando a configuração COSU é distribuída para os dispositivos, os apps são transferidos e fixados na tela do dispositivo AMA. Independentemente da configuração COSU que está sendo transferida para o dispositivo, ainda é possível gerenciar os aplicativos instalados no dispositivo AMA. Veja a seguir detalhes do gerenciamento de apps nesses dispositivos:

- Apenas aplicativos públicos e privados são compatíveis; não há compatibilidade para aplicativos internos e clipes da Web.
- Os aplicativos são transferidos apenas quando as opções "Instalar no dispositivo" ou "Instalação silenciosa" estiverem ativadas nas configurações da instalação. Os aplicativos que forem atribuídos ao usuário/dispositivo e não tiverem nenhuma dessas opções ativadas não serão vistos no dispositivo nem na Play Store do dispositivo em nenhuma ação do usuário.
- As configurações de aplicativo compatíveis são Google Play gerenciado e Dispositivo gerenciado de trabalho (AFW). Há suporte para configurações gerenciadas de aplicativos, inclusive suporte para configuração gerenciada de aplicativos OEMConfig.

    O tempo para conclusão da instalação e desinstalação das configurações pode variar de acordo com as notificações do Google (serviço de mensagens) que informam se a ação desejada foi ou não executada.

- O Go app será agora instalado por padrão como parte do registro do dispositivo AMA. Durante o processo de registro, o aplicativo será fixado na tela e, assim que a configuração estiver concluída, será executado em segundo plano.

    Com exceção do requisito de registro do dispositivo com base no fabricante, políticas de versão do SO e de nível do patch de segurança não são compatíveis. Criação de lista de dispositivos permitidos que permite que apenas dispositivos permitidos sejam registrados no Ivanti Neurons for MDM.

Gerenciando suporte a feedback de aplicativos em dispositivos AMAPI

Em dispositivos AMAPI (COSU), é possível gerir o suporte a feedback de aplicativos. Quando um dispositivo é registrado no modo AMAPI (COSU), a configuração do aplicativo gerenciado é enviada ao Ivanti Neurons for MDM diretamente do Google, sem nenhuma intervenção do Go app. As informações de feedback dos aplicativos gerenciados podem ser visualizadas no nível do dispositivo, em **Detalhes do dispositivo > Aplicativos instalados > Exibir feedback**, ou no nível do aplicativo individual, navegando-se até o app específico do Android no catálogo de aplicativos, na aba "Feedback de Configuração do Aplicativo", para obter o relatório geral em todos os dispositivos. Para informações sobre o mecanismo de feedback de aplicativo, consulte "Sincronização e busca de feedback de aplicativo" na página 292.

Limitações da AMAPI

Atualmente, o AMAPI tem as seguintes limitações:

- Apenas dispositivos dedicados (modo COSU) são compatíveis.

Configurações com suporte

Há suporte para as seguintes configurações para AMAPI:

- Distribuição do aplicativo (um ou vários aplicativos)
- Configuração de aplicativos gerenciados para apps enviados ao dispositivo
- Configuração Wi-Fi
- Configuração do Android Enterprise Lockdown-Dedicated (COSU)
- Configuração VPN Sempre Ativa

API do Google Apps

Clientes Google que utilizam o Single Sign On (SSO) para autenticar o acesso do usuário aos serviços do Google Apps podem não conseguir usar o Exchange para conectar os usuários ao e-mail, aos contatos e ao calendário, devido a limitações no protocolo que impedem que os dispositivos ofereçam suporte a redirecionamentos ativados por SSO para serviços de autenticação externa. Esse serviço resolve esse problema criando e gerenciando senhas de contas para garantir conectividade ActiveSync.

Pré-requisitos

Antes de tentar configurar a API do Google Apps, é necessário:

- Ter acesso de administrado a uma conta em https://console.developers.google.com/.
- Ter acesso de administrado a uma conta em https://admin.google.com.

Ativação do recurso API do Google Apps

Procedimento

1. Selecione **Administrador > Google > API do Google Apps**.
2. Clique em **Etapa 1: Google Dev** na parte inferior do retângulo à esquerda com o título 1.

   A Etapa 1: a página Google Dev será exibida.
3. Siga as instruções que aparecem na Etapa 1: na página Google Dev clique em **Concluir**.
4. Clique em **Etapa 2: Google Admin** na parte inferior do retângulo do meio com o título 2.

   A Etapa 2: a página Google Admin será exibida.
5. Siga as instruções que aparecem na Etapa 2: na página Google Admin clique em **Concluir**.
6. Insira o nome do usuário do administrador Google no campo **Inserir nome de usuário do administrador Google** no retângulo à direita com o título 3.
7. No mesmo retângulo, clique em **Escolher Arquivo** para atualizar o arquivo JSON que você baixou na Etapa 1.
8. Clique em **Salvar**.

Se você não conseguir visualizar a página API do Google Apps, pode ser que você não tenha as permissões necessárias. Você precisará de uma das seguintes funções:

- Gerenciamento do sistema
- Somente leitura do sistema

Administrador – Android Enterprise

Licença: Silver

- Aplicativos de produtividade Ivanti, Inc habilitados para Android Enterprise, como Email+, Docs@Work e Web@Work, exigem licença Gold.
- Tunnel for Android Enterprise requer licença Platinum.

O Android Enterprise permite o uso e a configuração de aplicativos Android Enterprise. Os usuários do Android Enterprise podem visualizar e instalar aplicativos a partir do catálogo de aplicativos e também pelo Google Play.

Se for um cliente novo, a distribuição de aplicativo é definida, por padrão, de acordo com o dispositivo. Não é possível alterar essa configuração. Para clientes que estão fazendo upgrade, é possível escolher entre a distribuição de apps por usuário ou por dispositivo. Também para os clientes que estão fazendo upgrade, a distribuição de aplicativo por usuário é selecionada por padrão. Muitos usuários têm vários dispositivos. Se um usuário tiver vários dispositivos, quando a distribuição de aplicativo for definida por dispositivo, você poderá tornar um conjunto diferente de apps disponível em cada dispositivo.

Esta seção contém os seguintes tópicos:

- "Configurar o Android Enterprise" abaixo
- "Como configurar o Work Profile do Android Enterprise" na página seguinte

Configurar o Android Enterprise

1. No portal do Ivanti Neurons for MDM, em **Administrador > Google > Android Enterprise**.
2. Selecione uma das opções a seguir:
    - **Conta gerenciada do Google Play:** para empresas que não assinam o G Suite, este método permite que os usuários sejam inscritos no Android Enterprise sem envio de qualquer informação pessoal (endereços de e-mail ao Google). O Ivanti Neurons for MDM provisionará e gerenciará os usuários automaticamente com o Google. Você será solicitado a autorizar o Android Enterprise com uma conta de administrador do Google.

- **Conta gerenciada do Google:** para empresas que assinam o G Suite, este método permite que os usuários sejam inscritos no Android Enterprise com as próprias contas do Google. Cada usuário precisa ter uma conta do Google para se inscrever no Android Enterprise.

3. Siga as instruções na tela para concluir o processo de configuração:

   No método automático, isso inclui:

   - Habilitar sua API UEM e criar as credenciais corporativas.
   - Registrar-se no Google autorizando o proprietário da integração. Essa deve ser uma conta de TI, não uma conta pessoal.
   - Configurar sua credencial arrastando e soltando sua ID de cliente JSON da conta de serviço.

4. No método alternativo, isso inclui:

   - Consulte a ID DO CLIENTE na seção abaixo e adicione-a ao Google Admin.
   - Consulte seu token MDM no Google Admin e a conta de serviço no Google Cloud Console.
   - No Ivanti Neurons for MDM, insira seu token MDM, o domínio do Google corporativo e o endereço de e-mail do administrador corporativo para se conectar ao serviço do Google.
   - No Ivanti Neurons for MDM, arraste e solte seu ID de Cliente JSON da Conta de Serviço.
   - No Ivanti Neurons for MDM, autorize o Ivanti Neurons for MDM a visualizar e/ou gerenciar seus usuários do Google clicando em **Autorizar**.

A interface de usuário do Ivanti Neurons for MDM o guiará nessas etapas.

ID do CLIENTE para vincular o Ivanti Neurons for MDM à conta Google gerenciada

Adicione o ID de cliente como **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com** no Admin Console para vincular o locatário do Ivanti Neurons for MDM à conta gerenciada do Google.

Como configurar o Work Profile do Android Enterprise

1. No portal do Ivanti Neurons for MDM, acesse **Configurações**.
2. Clique em **+Adicionar**.
3. Selecione a configuração **Bloqueio e quiosque: Android Enterprise**.

4. Insira um nome de configuração e uma descrição.
5. Clique no tipo de bloqueio do **Work Profile**.

   Selecione as configurações de bloqueio que você deseja aplicar aos dispositivos de destino.

   Importante: quando o usuário adiciona uma conta do Google usando Adicionar conta em Configurações, o servidor de autenticação do Google verifica se o domínio da conta está registrado como um domínio gerenciado por UEM. Verifique se a opção **Aplicar as políticas de UEM em dispositivos Android** está selecionada. Se estiver, o Go client é automaticamente instalado ou atualizado (se não estiver instalado no dispositivo) e iniciado. Quando o usuário passa pelo processo de registro, é solicitado que ele crie um Perfil de trabalho e a conta do Google é automaticamente migrada para ele.

Trabalhar com dispositivos ChromeOS

Esta seção contém os seguintes tópicos:

ChromeOS e Ivanti Neurons for MDM

O ChromeOS é um sistema operacional baseado em Linux criado e distribuído pelo Google. Ivanti Neurons for MDM suporta dispositivos que rodam Android, Windows, iOS e macOS. Agora, esse suporte também foi estendido a dispositivos ChromeOS. Ivanti Neurons for MDM fornece uma solução unificada e simples de gerenciamento de mobilidade para configurar e gerir seus dispositivos ChromeOS. A Ivanti fornece uma solução unificada, simples e rica em recursos para dispositivos ChromeOS, semelhante aos fluxos de trabalho administrativos disponíveis para iOS, Android, Windows e Mac no Ivanti Neurons for MDM. O administrador pode simplesmente conectar o Ivanti Neurons for MDM com seu Google Cloud (também referido como Google Admin Console) usando uma integração simples em **Administrador > Google > Gerenciamento do ChromeOS**.

Pré-requisitos

1. Deve ter uma conta gerenciada do Google Admin.
2. Os usuários LDAP e OUs devem ser importados no Google Admin Console. Ivanti Neurons for MDM suporta apenas OUs importadas de uma origem LDAP. UOs locais não são suportadas.

3. O administrador deve ter sincronizado as unidades organizacionais (grupos de usuários) no Ivanti Neurons for MDM. Isso pode ser feito configurando o servidor LDAP e adicionando as unidades organizacionais.

   Os administradores de locatários que desejem usar os recursos do Chrome devem entrar em contato com a equipe de suporte para habilitar "feature.chromeos.admin.signup".

Autorizando Google

Os dispositivos ChromeOS disponíveis no console do Google Admin não podem ser registrados diretamente no Ivanti Neurons for MDM. Em vez disso, esses dispositivos são registrados no Google, e as informações sobre eles são sincronizadas entre o Google e o Ivanti Neurons for MDM. O administrador deve autorizar o Google a importar os dispositivos e a realizar outras ações, como atribuir aplicativos, configurações, etc.

Procedimento

1. Acesse **Administrador -> Google > Gerenciamento do ChromeOS**.
2. Clique em **Autorizar Google**.
3. Selecione a conta de administrador do Google que você deseja autorizar.
4. Clique em **Continuar** para aceitar as permissões para fornecer os serviços necessários.

   A confirmação **ChromeOS configurado com sucesso** aparece na tela. As informações de domínio também podem ser encontradas abaixo da confirmação.

Sincronizando dispositivos ChromeOS a partir do Google

O administrador deve sincronizar os dispositivos ChromeOS no console do Google Admin. Ao usar o console do Google Admin para acessar os dispositivos ChromeOS pela primeira vez, o administrador deve sincronizar manualmente os dispositivos usando a opção Sincronizar Agora, na página Gerenciamento do ChromeOS.

Depois de sincronizar os dispositivos manualmente na primeira vez, as sincronizações subsequentes acontecerão automaticamente a cada hora.

Distribuir aplicativos Android para dispositivos ChromeOS

O administrador pode distribuir os aplicativos Android do App Catalog para dispositivos ChromeOS.

Pré-requisitos

1. O Android Enterprise deve estar configurado. Para informações sobre como configurar o Android Enterprise, consulte "Configuração do Android Enterprise" na página 518.
2. Os aplicativos Android devem estar presentes no App Catalog.
3. Certifique-se de que o usuário do dispositivo ChromeOS (Chromebook) faça parte de um grupo de usuários (também referido como Unidade Organizacional) antes de distribuir aplicativos Android e a Configuração ChromeOS Blueprint.

Depois que o aplicativo Android for identificado, você precisará distribuí-lo seguindo o processo semelhante ao que segue para distribuir qualquer outro aplicativo. Ao distribuir o aplicativo Android, selecione os grupos de usuários para os quais deseja distribuir o aplicativo e execute uma instalação silenciosa no dispositivo.

Se a sua implantação existente do aplicativo Android estiver definida para ser distribuída a usuários, dispositivos ou grupos de dispositivos, será preciso alterar a distribuição para que seja feita a grupos de usuários. Isso pode afetar as implantações existentes se o aplicativo já estiver em uso. Recomenda-se fazer isso em um aplicativo completamente novo primeiro.

As configurações de instalação permitem aos administradores controlar a instalação silenciosa final e são necessárias para enviar o aplicativo aos dispositivos ChromeOS. Grupos de usuários devem ser selecionados aqui.

Configuração ChromeOS Blueprint

A Configuração ChromeOS Blueprint tem os seguintes parâmetros:

- Configurações do dispositivo
- Configurações de usuário e navegador
- Configurações de sessão de visitante gerenciada

Você pode aplicar a configuração ChromeOS em grupos de usuários específicos (também referidos como unidades organizacionais). Quando você tentar distribuir a Configuração ChromeOS Blueprint, apenas a seção Grupos de Usuários estará disponível, e todos os Grupos de Usuários LDAP que também estejam associados ao Google Admin Console autorizado serão listados nela. Você pode selecionar um ou mais dos grupos listados e aplicar a configuração.

Procedimento

1. Acesse **Configurações > Adicionar**.
2. Selecione **Google ChromeOS** na seção SO. A guia **Configuração ChromeOS Blueprint** aparece na tela.
3. Clique em **ChromeOS Blueprint**. A página **Criar Configuração ChromeOS Blueprint** aparece na tela.
4. Insira um nome para configuração na caixa **Nome**.
5. Em Definição da Configuração, você pode modificar as configurações do dispositivo, as configurações do navegador e do usuário e as configurações da sessão de visitante gerenciada, conforme necessário, e alternar o botão "Enviar ao dispositivo" para aplicar as configurações modificadas.
6. Clique em **Avançar**.
7. Selecione **Personalizada** nas opções de distribuição.

   Somente os grupos de usuários LDAP estarão disponíveis para distribuir a configuração.

   No caso de distribuir a configuração para todos, isso pode ser feito apenas para os grupos de usuários LDAP disponíveis no Ivanti Neurons for MDM e no Google Admin Console.

8. Selecione um ou mais grupos e clique em **Concluído**.

Se as configurações distribuídas tiverem a distribuição cancelada, as configurações aplicadas não serão revertidas.

Ações do dispositivo

As seguintes ações são compatíveis com dispositivos ChromeOS:

- **Apagar** - a ação Apagar exclui todos os dados do dispositivo e restaura-o às configurações de fábrica. Para mais informações, consulte "Como apagar um dispositivo" na página 280.
- **Bloquear** - a ação Bloquear impede você de realizar qualquer outra ação no dispositivo. Para mais informações, consulte "Como bloquear um dispositivo" na página 273.

- **Desbloquear** - a ação Desbloquear libera o dispositivo para uso posterior. Para mais informações, consulte "Como desbloquear um dispositivo" na página 283.

Perguntas frequentes

Esta seção lista algumas dúvidas comuns que você pode ter ao usar dispositivos ChromeOS no Ivanti Neurons for MDM.

- Como o gerenciamento do Chromebook difere do de outros sistemas operacionais?

  A partir de agora, o Google só permite distribuir configurações com base em grupos de usuários LDAP, e o administrador deve garantir que, ao trabalhar com configurações ou aplicativos, a distribuição seja baseada em grupos de usuários LDAP. Grupos de usuários locais e grupos de dispositivos não são compatíveis com o gerenciamento de dispositivos ChromeOS.

- De qual licenciamento preciso com a Ivanti para gerenciar dispositivos ChromeOS?

  Os dispositivos ChromeOS devem ter licenças como Chrome Enterprise Upgrade ou Chrome Education Upgrade. Elas podem ser adquiridas de revendedores como parte do hardware ou como licenças independentes. Consulte a documentação do Google para obter mais informações. Para começar a usar o gerenciamento de dispositivos Chrome, é necessário o licenciamento Secure UEM (Unified Endpoint Management) com a Ivanti.

- O Mobile Threat Defense (MTD) ou outra solução semelhante estará disponível? Preciso de uma licença separada para o MTD?

  Isso não está disponível atualmente no produto, consulte as limitações atuais. Forneceremos mais informações sobre alterações nas funcionalidades do recurso via Perguntas Frequentes e anúncios de lançamento.

- Por que a guia de configurações e aplicativos não tem detalhes como no caso de outros dispositivos?

  Como as configurações são distribuídas a Grupos de Usuários, e não aplicadas com base no usuário conectado, elas não são mostradas atualmente nos detalhes do dispositivo. Os apps seguem a mesma lógica de distribuição e possuem a mesma limitação. Forneceremos mais informações sobre as mudanças nessas limitações via Perguntas Frequentes e anúncios de lançamento.

- Quantas configurações são atualmente compatíveis com ChromeOS?

Com o ChromeOS, reduzimos o número de blocos de configuração disponíveis e reduzimos as tarefas administrativas associadas à configuração. Referimo-nos a essa configuração como "ChromeOS Blueprint". A ChromeOS Blueprint suporta cerca de 700 configurações nesses dispositivos. Consulte a documentação do Google para obter as opções de configuração.

- Qual a facilidade de gerir uma configuração para todos os dispositivos?

  Os administradores podem simplesmente clonar uma configuração existente e modificá-la (se necessário) para seus respectivos grupos de usuários. Você não precisa começar do zero.

- Como adiciono configuração de VPN a dispositivos Chrome?

  Isso pode ser feito usando aplicativos Android, sem usar VPN nativa.

- Ações como Desativar e Apagar funcionam nesses dispositivos?

  Chromebooks em ambiente empresariais são sempre gerenciados por uma organização, e os dados desses dispositivos são considerados completamente organizacionais. Com isso em mente:

  - Desativar fica bloqueado
  - Apagar é permitido
  - Bloquear é permitido
  - Desbloquear é permitido
  - Outras ações: não são suportadas

- Quais Chromebooks, em termos de hardware, são suportados pela Ivanti?

  Espera-se que os dispositivos compatíveis com as soluções de gerenciamento de dispositivos do Google Cloud sejam suportados pela Ivanti. Atualmente, a Ivanti não publica uma lista do hardware específico suportado pela solução dela.

- Qual versão do Chrome OS é suportada?

  O Google Cloud suporta apenas a versão estável mais recente do ChromeOS, e o suporte do Ivanti segue o modelo suportado pelo Google, devido à natureza das integrações de back-end.

- Quais são as limitações atuais, já que este é o primeiro lançamento desse recurso?

Com o novo suporte do Chrome OS, estamos trabalhando arduamente para fornecer os recursos que nossos clientes tanto anseiam. Abaixo estão algumas limitações que os administradores devem observar:

- As extensões do Chrome OS (aplicativos de navegador) não são atualmente suportadas (como "aplicativos") para distribuição.
- A configuração de aplicativo gerenciado para aplicativos Android não é suportada no momento.
- A API de configuração Wi-Fi foi lançada recentemente e não é suportada atualmente.
- Não há suporte a distribuição de certificados no momento.
- A distribuição do app Ivanti Go (anteriormente conhecido como MobileIron Go) para Android não é suportada no momento.
- O aplicativo Ivanti Tunnel (VPN) não é suportado no momento.
- Espaços e delegação de espaço não são suportados no momento.
- A solução Mobile Threat Defense não é suportada no momento.
- A solução Zero Sign-on da Ivanti é suportada nesses dispositivos, categorizados como dispositivos não gerenciados.
- As ações de política não são totalmente suportadas.

Etapas recomendadas para avaliação

Recomendam-se as seguintes etapas para validar uma solução:

1. Crie uma UO (grupo de usuários) separada que tenha um usuário de teste na fonte de diretório (por exemplo, Active Directory). Isso evitará qualquer impacto nas Unidades Organizacionais ativas.
2. Sincronize os usuários entre Ivanti, Google e a fonte de diretório (LDAP). Verifique se "OU de teste" está disponível em Grupos de Usuários.
3. Integre o Ivanti Neurons for MDM com o Google conforme destacado nas etapas acima.
4. Crie a configuração ChromeOS Blueprint e distribua-a apenas ao grupo de usuários "OU de teste".
5. Inicialize um Chromebook (pronto para uso ou registrado anteriormente). Verifique se ele está disponível na lista Dispositivos.
6. Verifique se as configurações ChromeOS Blueprint estão disponíveis no dispositivo.
7. Siga etapas semelhantes para distribuição de aplicativos Android.

Gerenciamento de firmware

Esta seção contém os seguintes tópicos:

Como registrar no serviço Zebra OTA

Quando você estiver registrado no serviço Zebra OTA (Over The Air, Sem fio), é possível ativar a configuração Zebra OTA para receber e atualizar os detalhes de firmware dos dispositivos Zebra registrados com o Ivanti Neurons for MDM.

Procedimento

1. Acesse **Administrador > Zebra OTA**. A página **Serviço Zebra OTA** será exibida.
2. Clique em **Começar**.
3. Insira suas credenciais do Zebra OTA para fazer o login e siga as etapas para solicitar uma aprovação para utilizar os serviços Zebra.
4. Clique em **Concluir verificação** para confirmar a conexão com o serviço Zebra. Quando a conexão for confirmada, o status do registro bem-sucedido é exibido na página do serviço Zebra OTA.

Para revogar o registro, clique em **Revogar** na coluna **Ações**. A ação Revogar remove todas as configurações do Zebra OTA das configurações existentes. Para se inscrever novamente no Zebra OTA, clique em **Atualizar**. A ação de atualização não afeta as configurações existentes.

Após o registro, você pode ativar a configuração de firmware do Zebra que os Go clients recebem e aplicam aos dispositivos Zebra (executando na versão do Android 8.0 ou em versões mais novas com suporte) no modo Proprietário do dispositivo. Quando a configuração é aplicada, o firmware é baixado e instalado no dispositivo, conforme agendado na configuração. Para saber mais sobre a habilitação da configuração do Zebra OTA, consulte Configuração de atualização do sistema.

Após concluir a atualização do firmware, você pode visualizar o status de atualização do firmware no dispositivo Zebra na coluna **Atualizar sistema** na página Dispositivos. A seguir, estão os possíveis status:

- **Desconhecido** - Não suportado pelo cliente ou SO
- **Atual** - A maioria das atualizações atuais do dispositivo estão disponíveis
- **Pendente** - A configuração de atualização do sistema é aplicada, mas a atualização não foi baixada ou aplicada
- **Em download** - A atualização do sistema está sendo baixada para o cliente
- **Disponível** – A atualização do sistema está disponível para o dispositivo
- **Erro** – Erro no download ou instalação.

A coluna **Versão do patch do Zebra** na página Dispositivos exibe as informações de patch do Zebra do dispositivo.

A **Versão do Patch Zebra** não é compatível com dispositivos Android 11 e posteriores; apenas o **Upgrade Completo Zebra** é suportado.

Gerenciamento de Licenças Samsung E-FOTA (descomissionado)

O serviço Samsung E-FOTA será descomissionado em julho de 2022. Para mais informações, consulte o comunicado da Samsung.

Não é mais possível configurar o serviço Samsung E-FOTA a partir de agora. No entanto, se você tem uma configuração E-FOTA existente, pode desativá-la navegando até **Administrador** > **Gerenciamento de Firmware** > **Samsung E-FOTA** e clicando na opção **Desativar**.

Suspensão do locatário

O acesso a um locatário utilizado com uma licença de avaliação ou de produção pode ser suspenso pelo Ivanti Neurons for MDM. Uma licença de avaliação pode ser suspendida quando o período de avaliação expirar ou quando a permissão de uso for excedida. Uma Licença de Produção pode ser suspensa quando o período de assinatura expirar ou o limite de uso for excedido. O Ivanti Neurons for MDM restaurará um locatário suspenso quando a licença for renovada ou quando forem adquiridas licenças adicionais, no caso de um excedente.

Quando uma licença de locatário for suspensa:

- Os dispositivos registrados continuam funcionando normalmente.
- Os administradores não poderão fazer login no Admin Portal.
- Não será possível registrar novos dispositivos.
- O acesso a API pelo locatário será bloqueado.
- Os usuários finais poderão continuar acessando o portal de autoatendimento.

Ação de suspensão do locatário e mensagens de erro

Ação de suspensão	Erro	Mensagem de erro exibida	Localização
O acesso à API de integração com o cliente final é bloqueado.	A solicitação para a API falha.	Acesso negado. Sua licença de avaliação expirou. Renove sua licença para reativar o acesso à API. Entre em contato com o administrador do sistema para obter mais informações.	API erro 401.
Novos dispositivos estão bloqueados para o registro.	Será exibida uma mensagem de erro na tela de inscrição.	Não foi possível registrar seu dispositivo. A licença para seu sistema expirou. Entre em contato com o administrador do sistema para obter mais informações. Dispositivos cadastrados anteriormente continuarão funcionando normalmente.	Após a verificação de senha.
O administrador fica bloqueado para fazer login no Admin Portal.	Será exibida uma mensagem de erro na tela de login.	Não foi possível fazer o login. Sua licença expirou. Renove sua licença para recuperar o acesso ao Admin Portal e inscrever novos dispositivos. Os dispositivos já inscritos continuarão funcionando normalmente. Entre em contato com seu representante de vendas para renovar suas licenças. Lembre-se de que a senha do Admin expira após um ano (365 dias).	Após a verificação de senha.

Gerenciar scripts

Os administradores podem gerenciar scripts que podem ser usados em Configurações e enviados para dispositivos.

Esta seção contém os seguintes tópicos:

Todos os scripts

Aplicável para: dispositivos macOS

Na página **Administrador > Todos os scripts** , o Ivanti Neurons for MDM permite que os usuários com função de Gerenciamento do sistema criem ou carreguem e gerenciem scripts que podem ser usados em configurações e distribuídos para os dispositivos. Você pode associar atributos personalizados com os scripts e atribuir os valores resultantes aos dispositivos configurados. Use as trilhas de auditoria para visualizar os registros das mudanças de script e os resultados de execução.

Você pode escrever um script que executa quaisquer configurações nos dispositivos. Por exemplo, você pode executar scripts que:

- forcem os usuários do dispositivo a alterar suas senhas mensalmente,
- travar a tela após 5 minutos de inatividade ou
- configurar uma rede Wi-Fi protegida.

Esta seção contém os seguintes tópicos:

Adicionando um script

Você pode criar ou carregar um repositório de scripts bash. Esse repositório pode ser usado em uma configuração, como Mobile@Work para o script macOS, para selecionar um script e distribuí-lo para execução em dispositivos de acordo com a programação especificada na configuração.

Por exemplo, você pode criar um script shell para execução nos dispositivos. Você pode usar encapsulamentos, se necessário. Não há suporte para a execução dos arquivos binários de dentro de um script shell.

A Ivanti recomenda testar seus scripts shell antes de executá-los em dispositivos para garantir sua robustez e qualidade. Execute seus scripts localmente e corrija quaisquer erros resultantes.

Procedimento

1. Acesse **Administrador** > **Todos os scripts**.
2. Clique em **+ Adicionar**.
3. Nomeie e descreva o script.
4. Selecione um **Tipo de Script** a seguir:
   - **bash**
   - **zsh**
   - **python**
   - **swift**
5. Marque a caixa **Executar como root** para executar o script como root nos dispositivos. Por padrão, essa opção está desmarcada.
6. No **Editor de script**, você pode digitar, arrastar e soltar ou copiar e colar um script na caixa de texto.
7. Como alternativa, clique em **Importar código de um script** para arrastar e soltar um arquivo de script existente ou clique em Escolher arquivo para procurar e selecionar o arquivo de script que será carregado no Ivanti Neurons for MDM. Isso substituirá qualquer script existente no editor de scripts. Essa ação não poderá ser desfeita. Clique em **Importar**. O código do script carregado será exibido no editor do script.
8. (Opcional) Na seção **Atributos personalizados disponíveis**, selecione um ou mais atributos personalizados do dispositivo exibido para associá-los ao script. Eles podem ser usados para atribuir os valores de execução do script resultante para os atributos personalizados do dispositivo dos dispositivos configurados. Clique em **Código de amostra para atributos personalizados** para visualizar um código de amostra usando atributos personalizados em um script.
9. Clique em **Salvar**.

Os nomes de atributo personalizados no script devem estar em letras minúsculas. Se os atributos personalizados são referidos em quaisquer scripts, então os atributos não podem ser removidos. Quando você modifica um atributo personalizado (por exemplo, seu nome) e se ele for associado a um script, então você deve fazer as mudanças correspondentes nos scripts associados.

Modificando um script

Para editar ou remover um script:

1. Acesse **Administrador > Todos os scripts**.
2. Na coluna **Ações** para o script, clique no ícone correspondente para editar ou excluir a ação.
3. Siga as instruções na tela para concluir a ação.

Quando um script (conteúdo, nome, descrição) é alterado, todas as configurações que estão associadas ao script são redistribuídas para os dispositivos.

Usando variáveis de script

Defina e armazene entradas de script, como variáveis de ambiente e de substituição, no repositório de scripts. Na configuração do script Mobile@Work para macOS, dependendo de qual script é vinculado, as variáveis de script relacionadas estarão disponíveis para uso quando necessárias. Esse recurso requer o Mobile@Work para macOS 1.71.0 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Utilize as variáveis para executar um script com diferentes valores a cada execução. Por exemplo, um administrador pode criar um script para utilizar a variável de ambiente ${userEmailAddress} como a variável de script e associá-la a uma configuração de script Mobile@Work para macOS. Quando a configuração é distribuída e instalada em cada dispositivo de usuário, o Ivanti Neurons for MDM envia um endereço de e-mail de usuário registrado diferente para que cada dispositivo realize determinadas ações. O portal administrativo do Ivanti Neurons for MDM suporta variáveis personalizadas.

Para adicionar uma variável de script:

1. Acesse **Administrador > Todos os scripts**.
2. Na seção Entrada de script, clique em **+ Adicionar**.
3. Na página pop-up Adicionar entrada de script – variável de ambiente, digite os seguintes dados:
    - Rótulo a ser exibido – este texto será mostrado como um rótulo na página de configuração do script Mobile@Work para macOS. Por exemplo, Inserir pasta SO, Inserir número Apache etc.
    - Nome da variável de ambiente – por exemplo, JAVA_HOME, OS_VERSION etc. O Ivanti Neurons for MDM substitui os valores das variáveis de script ao enviar os detalhes da configuração para um dispositivo de destino, sendo que os valores permanecem no banco de dados.

- Valor padrão da variável de ambiente: por exemplo, 1024, bin/java, ${PhoneNumber} etc. As variáveis de entrada seriam usadas no script carregado ou editado por um administrador. Veja também as seguintes observações.

4. Na região Pré-visualização, revise como o valor da variável de ambiente será mostrado na forma de entrada de script na página de configuração.
5. Clique em **Salvar**.

Dessa forma, apenas o rótulo e o valor padrão estão disponíveis para a configuração, mas o nome da variável de ambiente não é disponibilizado, o que fornece uma camada de abstração.

- Valores alfanuméricos (por exemplo, 1024, bin/java, root@localhost) ou atributos do sistema (por exemplo, ${userFirstName}) são aceitos como valor da variável de ambiente.
- Na página de configuração, é possível modificar ou excluir o valor da variável de ambiente durante a implantação.
- Se o valor da variável de ambiente não for fornecido, certifique-se de informar um valor durante a implantação do script. Caso contrário, o valor vazio será passado ao script.
- Depois da distribuição e instalação da configuração do script no dispositivo, a edição das variáveis de ambiente na página Administrador > Todos os scripts não afetará as configurações associadas ao script. Consulte também Configuração de script Mobile@Work para macOS.

Como editar uma variável de script

Para modificar uma variável de script, clique com o ícone de edição (lápis) na variável e salve as alterações.

Se uma configuração de script fizer referência a um script com variáveis, a edição do rótulo de uma variável de script existente também será refletida na configuração do script. No entanto:

- Uma alteração no valor padrão da variável de script não será refletida nas configurações existentes.
- Uma alteração no valor padrão da variável de script será refletida em todas as novas configurações criadas com o script anterior.

Como excluir uma variável de script

Para excluir uma variável de script, clique com o ícone para excluir (sinal de menos) na variável e confirme.

Uma variável de script recém-criada e a exclusão de uma variável de script existente serão refletidas inclusive em uma configuração já existente.

Testando um script

Teste rapidamente a execução de um script na ferramenta de depuração antes de testá-la em um dispositivo, sem necessidade de salvar os scripts. Este recurso requer o Mobile@Work para macOS 1.67 até a versão mais recente com suporte do Ivanti Neurons for MDM.

Procedimento

1. Acesse **Administrador > Todos os scripts**.
2. No Editor de scripts, adicione ou importe um script.
3. Se o locatário tiver vários espaços, selecione um espaço.
4. Na seção Script de teste, selecione **macOS** como plataforma.
5. No campo de texto **Localizar dispositivos**, encontre e selecione o dispositivo no qual o script pode ser testado. O dispositivo pode ser pesquisado pelo número de série,nome de usuário,nome do dispositivo eversão do SO.
6. Clique em **Testar agora**. Dessa forma, uma variável de ambiente pode ser adicionada, editada e excluída, e o script pode ser testado com esse estado (sem nem mesmo salvar as alterações realizadas).
7. Aguarde o script a ser enviado e executado no dispositivo.
8. Revise os resultados publicados do teste nas seções Entrada de script (que contém os detalhes da variável de ambiente), Saída de script e Atributos personalizados. Os valores padrão das variáveis de ambiente também são exibidos.

Verificando os resultados de execução de script

Para visualizar os registros dos resultados de execução de script:

1. Acesse **Dispositivos**.
2. Clique no nome do dispositivo.
3. Clique na guia de **Registros**.
4. Em uma linha que exibe a ação da Execução de script, você pode verificar as seguintes informações:

- nome do script na coluna Detalhes;
- status de execução do script na coluna Status;
- data e hora da execução do script na coluna Data; e
- registros de execução de script (registro de dispositivo plist) ao clicar no ícone de olho na coluna Ações.

5. Use os filtros para exibir as linhas **Execução de script**. Registros dessas linhas incluem o resultado (plist) do resultado padrão e erro padrão para os scripts.
6. Use os filtros para exibir as linhas **Processamento de resultado de execução de script**. Registros para essas colunas incluem detalhes (plist) de como os resultados foram processados.
   - Se um script não possui atributos personalizados associados a ele, não haverá resultados para processar. Esses scripts não serão exibidos na lista de linhas filtradas.
   - Se um script possuir atributos personalizados associados a ele e se eles estiverem no formato esperado, então os atributos personalizados dos resultados são mapeados e o status é exibido como Bem-sucedido. Você pode verificar os atributos personalizados e seus valores na guia **Atributos**.
   - Se um script possuir atributos personalizados associados a ele e se eles não estiverem no formato esperado, então os atributos personalizados dos resultados não são mapeados e o status é exibido como Erro.
   - Se o formato do resultado for correto, mas nem todos os atributos personalizados associados forem enviados no resultado, o status é exibido como Erro.
   - Se uma variável de script for enviada junto com o script, os logs do Processamento de resultado da execução do script incluirão detalhes (plist) da variável de script.

Tópicos relacionados:

- Configuração de script Mobile@Work para macOS
- Como criar uma configuração

Atribuição de marca

Esta seção contém os seguintes tópicos:

Administrador > Catálogo de aplicativos para Apple (Atribuição de marca)

Licença: Gold

É possível atribuir uma marca ao **catálogo de aplicativos**[1] da Apple para torná-lo mais familiar para seus usuários finais de dispositivos iPhone, iPad e Mac. É possível personalizar os seguintes itens no catálogo de aplicativos para Apple:

- Ícone do aplicativo (PNG, 360 pixels quadrado)
- Nome do aplicativo
- Imagem do banner do aplicativo (PNG, 360x64)
- Cor do texto

Existem dois modos de acessar o App Catalog da Apple: **App Catalog independente** e **App Catalog integrado**. O App Catalog independente está disponível para iPhone, iPad e dispositivos Mac. O Catálogo de Aplicativos integrado está disponível para dispositivos iOS e Mac.

Dando uma marca ao Apple app catalog

As alterações feitas nesta página afetam a tela inicial, tela de apresentação e tela de início do aplicativo. O procedimento é semelhante tanto para o App Catalog independente quanto para o App Catalog integrado.

Procedimento

1. Na página **Atribuir uma marca ao App Catalog da Apple**, clique em **Personalizar** (canto superior direito).
2. Na sessão **Ícone do aplicativo**, arraste o arquivo do logotipo até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo no seu sistema de arquivos. O ícone do aplicativo é exibido na tela inicial do iOS

[1] a list of mobile apps you have made available for your users. Includes apps that users can download from public app stores and apps you intend to distribute using the device management system (In-house apps).

3. Na seção **Nome do aplicativo**, edite o texto **Nome do App Catalog** para alterar o rótulo mostrado na tela de apresentação.
4. O nome e o ícone são aplicados no banner da tela inicial. Para alterar uma imagem do banner personalizado, desmarque a opção **Aplicar o nome e o ícone no banner da tela inicial**. Isso exibirá a seção **Imagem do banner do aplicativo**.
5. Para alterar a imagem do banner do aplicativo, arraste e solte o novo arquivo de imagem do banner na caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo no seu sistema de arquivos. A imagem do banner do aplicativo aparece na barra superior na tela inicial do aplicativo.
6. Na seção **Cor do texto**, clique na caixa de código de cor hexadecimal para escolher uma cor ou insira o código de cor hexadecimal a ser atribuído ao texto e aos ícones. Isso será aplicado ao texto na tela de apresentação, nome do aplicativo, banner e botão de ação.
7. Clique em **Salvar alterações**.

O nome do App Catalog inserido se aplica a Android, iOS e macOS.

Dando uma marca ao Android App Catalog

Licença: Gold

Atribua a marca ao Android **app catalog**[1] para deixá-lo com uma aparência mais familiar para seus usuários finais. É possível personalizar os seguintes itens no catálogo de aplicativos para Android:

- Logotipo do catálogo (PNG, 360x64)
- Nome do catálogo
- Cor da barra de ações
- Ícone de atalho
- Nome do atalho

Dando uma marca ao Android app catalog

Procedimento

1. Na tela **Atribuição de marca ao App Catalog para Android**, clique em **Personalizar** (canto superior direito).
2. Para alterar o logotipo do App Catalog, arraste o arquivo do logotipo até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo no seu sistema de arquivos.
3. Clique no campo **Cor da barra de ações** para exibir uma paleta de cores para seleção ou insira o número hexagonal da cor de sua preferência.
4. Edite o texto **Nome do Catálogo de Aplicativos** para alterar o rótulo do catálogo.

   O nome do App Catalog inserido se aplica a Android, iOS e macOS.
5. Para alterar o ícone do atalho, arraste o arquivo do ícone até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo no seu sistema de arquivos.

---

[1] a list of mobile apps you have made available for your users. Includes apps that users can download from public app stores and apps you intend to distribute using the device management system (In-house apps).

6. Edite o texto do **Nome do atalho** para alterar o rótulo do atalho do aplicativo.
7. Clique em **Salvar alterações**.

Administrador > Atribuição de marca para o quiosque Android

Licença: Silver

Atribua a marca na página do quiosque Android para deixá-lo com uma aparência mais familiar para seus usuários finais. É possível personalizar os seguintes itens:

- logotipo do banner (PNG, 840x114) ou texto
- cor da borda do banner
- cor de fundo do banner
- cor de fundo da tela
- imagem do plano de fundo da tela (1280x800)
- formato do plano de fundo da tela

Como atribuir marca ao quiosque Android

Procedimento

1. Navegue até **Administrador>Quiosque Android**.
2. Na página **Atribuição de marca ao modo de quiosque**, clique em **Criar marca**.
3. No campo **Nome**, digite o nome da atribuição de marca ao modo de quiosque.
4. Se você quiser desativar o banner, desmarque **Habilitar banner superior**.
5. Clique no campo **Cor de fundo do banner** para exibir uma paleta de cores para seleção ou insira o número hexadecimal da cor de sua preferência.
6. Clique no campo **Cor da borda do banner** para exibir uma paleta de cores para seleção ou insira o número hexadecimal da cor de sua preferência.
7. Selecione **Imagem/Logotipo** ou **Texto** para definir o conteúdo do banner.
8. Se você selecionar **Imagem/Logotipo**, arraste e solte o arquivo de imagem ou clique em **Escolher arquivo** para selecionar um.
9. Se você selecionar **Texto**, digite o texto que deseja exibir no banner.

10. Clique na guia **Plano de fundo**.
11. Clique no campo **Cor de fundo** para exibir uma paleta de cores para seleção ou insira o número hexadecimal da cor de sua preferência.
12. Para alterar a imagem do plano de fundo:

    a. Exclua a imagem padrão.

    b. Arraste e solte a imagem de sua preferência ou clique em **Escolher arquivo** para selecionar um.

    c. Selecione o layout preferido.
13. Clique em **Salvar alterações**.
    A atribuição de marca criada ao modo quiosque é exibida na página **Atribuição de marca ao modo de quiosque**. Para mais edições na atribuição de marca personalizada, clique no ícone Editar na coluna **Ações**. Para excluir a marca personalizada, clique no ícone Excluir. Quando a marca de quiosque personalizada for excluída, a configuração que a utiliza passará a usar a marca padrão.

Colocar marca em modelos de email

Você pode atribuir a marca ao convite de email do usuário final para deixá-lo com uma aparência mais familiar para seus usuários finais. Clique em **Reverter para configurações padrão** para limpar as personalizações.

Você pode personalizar os seguintes modelos de email em todos os idiomas suportados:

- **Convite para o usuário final** – Convide um usuário a conectar seus dispositivos para obter acesso a apps e configurações.
- **Notificação de redefinição de senha** – O sistema envia e-mails de lembrete sete dias e 24 horas antes de expirar a senha para contas locais. Isso não se aplica às contas do LDAP.
- **Confirmação de registro** – E-mail enviado após um usuário concluir o registro. Use para agradecer aos usuários pelo registro e informar mais recursos de aprendizado.
- **Notificação de conformidade com as políticas** – E-mail enviado quando os dispositivos ficam fora de conformidade.

Esta seção contém os seguintes tópicos:

- "Pré-visualização e teste de modelo de email" abaixo
- "Personalizar os cabeçalhos de mensagem" na página seguinte
- "Personalizando um modelo de e-mail" na página 1434
- "Variáveis de e-mail suportadas" na página 1439

Pré-visualização e teste de modelo de email

É possível pré-visualizar e testar modelos de email. O teste permite enviar um email com base no modelo para um endereço de email especificado.

Para pré-visualizar e testar um modelo de email:

1. Clique em **Administrador**.
2. Em Modelos de e-mail, clique em **Convite para o usuário final**, **Notificação de redefinição de senha**, **Confirmação de registro** ou **Notificação de conformidade com as políticas**.
3. Clique no link **Pré-visualizar e testar** associado ao modelo de email que deseja pré-visualizar e testar.
4. Visualize o modelo renderizado no painel de modelo renderizado.
5. Especifique um endereço para o qual deseja enviar o email de teste.

   Se o endereço de e-mail especificado pertencer a um usuário atual, o e-mail de teste substituirá os valores da maioria das variáveis de modelo de e-mail, dando uma ideia muito precisa da experiência do usuário com o e-mail. Mas o e-mail de teste não substitui valores de variáveis que o Ivanti Neurons for MDM gera no momento em que é criado um convite de e-mail real.
6. Clique em **Enviar email de teste**.

Personalizar os cabeçalhos de mensagem

1. Clique em **Administrador**.
2. Clique em **Modelos de email**.
3. Clique no link do ícone **Editar** (na coluna Ações) associado ao modelo de email que deseja editar.
4. Forneça novas configurações conforme desejado para **Nome de exibição do email**, **Endereço de email remetente** e **Responder para endereço de email**.

   Ao personalizar as opções de envio e resposta de endereços de e-mail, recomendamos que você inclua o Serviço de retransmissão de e-mail na lista de permitidos para garantir que seus e-mails não sejam bloqueados por serviços de filtragem de SPAM de e-mail. Consulte este documento para obter mais informações.
5. Clique em **Salvar**.
6. Reveja a pré-visualização do modelo de email e clique em **Salvar**.

Personalizando um modelo de e-mail

1. Selecione **Admin** > **Identidade visual** > **Modelos de e-mail**.
2. Selecione o modelo a editar, **Convite para o usuário final**, **Notificação de redefinição de senha**, **Confirmação de registro** ou **Notificação de conformidade com as políticas**.
3. Clique no ícone de caneta de edição ao lado do modelo de email que deseja personalizar.

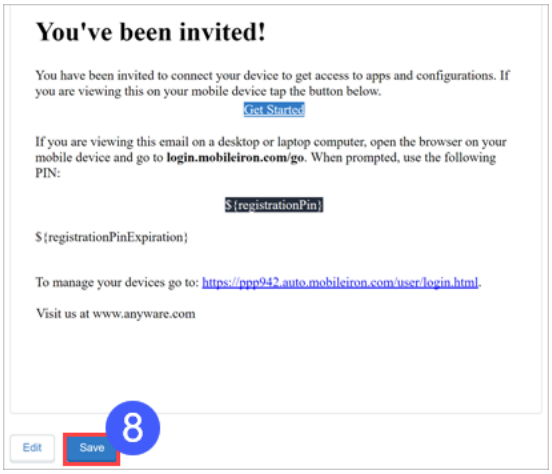
4. Se desejar, edite a linha de assunto.

5. Edite o modelo de e-mail que contém elementos HTML no painel do corpo para personalizar o conteúdo da mensagem.

   Você pode usar as variáveis exibidas à direita no corpo do email. Veja as Variáveis de email suportadas.

6. Clique em **Pré-visualizar** para pré-visualizar o modelo de email conforme cria as iterações de acordo com as suas necessidades.

7. Quando estiver pronto para salvar o modelo, clique em **Pré-visualizar**. Isso renderiza a pré-visualização e fornece a função de salvar.



8. Clique em **Salvar** se estiver satisfeito com a pré-visualização.

Conteúdo permitido e bloqueado em convite personalizado do usuário

Enquanto você personaliza o modelo de e-mail de convite do usuário no **Convite do usuário final**, há um conjunto de tags HTML na lista de permitidos e atributos que são permitidos. Também existe uma lista de sequências bloqueadas que não são permitidas no convite do usuário para evitar vulnerabilidade de Cross Site Scripting (XSS).

Você pode usar apenas as tags e os atributos permitidos no e-mail de convite. A tabela a seguir lista as tags permitidas e os atributos correspondentes que são permitidos.

Algumas tags Permitidas (exemplo: <big>) não devem ter nenhum atributo Permitido e, portanto, são exibidas em branco.

Tags permitidas	Atributos permitidos
<big>	[]
<img>	["id","label","editable","height","border","src","style","width", "align", "class","cellpadding","alt","title","data-max-width","data-default"]
	[]
<singleline>	["label"]
<tbody>	[]
<!DOCTYPE>	[]
<h1>	["style"]
<h2>	["style"]
<hr>	["noshade","style"]
<h3>	[]
<body>	["style", "class", "bgcolor", "paddingwidth", "paddingheight", "offset", "toppadding", "leftpadding", "lang","link","vlink","border","cellspacing","cellpadding"]
<title>	["id"]
<head>	[]

	["style","class","width","align","id"]
 	[]
<path>	["d"]
	["style"]
<html>	["xmlns","xmlns:mso","xmlns:msdt"]
	["start"]
<table>	["class","width","border","cellspacing","cellpadding","style","height","bgcolor", "align","background"]
<a>	["href","style","target","rel","class","title"]
<b>	[]
<o:p>	[]
<svg>	["xmlns","class","viewbox","width","height","role","aria-labelledby"]
	[]
	[]
<i>	[]
<label>	["style"]

<td>	["valign","width","height","class", "cellpadding", "cellspacing","border","bgcolor","align", "style","colspan","id"]
<p>	["style","class","align"]
<u>	[]
<meta>	["name","content","http-equiv","charset"]
<multiline>	["label"]
<style>	["type","id"]
	["style"]
<tr>	["style"]
	["style","class","lang"]
<font>	["color"]

A seguir está a lista de sequências bloqueadas que não são permitidas no convite personalizado do usuário.

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4- ,+ADw-/SCRIPT+AD4-, xml:base
- Caracteres especiais e pesquisa para javascript ou script
- O conteúdo meta possui "url=" que diferencia maiúsculas de minúsculas
- O img src não contém .svg.
- Valor de atributo contendo "\00"

Se alguma das sequências acima bloqueadas for usada no conteúdo HTML do convite de usuário final, uma mensagem de erro será exibida ao clicar em **Pré-visualização**. Essa mensagem de erro lista o conteúdo HTML que não é permitido no convite do usuário final. Editar e remover o conteúdo HTML que não é permitido e, então, clicar em **Pré-visualizar** para continuar.

Você não poderá salvar os modelos editados que possuem conteúdo HTML bloqueado.

Variáveis de e-mail suportadas

O Ivanti Neurons for MDM oferece diversas variáveis que podem ser usadas para personalizar seus modelos de e-mail.

Variáveis de convite do usuário final

Variável	Descrição
${userActivationUrl}	O URL de ativação do usuário – este é ohiperlink em torno dotexto ${email.idp.invitation.get.started}.
${clusterRegistrationUrl}	O URL de registro do cluster – NÃO éencontrado no modelo padrão, mas éindiretamente referenciado (através davariável ${email.idp.invitation.pg4}).
${productBrandName}	O nome da marca do produto - definido como a tag <title> no cabeçalho do modelo padrão.
${companyLogoUrl}	O URL do logotipo da empresa – esta é aimagem no modelo padrão – eleaponta para uma imagem no MobileIronCDN.
${message:${email.idp.invitation.register.your.device}	O registro do título do dispositivo do usuário.
${message:${email.idp.invitation.title}}	Título do convite por e-mail.
${message:${email.idp.invitation.pg1}}	Confirmação de que o usuário está no dispositivo.
${message:${email.idp.invitation.get.started}}	O texto do convite por e-mail Introdução.
${message:${email.idp.invitation.pg2}}	Instruções de login e registro.
${message:${email.idp.invitation.pg3}}	E-mail e aplicativos enviados às informações do dispositivo.
${message:${email.idp.invitation.pg4}}	Informações de registro se o usuário não estiver em seu dispositivo, o que inclui o URL de registro do cluster.
${message:${email.footer}}	O rodapé do convite por e-mail que inclui o rótulo do site da empresa.
${companyWebsiteLabel}	O rótulo do site da empresa – NÃO éencontrado no modelo padrão, mas éindiretamente referenciado (por meio davariável ${email.footer}).

Variáveis de notificação de expiração de senha

Variável	Descrição
${passwordResetUrl}	O URL de redefinição de senha.
${productBrandName}	O nome da marca do produto - definido como a tag <title> no cabeçalho do modelo padrão.
${companyLogoUrl}	O URL do logotipo da empresa – esta é aimagem no modelo padrão – eleaponta para uma imagem no MobileIronCDN.
${message:${password.expiration.notification.title}}	O título da notificação de expiração de senha.
${message:${password.expiration.notification.pg1}}	O parágrafo introdutório da notificação de expiração de senha.
${message:${email.password.reset.url.name}}	O nome da URL de redefinição de senha.
${message:${email.footer}}	O rodapé do convite por e-mail que inclui o rótulo do site da empresa.
${companyWebsiteLabel}	O rótulo do site da empresa – NÃO éencontrado no modelo padrão, mas éindiretamente referenciado (por meio davariável ${email.footer}).

Variáveis de confirmação de registro

Variável	Descrição
${productBrandName}	O nome da marca do produto - definido como a tag <title> no cabeçalho do modelo padrão.
${companyLogoUrl}	O URL do logotipo da empresa – esta é aimagem no modelo padrão – eleaponta para uma imagem no MobileIronCDN.
${message:${email.confirmation.title}}	O título de confirmação do registro.
${message:${email.confirmation.pg1}}	O parágrafo introdutório da confirmação do registro.

Variáveis de conformidade com as políticas

Variável	Descrição
${policyMessageTitle}	Essa variável será substituída pelo conteúdo que é inserido na linha de assunto da ação de conformidade de envio de e-mail dentro da política.
${policyMessageContent}	Essa variável será substituída pelo conteúdo que é inserido na mensagem da ação de conformidade de envio de e-mail dentro da política.
${productBrandName}	O nome da marca do produto - definido como a tag <title> no cabeçalho do modelo padrão.
${companyLogoUrl}	O URL do logotipo da empresa – esta é aimagem no modelo padrão – eleaponta para uma imagem no MobileIronCDN.
${message:${email.footer}}	O rodapé do convite por e-mail que inclui o rótulo do site da empresa.
${companyWebsiteLabel}	O rótulo do site da empresa – NÃO éencontrado no modelo padrão, mas éindiretamente referenciado (por meio davariável ${email.footer}).

Variáveis de atributos de usuário personalizados

Um administrador pode usar atributos de usuário personalizados como variáveis de email no modelo de email personalizado com as seguintes condições:

- Os atributos de usuário personalizados estão na página **Administrador > Atributos**.
- Um administrador designou os atributos de usuário personalizados a usuários e forneceu valores aos atributos de usuário personalizados para cada usuário.

Portal de autosserviço

O convite para registro inclui um link para o Portal de autosserviço. Os usuários finais podem usar esse portal para realizar as seguintes tarefas:

- Bloqueio (não compatível com o Windows Phone 8.1)
- Desbloqueio (não compatível com o Windows Phone 8.1)
- Exibir localização (se habilitada na configuração de privacidade; não compatível com Windows Phone 8.1)
- Apagar
- Desativar
- Altere as informações da conta (nome, senha, endereço de e-mail)
- Forçar registro (não compatível com o Windows Phone 8.1)
- Adicionar certificados de criptografia e assinatura

Para registrar dispositivos adicionais, os usuários finais clicam no link do portal de registro exibido no Portal de autosserviço.

Se os usuários finais inserirem a URL de maneira errada no Portal de autosserviço, envie-os para https://mydevices.mobileiron.com/user/login.html.Para usuários do iOS, considere criar uma Configuração do Web Clip para o Portal de autosserviço.

Upload de certificados de assinatura e de criptografia

Você pode permitir que os usuários finais carreguem seus certificados de assinatura e criptografia de e-mail no Portal de autoatendimento, na configuração Certificados fornecidos pelo usuário. É possível alterar essa configuração usando a configuração Certificados fornecidos pelo usuário. Com isso configurado, os usuários finais podem fazer upload de seus certificados de assinatura e criptografia de e-mail.

1. Na guia **Meus certificados**, clique em **Adicionar certificado**. A janela **Adicionar certificado** é exibida.
2. Atualize os seguintes campos:

Nome do campo	Descrição
Tipo do certificado	Selecione o tipo do certificado que será transferido. As opções são: • **Certificado de criptografia** • **Certificado de assinatura** Essas opções são criadas no portal administrativo do Ivanti Neurons for MDM. Consulte Configuração do certificado de identidade para mais informações.
Certificado a ser transferido	Clique em **Escolher arquivo** para selecionar o certificado a ser transferido. O arquivo precisa estar no formato PKCS12.
Senha	Insira a senha do arquivo.

3. Clique em **Upload**.

Após o upload, você pode visualizar a lista de certificados em uma tabela com os seguintes detalhes.

Nome do campo	Descrição
Nome do certificado	Especifica o tipo de certificados, **Criptografia** ou **Assinatura**.
Emitido por	os detalhes do certificado emitido.
Transferido em	A data em que o certificado foi transferido.
Data da expiração	A data de expiração do certificado.
Ações	Você pode realizar as seguintes ações: • **Editar certificado** – editar detalhes do certificado. • **Limpar chave privada** - exclui a chave privada do pacote de certificados (PKCS#12). • **Excluir certificado** – exclui o certificado do servidor do Ivanti Neurons for MDM.

Quando o usuário faz upload de uma configuração de certificado, o servidor envia novamente por push a configuração que está usando o certificado.

Excluir e apagar a chave privada por um usuário não reenvia as configurações por push.

Para obter mais informações, consulte Identidade visual do Portal de autoatendimento.

Portal de autosserviço (Atribuição de marca)

Licença: Silver

Você pode personalizar o Portal de autosserviço com o logotipo da sua organização. Se você não adicionar seu logotipo, o Portal de autosserviço exibe o logotipo do serviço padrão.

Atribuição de marca ao portal de autosserviço

Procedimento

1. Na tela Atribuição de Marca ao Portal de Autosserviço, clique em **Personalizar** (canto superior direito).
2. Arraste o arquivo de logotipo (PNG, 182x34) para a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo em seu sistema de arquivos.
3. Clique em **Salvar alterações**.

Atribuição de marca ao registro de vários usuários (clipe da Web)

Personalize o registro seguro de vários usuários do iOS adicionando um novo título e ícone do clipe da Web.

Procedimento

1. Acesse **Admin > Registro de vários usuários (clipe da Web)**.
2. Na tela Registro de vários usuários (clipe da Web), clique em **Personalizar**.
3. Arraste o arquivo de logotipo até a caixa pontilhada ou clique em **Escolher arquivo** para selecioná-lo do seu sistema de arquivos.
4. Para alterar o rótulo, edite o texto **Entrada segura**.
5. Para alterar o ícone do clipe da web, arraste e solte o arquivo de clipe da web na caixa pontilhada ou clique em **Escolher arquivo** para selecionar o arquivo no seu sistema de arquivos.
6. Visualize as atualizações e clique em **Salvar alterações**.

Para dispositivos iPhone e iPod touch, crie ícones com 120 x 120 pixels ou 60 x 60 pixels (resolução padrão).

Para dispositivos iPad, crie ícones com 152 x 152 pixels ou 76 x 76 pixels (resolução padrão).

Para obter mais informações, consulte Entrada segura multiusuário para iOS.

Adição do gerenciamento de dispositivos que não tem iOS

Licença: Gold

Você está usando uma versão do Ivanti Neurons for MDM que é otimizada para dispositivos iOS. Esta seção descreve como alternar para permitir o gerenciamento de dispositivos não iOS. Após alternar, você também poderá gerenciar os seguintes dispositivos:

- Android 5.0 ou versões mais recentes com suporte
- Windows Phone 8.1
- Windows 10 móvel e desktop

A alternância para incluir a gestão de dispositivos não iOS não poderá ser revertida.

Para alternar com o intuito de incluir dispositivos não iOS:

1. Clique em **Administrador > Plataformas permitidas**.
2. Clique no botão **Permitir todas as plataformas**.
3. Marque a opção **Compreendo que essa ação não poderá ser desfeita** para confirmar que você sabe e entende que a operação não pode ser desfeita.
4. Clique no botão **Permitir todas as plataformas**.

Pacotes

Esta seção contém os seguintes tópicos:

Pacotes Secure UEM e Secure UEM Premium

Os pacotes Secure UEM e Secure UEM Premium oferecem os seguintes recursos:

	Secure UEM	Secure UEM Premium
Device management and security		
Easy on-boarding	✓	✓
Multi-OS security and management	✓	✓
Secure email gateway	✓	✓
App distribution and configuration	✓	✓
Mobile application management (MAM)	✓	✓
Scale IT operations		
Helpdesk tools	✓	✓
Reporting	✓	✓
Secure connectivity		
Per app VPN		✓
Conditional Access		✓
Secure productivity		
Secure email and personal information management (PIM) app		✓
Secure web browsing		✓
Secure content collaboration		✓
Mobile app containerization		✓
Derived Credentials		✓
Zero Sign-On		
Passwordless user authentication (single app)		✓

Esses pacotes estão sujeitos a alterações. Você deve entrar em contato com o setor de Vendas Ivanti para confirmar o esquema atual.

Antigos pacotes Bronze, Silver e Gold

Esta seção descreve os antigos pacotes Bronze, Silver e Gold. Os pacotes evoluíram para o esquema Secure UEM e Secure UEM Premium.

Bronze

Os recursos básicos do Ivanti Neurons for MDM são fornecidos no pacote Bronze. Você pode expandir o pacote Bronze:

- adicionando mais dispositivos
- adicionando Silver
- adicionando Gold
- adicionando Platinum

Essas adições expandem sua solução móvel além da configuração básica do dispositivo.

Os administradores podem entrar em contato com o Suporte se desejarem ativar um ou mais recursos sob demanda que estão desativados por padrão em seus locatários.

Licença

O upgrade para a versão Silver adiciona os seguintes recursos:

- **LDAP e Connector:** suporte para adicionar diretórios corporativos e autoridades de certificação no Ivanti Neurons for MDM.
- **Sentry:** suporte para controle de acesso ao email.
- **Espaços:** Suporte para designar dispositivos para o gerenciamento por administradores diferentes (administração delegada).
- **Modo supervisionado:** suporte em nível de dispositivo para configuração refinada, incluindo modo de aplicativo único.
- **Atribuição de marca ao portal de autosserviço:** use seu logotipo no portal de autosserviço.
- **Autoridades de certificação:** use o Ivanti Neurons for MDM como uma autoridade de certificação.
- **Instalação/desinstalação silenciosa de aplicativos:** implante e remova apps automaticamente de um dispositivo móvel.
- **Lista de apps permitidos/bloqueados/obrigatórios:**monitore e controle quais apps são instalados nos dispositivos.

- **Filtro de conteúdo da Web:** aplique políticas de lista de permitidos/bloqueados do site a todos os navegadores da web.
- **Funcionalidade específica da Apple:** habilitar/restringir AirPlay, AirDrop, distribuição de papel de parede iOS e Apple TV.
- **Gerenciamento de abertura:** controle quais aplicativos móveis podem abrir determinado conteúdo corporativo.
- **Apps and Books da Apple:** distribua licenças de aplicativos móveis aos dispositivos, recupere e atribua novamente essas licenças quando o dispositivo for desativado.
- **Suporte do Android enterprise (AFW)**
- **Registro de dispositivo:** permite que os clientes comprem dispositivos em grande volume e registrem automaticamente os dispositivos da Apple no MDM durante a ativação.
- **Configuração por aplicativo:** implante aplicativos móveis configurados em grande escala com pouca ou nenhuma ação obrigatória do usuário final.
- **Por VPN de aplicativo de terceiros:** agora, a segurança VPN é imediata, invisível e específica do aplicativo móvel.
- **Ações em camadas da política**
- **Filtros de distribuição de aplicativos**
- **Trilhas de auditoria**
- **Modo quiosque Android:** suporte para configurar dispositivos Android para operarem no modo quiosque.
- **Atribuição de marca para o quiosque Android:** altere o plano de fundo e o banner da tela do quiosque, exibidos na operação do dispositivo no modo de quiosque.
- **Prevenção de perda de dados (DLP) do Office 365 via APIs Microsoft Graph**: reforça controles de DLP para apps do Office 365 via APIs de gráfico.

Licença

Atualizar para a Gold inclui os recursos fornecidos pela Silver, além dos seguintes recursos:

- **Logon único:** os usuários se autenticam uma vez e são conectados automaticamente a outros aplicativos móveis corporativos.
- **Aplicação de marca personalizada no App Catalog para Android e iOS:** exiba o logotipo da sua empresa no App Catalog.
- **Limite de conteúdo aumentado:** 50 arquivos, 25 MB cada
- **AppConnect para iOS**: proteja e configure apps habilitados para AppConnect.
- **AppTunnel para iOS:** proteja o acesso de aplicativos a recursos corporativos.
- **Docs@Work para iOS:** permita que os usuários visualizem, armazenem e compartilhem documentos.
- **Logon único baseado em certificado do iOS 8**
- **Gerenciamento de iBook/ePub do iOS 8**
- **Suporte ao macOS**
- **Identidade visual do usuário**
- **Mobile Application Management (MAM) com AppConnect**
- **Credenciais derivadas**
- **Suporte a Windows 10 (inclui Bridge)**

Platinum

Atualizar para a versão Platinum inclui os recursos fornecidos pela Gold, além dos seguintes recursos:

- **Tunnel:** configure o acesso específico do aplicativo aos dados corporativos.
- **Help@Work**
- **Monitorar**
- **ServiceConnect (ServiceNow, Splunk)**

Área restrita para pré-visualização ou testes

Mediante aquisição do suporte **Premium Plus**, os clientes do Ivanti Neurons for MDM podem obter um locatário de área restrita para pré-visualizar e testar novas versões antes que elas cheguem à produção.

Como atualizar

Esta seção contém os seguintes tópicos:

Atualização de licença

Os recursos básicos são fornecidos no pacote Bronze. Você pode expandir o pacote Bronze:

- adicionar mais dispositivos
- adicionando Silver
- adicionando Gold
- adicionando Platinum

Essas adições expandem sua solução móvel além da configuração básica do dispositivo.

Solicitação de upgrade

Procedimento

1. Selecione **Opções de atualização** no menu suspenso do administrador.
2. Clique em **Solicitar atualização / Adicionar dispositivos** (canto superior direito).
3. Selecione os itens que você deseja adicionar e insira seu número de telefone.

   Um representante entrará em contato dentro de 24 horas com os detalhes.

Como fazer a atualização de uma versão anterior

Ao fazer uma atualização a partir de uma versão anterior, as configurações na página **Editar perfil de registro do dispositivo** não serão mantidas. Consulte as suas configurações antes de atualizar.

- Se a opção **Pular acesso ao ID da Apple e iCloud** estiver ativada, a opção **Pular configurações do Apple Pay** será habilitada após a atualização.
- Se a opção **Pular inserir senha** estiver ativada antes da atualização, as opções **Pular Touch ID** e **Pular configuração do Apple Pay** serão habilitadas após a atualização.

Procedimento

1. Após a conclusão da atualização, retorne à página **Editar perfil de registro do dispositivo** para editar o perfil de Registro do dispositivo e restaurar as configurações desejadas.
2. Clique em **Salvar**.

Após a atualização, várias definições de configuração são afetadas.

Opções de promoção são **desativadas**.

As configurações de instalação estão definidas como **Não**.

A opção **Não mostrar no App Catalog** não está mais selecionada.

Instalar silenciosamente no Android Samsung Knox está definido como Falso.

Os sinalizadores de gerenciamento do iOS estão definidos como:

- Backup no iCloud.
- Remover ao descadastrar.

Essas definições de sinalizadores de gerenciamento do iOS podem ser selecionadas para cada aplicativo individualmente.

Configurações do aplicativo:

- Os ajustes de aplicativo são agora chamados de configurações.
- Todas as demais definições de aplicativo continuam como eram antes da atualização.

Para obter mais informações, consulte Pacotes.

Licenças do dispositivo

Ivanti Neurons for MDM as licenças baseadas em dispositivo definem o número de dispositivos que podem ser registrados, a quantidade de conteúdo que pode ser configurada para distribuição aos dispositivos e quais recursos estão disponíveis. Se você chegar ao limite de dispositivos, será exibido um triângulo vermelho na página Administrador. Se você alcançar o limite de conteúdo, o serviço irá impedir mais adições e exibirá uma mensagem indicando que você alcançou o limite.

Abrindo um tíquete de suporte

Visite o Portal de Suporte Ivanti para abrir um chamado de suporte.