AppTec360 Enterprise Mobile Manager e ContentBox

Manual de Administração | Versão 5.0 (202110)

Índice

Visão geral

- Introdução ao AppTec360
- Sistemas operativos de dispositivos suportados
- Directórios LDAP suportados
- Explicação do “Modo Supervisionado” nos dispositivos Apple
  - Disponível no modo supervisionado
  - Ativar o modo supervisionado
  - Adiciona um dispositivo à DEP
- Explicação sobre o Android Enterprise
  - O que é o Android Enterprise?
  - Quais são os requisitos para utilizar o Android Enterprise?
  - Quais são os modos disponíveis no Android Enterprise?
  - Como posso atribuir aplicações a dispositivos Android Enterprise?
- Carrega as tuas próprias aplicações para a Google Play Store

Requisitos e instalação

- Requisitos
  - Requisitos do sistema
  - Chave de licença
  - Endereço IP e resolução DNS
  - Certificado SSL
  - Servidor SMTP
  - Regras de firewall
- Actualizações de segurança
  - Senhas padrão do dispositivo virtual
- Configuração do aparelho virtual
  - Preparação
    - Configura a partir de um anfitrião externo
  - Primeiro passo – Licença do aparelho
  - Segundo passo – Certificado SSL
    - Automático

- Personalizado
- Terceiro passo – Definições do servidor
- Quarto passo – Configuração do MySQL
- Quinto passo – Contrato de licença
- Resolução de problemas
- Recomendações de segurança

Definições gerais

Visão geral da conta

- Informações sobre a conta
  - Visão geral
  - Relatório de erros
  - Pedido de funcionalidades

Configuração global

- Definições de eMail
- Modelos de eMail
- Inscrição no SMS

Privacidade

- Acesso GPS

Acesso baseado em funções

- Gestão de funções
- Atribuições de funções
  - Atribuição de uma função
- Acesso à API
  - Acede à API REST da AppTec360
  - Regras gerais
  - Exemplo de pedido
  - Consultas
  - Exemplo de código em Python3

Configuração da Apple

- Certificado APNS
  - Passo 1
  - Passo 2
  - Passo 3
- Acesso gerido

- Inscrição de utilizadores
- iPad partilhado
- DEP
- Configurador e URL
  - URLs de inscrição na piscina
  - Perfil MDM – Configurador da Apple

Configuração do Android

- Configuração do Android
- Inscrição automática
- Android Enterprise
  - Primeiro método: Conta empresarial Android (Conta Google)
  - Segundo método: Conta G-Suite
  - Proteção contra reposição de fábrica
- Inscrição na AE
  - Método 1: Inscrição no código QR
  - Método 2: Registo NFC
  - Método 3: Conta Google
- KNOX Inscrição
- Zero-Touch

Configuração do Windows

- Configuração do Windows

ContentBox

- Configuração

Configuração LDAP

- Visão geral do LDAP

Gestão de aplicações

- BD de aplicações internas
  - Android
  - iOS
  - MacOS
  - Windows 10
- Definições da aplicação
  - Definições da aplicação iOS
  - Definições da aplicação Android

- Aplicações de terceiros
  - Android
  - iOS
- VPP / KNOX Premium
  - Licenças VPP
  - Token VPP
  - KNOX Premium Key
- Definições da App Store
  - Região e língua
- AE Play Store
  - Aplicações aprovadas
  - Aplicações da Play Store
  - Aplicações privadas
  - Aplicações Web
  - Layout da loja
- Pacote de aplicações

Controlo remoto

- TeamViewer
  - Conector TeamViewer
  - Instalar o TeamViewer QuickSupport
  - Controla o teu dispositivo à distância
  - Acesso sem vigilância
- Splashtop

Gestão de cartões SIM

- Importação em massa de CSV
- Transportadora e tarifa

Gestão de assinaturas

- Gestão de assinaturas

Registo geral de auditoria

- Registo de auditoria
- Definições do registo de auditoria

Gestão de certificados

Gestão móvel

Ecrã de gestão móvel

- Filtro do dispositivo
- Janela de pesquisa
- Opções de engrenagem
- Setas de navegação

Definições da conta de administração

- Informações do utilizador
- Definições da consola
- Registo de início de sessão

Administração da empresa (nó-raiz) na gestão móvel

- Criar um subgrupo
- Renomear o nó raiz
- Inscrição em massa
- Atribuição de massa
- Administração rápida de aplicações
- Importação de utilizadores CSV

Gestão de grupos na gestão móvel

- Criar um subgrupo
- Edita o grupo selecionado
- Elimina o grupo selecionado
- Criar um utilizador
  - Cria um novo utilizador-administrador

Gestão de utilizadores na gestão móvel

- Adicionar e registar um dispositivo

Gestão de perfis em Mobile Management

- Cria um perfil
- Editar perfil
- Copia o perfil
- Eliminar perfil
- Herança de perfis

Gestão de dispositivos na gestão móvel

- IOS
  - Editar dispositivo
  - Limpar código de acesso
  - Dispositivo de bloqueio

- Dispositivo de encerramento
- Reinicia o dispositivo
- Alarme e modo perdido | Desativar modo perdido
- Eliminar dispositivo
- Limpa o dispositivo
- Limpeza da empresa | Remover MDM
- Enviar mensagem
- Controlo remoto do TeamViewer
- Enviar pedido de inscrição

Android

- Editar dispositivo
- Limpar código de acesso
- Dispositivo de bloqueio
- Eliminar dispositivo
- Limpa o dispositivo
- Remove a MDM
- Enviar mensagem
- Passa para o modo COPE
- Enviar pedido de inscrição
- Migra o dispositivo antigo

Janelas

- Editar dispositivo
- Eliminar dispositivo
- Limpeza da empresa | Remover MDM
- Controlo remoto do TeamViewer
- Enviar pedido de inscrição

Gestão de conteúdos

- Ficheiros de grupo
- Explorador de ficheiros
- Pista de auditoria
- Lixo
- Armazenamento externo

Registo de auditoria

Configuração do iOS

- Geral
  - Síntese do perfil do grupo (apenas a nível do grupo)
  - Informações gerais
  - Definições
  - Revisão da configuração
  - Registo do dispositivo (apenas ao nível do dispositivo)
    - Registo de comandos
    - Status de comando possíveis
- Gestão de activos (apenas a nível do dispositivo)
  - Gestão de activos (apenas a nível do dispositivo)
    - Informações sobre o dispositivo
    - Wi-Fi
    - Celular
    - Bluetooth
- Gestão da segurança
  - Antirroubo (apenas ao nível do dispositivo)
    - Informação GPS (apenas ao nível do dispositivo)
    - Limpa e bloqueia (apenas ao nível do dispositivo)
    - Mensagem (apenas a nível do aparelho)
  - Configuração de segurança
    - Código de acesso
    - Certificado (apenas a nível do dispositivo)
    - Encriptação
    - Início de sessão único
  - Fim de vida (apenas a nível do dispositivo)
    - Limpa (apenas ao nível do dispositivo)
  - Definições de restrições
    - Funcionalidade do dispositivo
    - iCloud
    - Segurança e privacidade
- BYOD
  - Segurança incorporada no iOS (contentor)
    - Ativação
    - Senha do SecurePIM

- Segurança do SecurePIM
- Navegador SecurePIM
- Troca

Gestão de ligações

- Wi-Fi
  - Configuração de proxy
  - Tipo de segurança
- VPN
  - Tipo de VPN
    - VPN
    - VPN por aplicação
  - Configuração de proxy
- APN
- Celular
- Proxy HTTP
- AirPrint
- AirPlay

Gestão PIM

- Exchange Active Sync
- eMail
  - Correio de entrada
  - Correio de saída
- CalDav
- Calendários subscritos
- LDAP

Gestão Web

- Webclips
- Filtro de conteúdo da Web

Gestão de aplicações

- Gestor de aplicações empresariais
  - Aplicações instaladas (apenas ao nível do dispositivo)
  - Aplicações obrigatórias
    - Opções de instalação
  - Aplicações Web

- Restrições e definições
  - Aplicações colocadas na lista negra / na lista branca
  - Restrições da SysApp
  - App-VPN
  - Definições da aplicação
- Loja de aplicações para empresas
  - Aplicações iTunes
  - Internamente
- Modo quiosque
  - Tipo de aplicação
    - Embalagem
    - URL
  - Definições do modo de quiosque

Android Enterprise – Configuração de dispositivos totalmente gerida

Geral

- Síntese do perfil do grupo (apenas a nível do grupo)
- Síntese do dispositivo (apenas ao nível do dispositivo)
- Config Revision (apenas a nível do dispositivo)
- Registo do dispositivo (apenas ao nível do dispositivo)
  - Registo de comandos
  - Status de comando possíveis
- Definições do dispositivo
  - Configuração do cliente
  - Papel de parede

Gestão de activos (apenas a nível do dispositivo)

- Informações sobre o dispositivo
  - Wi-Fi
- Celular
- Bluetooth

Gestão da segurança

- Antirroubo (apenas ao nível do dispositivo)
  - Informação GPS (apenas ao nível do dispositivo)
  - Limpa e bloqueia (apenas ao nível do dispositivo)

- Mensagem (apenas a nível do aparelho)
- Configuração de segurança
  - Código de acesso do dispositivo
  - AntiVírus
- Fim de vida (apenas a nível do dispositivo)
  - Limpa (apenas ao nível do dispositivo)
- Definições de restrições
  - Restrições
- Gestão de certificados

Gestão de ligações

- Wifi
  - Tipo de segurança
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Tipo de VPN
    - VPN
    - VPN por aplicação
- Restrições

Gestão PIM

- Gmail Exchange

Gestão de aplicações

- Gestor de aplicações empresariais
  - Aplicações instaladas (apenas ao nível do dispositivo)
  - Aplicações de sistema (apenas ao nível do dispositivo)
  - Aplicações obrigatórias
  - Lista negra e lista branca
  - Aplicações do sistema AE
- Restrições e definições
  - Definições de gestão de aplicações
- Loja de aplicações para empresas
  - Internamente
- Empresa Play Store
  - AE Play Store

- Modo de quiosque e lançador
  - Modo quiosque
  - Lançador AppTec360
  - Definições da AppTec360
- Controlo remoto
  - Splashtop
  - TeamViewer
- Gestão de conteúdos
  - ContentBox
  - Navegador seguro
- API adicional
  - Samsung KNOX
    - Restrições
    - Correio eletrónico
    - Troca
    - APN
    - Bluetooth
    - Ligação

Android Enterprise – Dispositivo totalmente gerido com perfil de trabalho (COPE)

- Explicação geral do COPE
- Configuração de perfis para dispositivos COPE
- Reverter para um dispositivo totalmente gerido pela AE

Android Enterprise – Configuração de contentores

- Geral
  - Síntese do perfil (apenas ao nível do perfil)
  - Síntese do perfil do grupo (apenas a nível do grupo)
  - Síntese do dispositivo (apenas ao nível do dispositivo)
  - Revisão da configuração
  - Registo do dispositivo (apenas ao nível do dispositivo)
    - Registo de comandos
    - Status de comando possíveis
  - Definições do dispositivo

- Configuração do cliente
- Papel de parede

Gestão de activos (apenas a nível do dispositivo)

- Informações sobre o dispositivo
  - Wi-Fi
- Celular
- Bluetooth

Gestão da segurança

- Antirroubo (apenas ao nível do dispositivo)
  - Informação GPS (apenas ao nível do dispositivo)
  - Limpa e bloqueia (apenas ao nível do dispositivo)
  - Mensagem (apenas a nível do aparelho)
- Configuração de segurança
  - Código de acesso do dispositivo
  - Código de acesso do contentor
  - AntiVírus
- Fim de vida (apenas a nível do dispositivo)
  - Limpa (apenas ao nível do dispositivo)
- Definições de restrições
  - Restrições
- Gestão de certificados

Gestão de ligações

- Wifi
  - Tipo de segurança
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Tipo de VPN
    - VPN
    - VPN por aplicação
- Restrições

Gestão PIM

- Gmail Exchange

Gestão de aplicações

- Gestor de aplicações empresariais
  - Aplicações instaladas (apenas ao nível do dispositivo)
  - Aplicações de sistema (apenas ao nível do dispositivo)
  - Aplicações obrigatórias
  - Aplicações do sistema AE
- Restrições e definições
  - Definições de gestão de aplicações
- Loja de aplicações para empresas
  - Internamente
- Empresa Play Store
  - AE Play Store

Gestão de conteúdos

- ContentBox
- Navegador seguro

Configuração do Android

Geral

- Síntese do perfil do grupo (apenas a nível do grupo)
  - Síntese do dispositivo (apenas ao nível do dispositivo)
- Config Revision (apenas a nível do dispositivo)
- Registo do dispositivo (apenas ao nível do dispositivo)
  - Registo de comandos
  - Status de comando possíveis
- Definições do dispositivo
  - Configuração do cliente
  - Papel de parede

Gestão de activos (apenas a nível do dispositivo)

- Gestão de activos
  - Informações sobre o dispositivo
  - Wi-Fi
  - Celular
  - Bluetooth

Gestão da segurança

- Antirroubo (apenas ao nível do dispositivo)
  - Informação GPS (apenas ao nível do dispositivo)

- Limpa e bloqueia (apenas ao nível do dispositivo)
- Mensagem (apenas a nível do aparelho)
- Configuração de segurança
  - Código de acesso
  - Encriptação
  - AntiVírus
- Fim de vida (apenas a nível do dispositivo)
  - Limpa (apenas ao nível do dispositivo)
- Definições de restrições
  - Restrições
  - Proprietário do dispositivo AE

Contentor BYOD

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - Aplicações do sistema AE
  - Código de acesso do contentor
- Samsung KNOX
  - Ativação
  - Código de acesso Knox
  - Segurança Knox
  - Bolsa de Valores de Knox
  - Knox eMail
  - Aplicações Knox

Gestão de ligações

- Wifi
  - Tipo de segurança
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Restrições
- APN
- Bluetooth

Gestão PIM

- Troca
- eMail
- AE Gmail Exchange

Gestão de aplicações

- Gestor de aplicações empresariais
  - Aplicações instaladas (apenas ao nível do dispositivo)
  - Aplicações de sistema (apenas ao nível do dispositivo)
  - Aplicações obrigatórias
  - Aplicações do sistema AE
- Restrições e definições
  - Lista negra e lista branca
  - Restrições da aplicação de sistema
    - Samsung Apps
    - Aplicações Huawei
  - Definições de gestão de aplicações
- Loja de aplicações para empresas
  - Playstore
  - Internamente
- Empresa Play Store
- Modo de quiosque e lançador
  - Modo quiosque
  - Lançador AppTec360
  - Definições da AppTec360

Controlo remoto

- Splashtop
- Teamviewer

Gestão de conteúdos

- Caixa de conteúdo
- Navegador seguro

Configuração do PC com Windows 10

Geral

- Síntese do perfil do grupo (apenas a nível do grupo)
- Síntese do dispositivo (apenas ao nível do dispositivo)
- Definições

- Config Revision (apenas a nível do dispositivo)
- Registo do dispositivo (apenas ao nível do dispositivo)
  - Registo de comandos
  - Status de comando possíveis
- Gestão de activos (apenas a nível do dispositivo)
  - Informações sobre o dispositivo
  - Celular
  - Informações de sincronização
- Gestão da segurança
  - Antirroubo (apenas ao nível do dispositivo)
    - Informação GPS (apenas ao nível do dispositivo)
    - Definições GPS
  - Configuração de segurança
    - Código de acesso
    - Antivírus
    - Centro de Segurança
    - Configuração da firewall
    - Regras de firewall
  - Definições de restrições
    - Funcionalidade do dispositivo
  - BitLocker
    - Configuração do BitLocker
    - Estado do BitLocker
  - Gestão de certificados
    - Lista de certificados
    - Configuração do certificado
    - SCEP
- Gestão de ligações
  - Wifi
    - Tipo de segurança
    - Utiliza o servidor proxy
  - Restrições de Wifi
  - VPN
    - Tipo de ligação
    - Configurações genéricas de VPN
  - Restrições VPN
  - Bluetooth

- Gestão PIM
  - Exchange Active Sync
  - eMail
- Gestão de aplicações
  - Gestor de aplicações empresariais
    - Aplicações instaladas
    - Aplicações obrigatórias
    - Restrições da aplicação de sistema
    - Lista negra e lista branca

Configuração do MacOS

Geral

- Síntese do perfil do grupo (apenas a nível do grupo)
- Síntese do dispositivo (apenas ao nível do dispositivo)
- Config Revision (apenas a nível do dispositivo)
- Registo do dispositivo (apenas ao nível do dispositivo)
  - Registo de comandos
  - Status de comando possíveis

Gestão de activos (apenas a nível do dispositivo)

- Informações sobre o dispositivo
- WiFi
- Celular
- Bluetooth

Gestão de actualizações (apenas ao nível do dispositivo)

- Atualizar informações

Gestão da segurança

- Antirroubo
  - Limpa e bloqueia
- Configuração de segurança
  - Código de acesso
  - Certificado
- Definições de restrições
  - Funcionalidade do dispositivo
  - iCloud
  - Gestão dos meios de comunicação social

- Gestão de ligações
  - Wi-Fi
    - Configuração de Wi-Fi empresarial
  - VPN
  - Proxy HTTP
  - AirPrint
  - AirPlay
- Gestão PIM
  - Exchange Active Sync
  - eMail
  - CalDav
  - CardDav
  - LDAP

Painel de controlo e relatórios

- Definições do painel de controlo
- Vista do painel de controlo
- Relatórios alargados
  - Relatórios de conformidade
    - Dispositivos enraizados
    - Dispositivos em roaming
    - Dispositivos habilitados para roaming
    - Dispositivos supervisionados
    - Dispositivos inactivos
  - Relatórios de dispositivos
    - Dispositivos por propriedade
    - Todos os dispositivos
    - Suportes de dispositivos
    - Dispositivos SAFE
    - Dispositivos Windows BitLocker
  - Relatórios de aplicações
    - Aplicações instaladas
    - Aplicações mais instaladas
    - Aplicações obrigatórias
    - Aplicações na lista negra

- Relatórios de utilizadores
  - Tarifa
- Gestão de multilocatários
  - Vistas adicionais
    - Lista todos os clientes
    - Datas de validade do APNS
- Contacto
  - Para questões técnicas gerais
  - Para questões relacionadas com a instalação de um aparelho virtual
- Isenção de responsabilidade

Visão geral

Introdução ao AppTec360

A solução Enterprise-Mobile-Management da AppTec oferece a opção de gerir e configurar todos os dispositivos móveis com a sua consola de gestão intuitiva. Neste cenário, o servidor EMM pode ser executado no teu próprio ambiente ou podes utilizar a nossa solução baseada na nuvem.

Mesmo no que diz respeito à instalação centralizada de aplicações empresariais nos smartphones, vieste ao sítio certo. Com o Enterprise Mobile Manager, podes distribuir aplicações e documentos empresariais para dispositivos em segundos ou bloquear aplicações indesejáveis com listas brancas/negras.

A utilização de dispositivos privados nas empresas representa um novo desafio para a proteção de smartphones e tablets. Devido ao facto de os funcionários quererem utilizar cada vez mais os seus smartphones, os administradores de TI têm de proteger um grande número de diferentes tipos de dispositivos. Ajudamos-te a proteger todos os dispositivos e os dados sensíveis neles armazenados e a geri-los a partir de uma consola intuitiva.

Sistemas operativos de dispositivos suportados

A AppTec360 oferece suporte para dispositivos iOS, Android e Windows. Tem em atenção que a capacidade das funções das plataformas mencionadas pode ser diferente de um sistema operativo para outro.

- Apple iOS 11.0 ou superior*
- Apple macOS 10.11 ou superior
- Google Android 4.4 ou superior** na versão Cloud
- Google Android 4.1 ou superior** na versão OnPrem
- MS Windows 10 ou superior*** (computador de secretária, computador portátil e tablet)

**Tem em atenção que os dispositivos com iOS 10 ou anterior não podem ser registados devido a alterações drásticas feitas pela Apple no processo de registo.*

***Os dispositivos podem ser ligados e configurados mesmo que utilizem uma versão que já não é suportada pelo fabricante. Tem em atenção que pode haver funcionalidades que exijam uma determinada versão do Android. Nos casos de apoio, seguimos o apoio oficial do fabricante. No caso de problemas ou erros causados por uma versão desactualizada que já não seja suportada pelo fabricante, reservamo-nos o direito de oferecer apenas um apoio limitado.*

****A versão doméstica do Windows não é suportada devido a limitações do sistema operativo. Recomendamos vivamente que utilizes uma versão do sistema operativo que ainda seja suportada pelo fabricante. Não só por uma questão de compatibilidade, mas também por razões de segurança. Por isso, recomendamos o iOS 12 ou superior e o Android 9 ou superior.*

Directórios LDAP suportados

- Microsoft Active Directory
- Abre o LDAP

Informações actualizadas sobre "Sistemas operativos de dispositivos suportados" e "Directórios LDAP suportados" podem ser encontradas aqui:

https://www.apptec360.com/products/systemrequirements/

Explicação do “Modo Supervisionado” nos dispositivos Apple

O Modo Supervisionado representa uma interface alargada para dispositivos iOS.

No dispositivo respetivamente configurado, podem ser aplicadas limitações adicionais, no que diz respeito à funcionalidade do dispositivo do utilizador final. Estas constam igualmente do manual de administração e estão assinaladas com uma faixa.

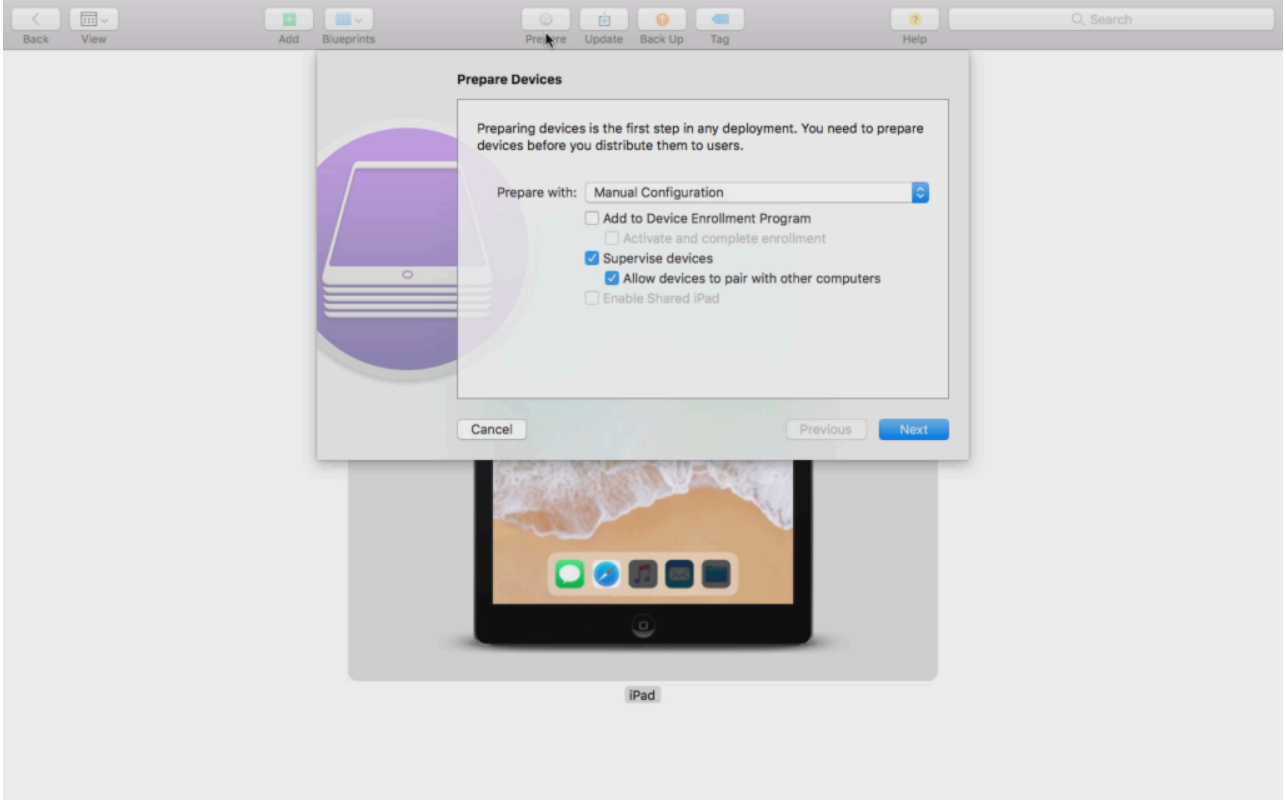
Disponível no modo supervisionado

O "Supervised-Mode" pode ser ativado com o programa "Apple Configurator". O Apple Configurator pode definir as predefinições em novos dispositivos iOS como uma ferramenta de configuração (através da interface USB).

A ferramenta pode instalar não só perfis de configuração, mas também aplicações. É gratuito, mas requer um computador Mac.

Ativar o modo supervisionado

1. Abre o Apple Configurator



2. Clica no dispositivo e escolhe "Preparar"
3. Escolhe "Configuração manual" e "Supervisionar dispositivos"
4. Clica em "Seguinte"
5. (Opcional) Agora podes adicionar um servidor MDM onde o dispositivo será registado. A ligação para isto pode ser encontrada em "Definições gerais - Configuração do iOS - Configurador e URL" Escolhe a tua Organização ou cria uma nova
6. Escolhe a tua Organização ou cria uma nova
7. Escolhe os passos que devem ser ignorados na configuração inicial e clica em "Seguinte" (CUIDADO: Se continuares, o teu dispositivo será eliminado!)

Agora o teu dispositivo será colocado no modo supervisionado. Isto pode demorar alguns minutos. Depois de o fazeres, o dispositivo é reiniciado.

Agora o teu dispositivo é supervisionado!

Adiciona um dispositivo à DEP

Também podes adicionar dispositivos ao DEP (Device Enrollment Programm) utilizando o Apple Configurator, se os teus dispositivos estiverem no iOS 11 ou superior.

Mais informações sobre o DEP: https://www.apple.com/business/dep/

Segue os mesmos passos que seguirias para supervisionar um dispositivo e assinala adicionalmente "Adicionar ao programa de registo de dispositivos". Ser-te-ão solicitados os teus dados de início de sessão DEP se nunca tiveres iniciado sessão no DEP com o Apple Configurator.

Depois de o processo estar concluído, o dispositivo pode ser encontrado no servidor DEP "Devices Added by Apple Configurator 2". Podes agora utilizar este servidor e ligá-lo à consola de gestão ou transferir o dispositivo para um servidor já existente.

Adicionaste com êxito um dispositivo à DEP!

Explicação sobre o Android Enterprise

O que é o Android Enterprise?

O Android Enterprise oferece um melhor controlo dos dispositivos de trabalho que são geridos com um MDM. Isto permite aos administradores ter controlo total sobre os seus dispositivos Android ou separar os dados da empresa dos dados privados nos dispositivos contentores. Além disso, o Android Enterprise permite um registo mais fácil dos dispositivos e uma distribuição fácil das aplicações.

Quais são os requisitos para utilizar o Android Enterprise?

O Android Enterprise pode ser utilizado gratuitamente por todos. Só precisas de ligar uma conta Google à MDM para ativar todas as funcionalidades do Android Enterprise. Podes encontrar mais informações sobre este assunto na secção Android Enterprise.

O Android Enterprise pode ser utilizado em dispositivos com Android 5.1 ou superior, com exceção do perfil de trabalho melhorado (ver abaixo). Recomendamos que utilizes pelo menos o Android 7 ou superior para uma inscrição mais fácil ou o Android 11 para utilizares todas as funcionalidades disponíveis.

Quais são os modos disponíveis no Android Enterprise?

Existem 3 modos diferentes para utilizares quando usas o Android Enterprise.

Dispositivo totalmente gerido pela AE (gerido pelo trabalho): Um dispositivo totalmente gerido que é utilizado apenas para trabalho. Isto permite que o administrador tenha controlo total sobre o dispositivo. Isto não permite uma utilização privada do dispositivo. Para registar dispositivos neste modo, os dispositivos têm de ser reiniciados e registados com um Código QR (ver Registo AE) ou registados através do Registo Knox ou do Zero Touch.

Contentor AE BYOD: O contentor BYOD (bring your own device) permite que os utilizadores acedam aos dados da empresa no seu telemóvel privado num contentor separado. Neste modo, as aplicações privadas não podem ver os dados e as aplicações da empresa e vice-versa. Para registar dispositivos neste modo, a aplicação AppTec tem de ser descarregada e pode ser lido um código QR. Cria um dispositivo na consola e selecciona "AE Container (BYOD & Enahnced Work Profile)" como tipo de dispositivo. Clica no código QR do dispositivo recém-gerado para obteres o código QR e define o primeiro interrutor para "Legacy & BYOD".

AE Enhanced Work Profile: (requer Android 11 ou superior) Enquanto o BYOD Container acima mencionado coloca os dados da empresa num dispositivo privado, o Enhanced Work Profile faz o mesmo, mas num dispositivo da empresa. Cria o mesmo contentor, mas dá ao administrador um pouco mais de controlo sobre o dispositivo, pelo que o utilizador não pode simplesmente remover a

MDM do dispositivo. Cria um dispositivo na consola e selecciona "AE Container (BYOD & Enahnced Work Profile)" como tipo de dispositivo. Clica no código QR do dispositivo recém-gerado para obteres o código QR e define o primeiro interrutor para "Enhanced Work Profile" (perfil de trabalho melhorado). Este código QR pode ser digitalizado depois de reiniciares o dispositivo e tocares 6 vezes no ecrã, tal como explicado no Método 1 em Inscrição AE.

Como posso atribuir aplicações a dispositivos Android Enterprise?

Primeiro, tens de aprovar as aplicações que queres utilizar em Definições gerais → Gestão de aplicações → AE Play Store → Aplicações da Play Store. Depois de aprovares uma aplicação, podes atribuí-la à lista de aplicações obrigatórias → do teu perfil, clicando no "+" e seleccionando a aplicação no separador "AE Play Store". Isto irá transferir e instalar a aplicação automaticamente. Não é necessária uma conta Google no dispositivo e o utilizador não tem de confirmar ou autorizar.

Carrega as tuas próprias aplicações para a Google Play Store

É possível carregar as tuas aplicações internas na Google Play Store. Desta forma, podes beneficiar de diferentes vantagens, como o mecanismo de atualização da Play Store.

Para o fazeres, precisas de uma Conta de Programador Google. Inicia sessão utilizando a Consola do Google Play(https://play.google.com/apps/publish)

Clica em "Criar aplicação". Escolhe o teu idioma predefinido e o título da aplicação.

Create application

Default language *

English (United Kingdom) – en-GB ▾

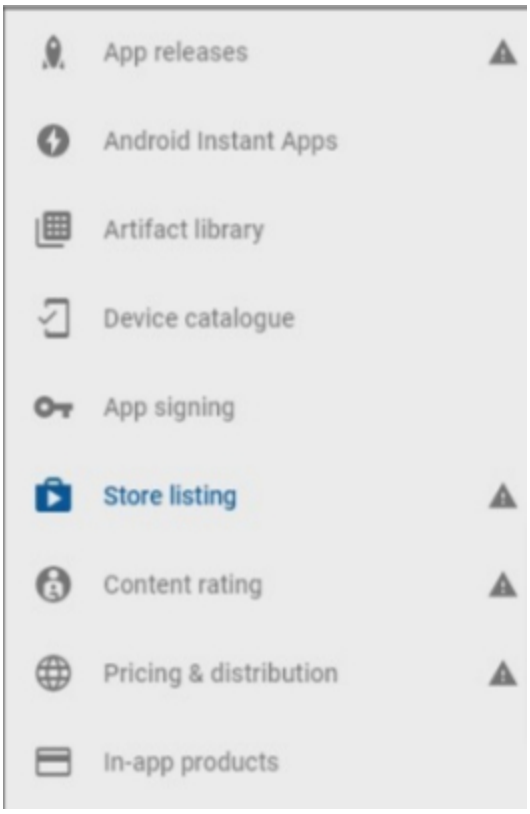
Title *

AppTec Demo App

15/50

CANCEL CREATE

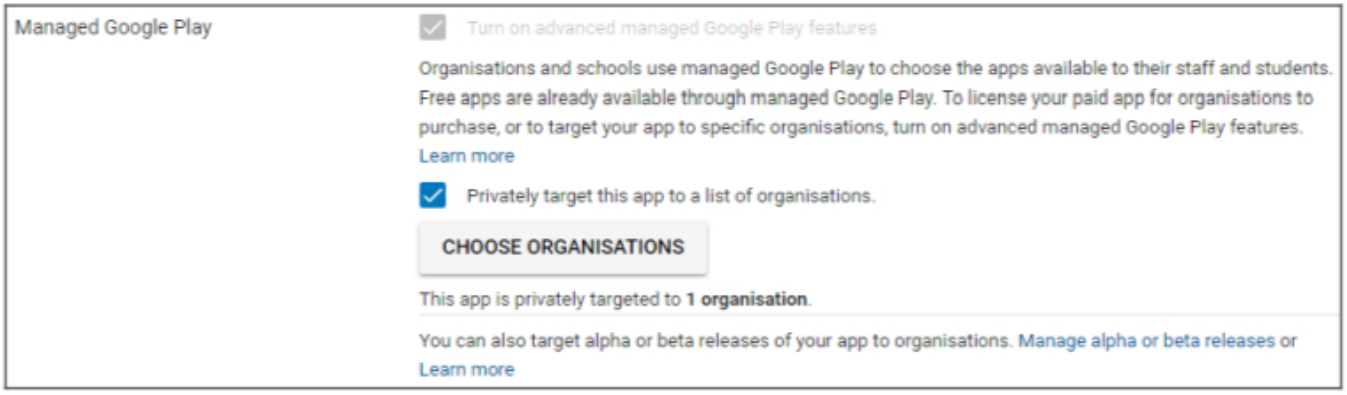
Na página seguinte, ser-te-á pedido que introduzas diferentes detalhes sobre a tua aplicação.



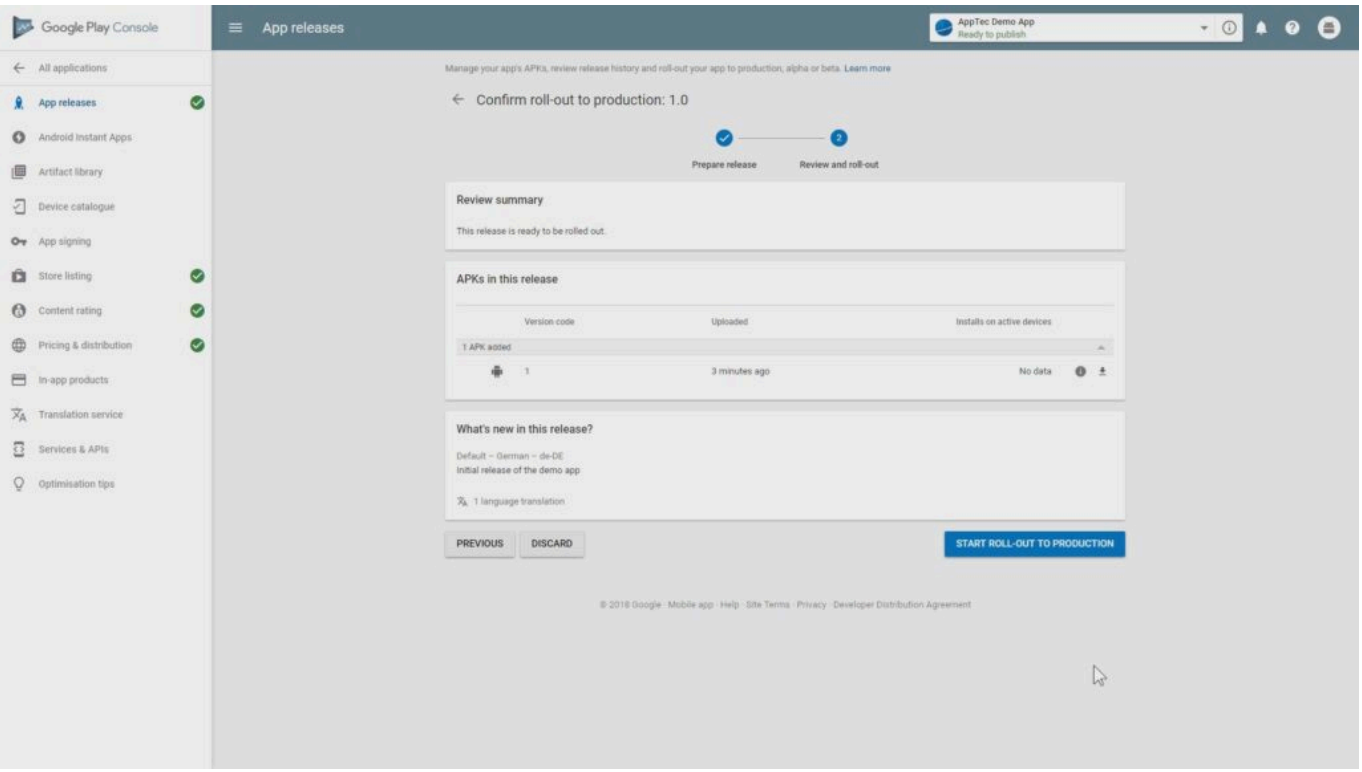
Depois de introduzires todos os detalhes, verás diferentes símbolos de dicas no lado esquerdo.

Passa por cima delas para veres quais os passos que faltam e segue-os pela ordem que quiseres.

Nota: Certifica-te de que assinalas as duas caixas de verificação em "Gerido pelo Google Play" em "Preços e distribuição". Caso contrário, a aplicação será pública e poderá ser acedida por todos. Certifica-te também de que escolhes o país de distribuição.



Depois de concluíres todos os passos, podes ir para "Lançamentos de aplicações". Clica em "Rever" e "Iniciar lançamento para produção" para finalizar o teu projeto e publicar a aplicação.



Pode demorar algum tempo até que a aplicação esteja disponível na Play Store. Quando o processo estiver concluído, podes procurar a tua aplicação na loja Play for Work e aprová-la. Depois disso, podes simplesmente atribuir a aplicação a dispositivos utilizando a consola EMM, tal como fazes com outras aplicações.

Requisitos e instalação

Requisitos

Requisitos do sistema

A aplicação virtual está disponível no formato de virtualização aberta (VMWare, VirtualBox, Citrix Xen Server) e como ficheiro .vhdx (Hyper-V) comprimido*.

*Nota: A máquina tem de ser criada com a Geração 1 quando utilizas o Hyper-V.

O disco virtual tem um tamanho alvo de 20 GB e a máquina requer 4 GB de RAM.

A aplicação é baseada em Debian 9 64bit

Actualiza a máquina importada para a compatibilidade mais recente (por exemplo, no VMWare) e certifica-te de que o tipo de SO da máquina está definido corretamente no teu hipervisor.

Chave de licença

Para ativar e instalar o servidor com êxito, precisas de um ficheiro de licença válido. Podes obter um da AppTec360 diretamente e/ou do teu respetivo revendedor.

Endereço IP e resolução DNS

O aparelho AppTec360 tem de ser acessível pelo dispositivo utilizando o nome de anfitrião para o qual a licença foi emitida.

Para registar dispositivos Windows 10, também tens de configurar um subdomínio adicional sob a forma de "enterpriseenrollment.", apontando para o dispositivo.

Certificado SSL

Como todas as ligações de e para os dispositivos têm de ser protegidas com SSL, precisas de um certificado válido para o nome do anfitrião emitido por uma Autoridade de Certificação em que o dispositivo confie. A chave privada do certificado tem de ser carregada sem proteção por palavra-passe. Na maioria dos casos, é necessário um certificado intermédio para a CA para que os dispositivos reconheçam o certificado do servidor.

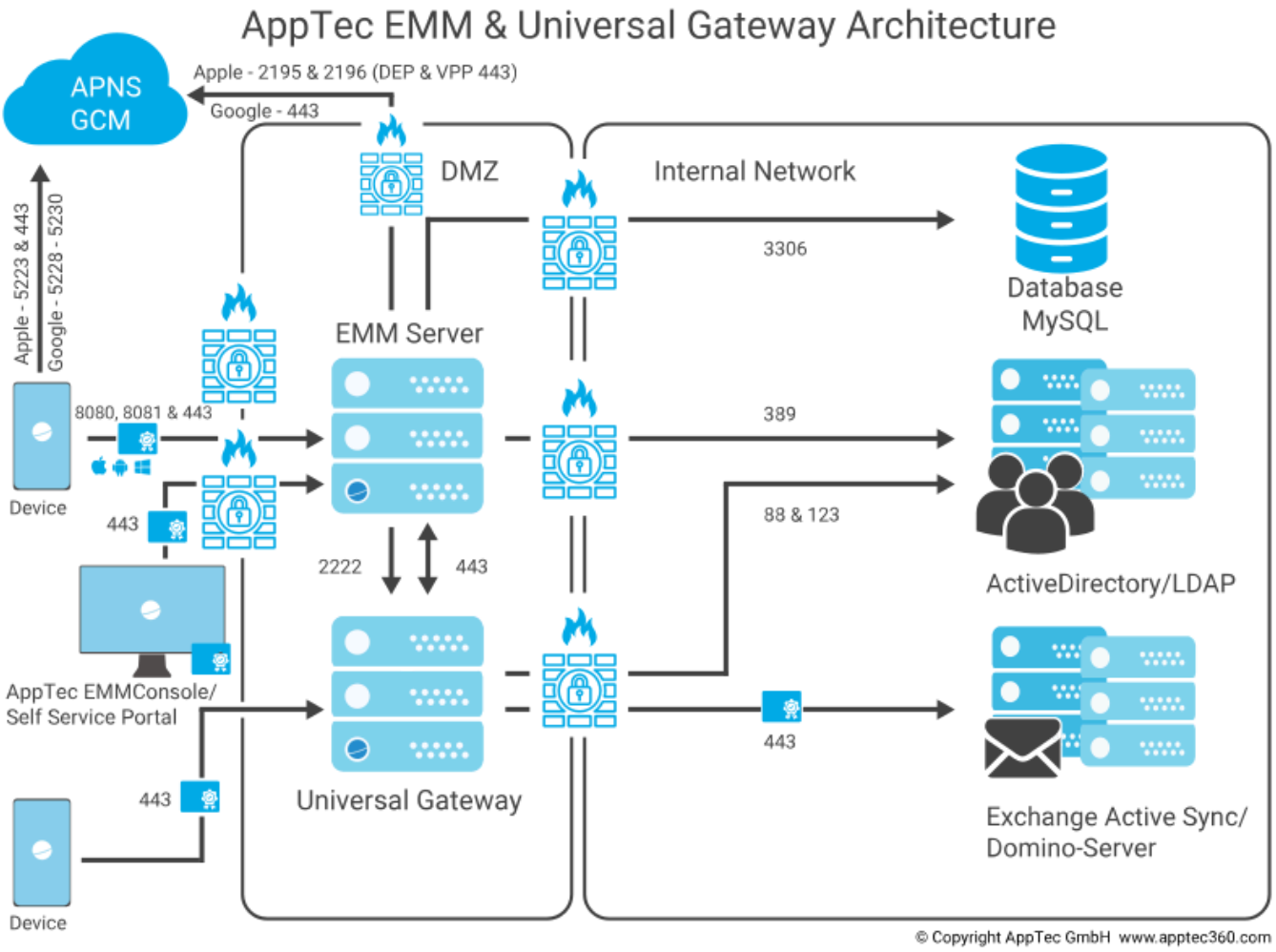
Os dispositivos Windows 10 irão requerer um certificado específico para o teu subdomínio de registo empresarial.

A partir da versão 202104 do aparelho, também podes utilizar os certificados Let's Encrypt, que são gerados automaticamente (descrito no Passo 2 - Certificado SSL).

Servidor SMTP

É necessário um servidor de correio eletrónico e/ou um relé de correio eletrónico, para permitir que o AppTec360 EMM envie mensagens de correio eletrónico (por exemplo, para registo de dispositivos e validação de contas).

Regras de firewall



Este diagrama mostra qual a ligação necessária em função dos serviços que pretendes utilizar.

Para uma descrição mais pormenorizada, consulta o quadro da página seguinte.

Qualquer (externo/dispositivos)	→	**AppTec360 Appliance / emmconsole.com**
Portos	443	Gestão, Enterprise AppStore e Comunicação com o Windows Phone
	8080	Comunicação Android e iOS
	80	Configura pela primeira vez o Let's Encrypt. Usa o 443 depois.
Qualquer (Dispositivos)	→	**Qualquer (externo)**
Portos	5223, 443	Apple Push Service, tem de ser contactável sem proxy, 443 como Fallback, ver https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), tem de ser acessível sem proxy
Aparelho AppTec360	→	**Controlador de domínio**
Portos	389, (LDAPS 636)	Sincronização de utilizadores com LDAP
Aparelho AppTec360	→	**Qualquer um**
Porto	443	Utilizado para o serviço Push do Android (GCM) Pesquisa na AppStore / Play Store
Aparelho AppTec360	→	**emmconsole.com**
Portos	443	Actualizações da AppTec360 Appliance, geração de certificados APNS
Aparelho AppTec360	→	**Rede Apple (17.0.0.0/8)**
Portos	2195, 2196	Serviço Push da Apple e Serviço de Feedback
	443	DEP E VPP

Actualizações de segurança

O sistema operativo Debian deve ser atualizado regularmente para obter as mais recentes correcções de segurança. No entanto certifica-te que não actualizas manualmente para uma nova versão principal de Debian. Quando o AppTec360 EMM for compatível com uma versão principal mais recente, adicionaremos uma forma de atualização numa atualização da aplicação.

Senhas padrão do dispositivo virtual

Utilizador de início de sessão (o início de sessão Root está desativado. Utiliza "sudo" para tarefas de administração)

apptec

Palavra-passe de acesso

apptec

Utilizador raiz do MySQL

raiz

Senha da raiz do MySQL

apptec

Utilizador predefinido do MySQL

AppTec

Palavra-passe de utilizador predefinida do MySQL

AppTec

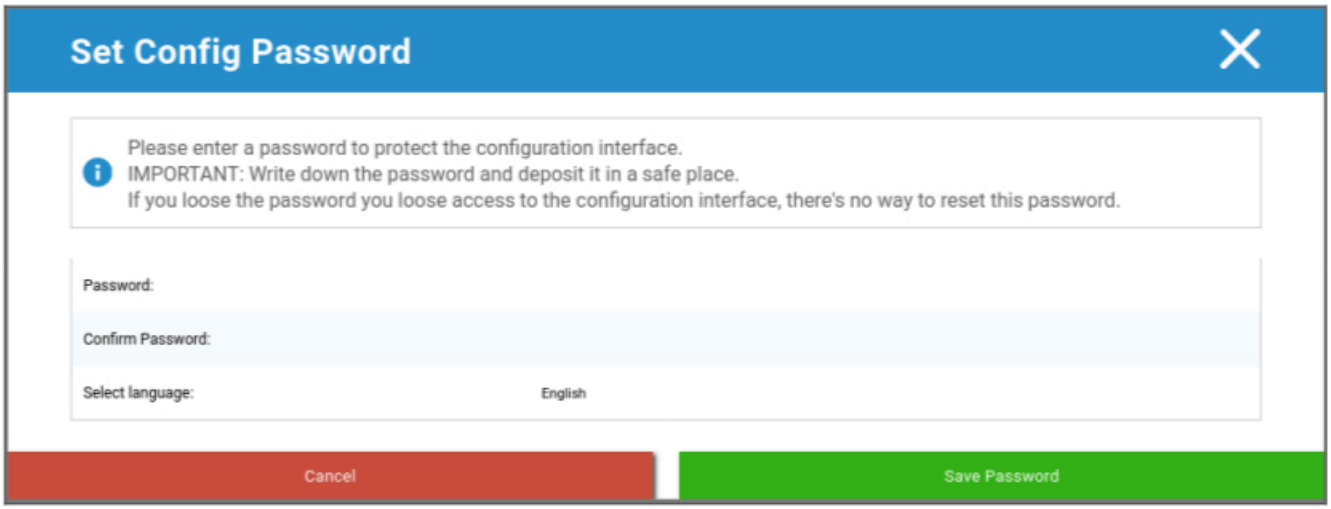
Configuração do aparelho virtual

Importante: Antes de começares a configurar o Aparelho Virtual, a resolução do ecrã deve ser definida para, pelo menos, 1280 x 800 pixels.

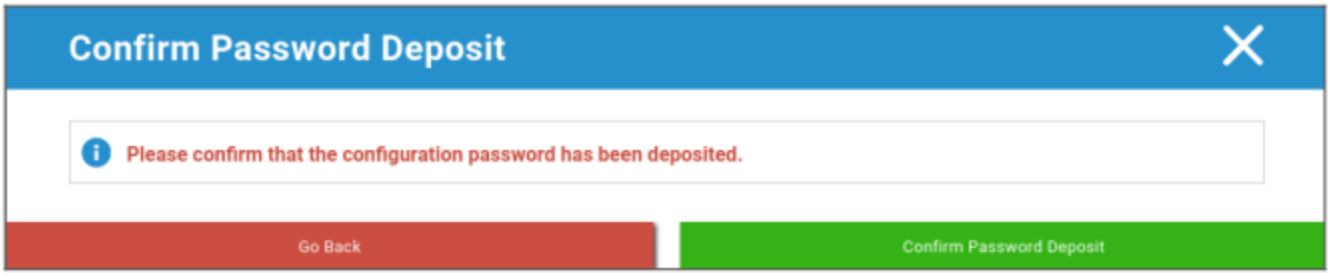
Depois de te ligares à Appliance, o Firefox deve iniciar-se automaticamente e mostrar a interface de configuração.

Preparação

Primeiro, tens de fornecer uma palavra-passe para a interface de configuração. Esta palavra-passe é utilizada para encriptar todas as informações e ficheiros introduzidos na interface de configuração. Aqui também podes definir o idioma em que a interface deve ser apresentada (pode ser alterado mais tarde).

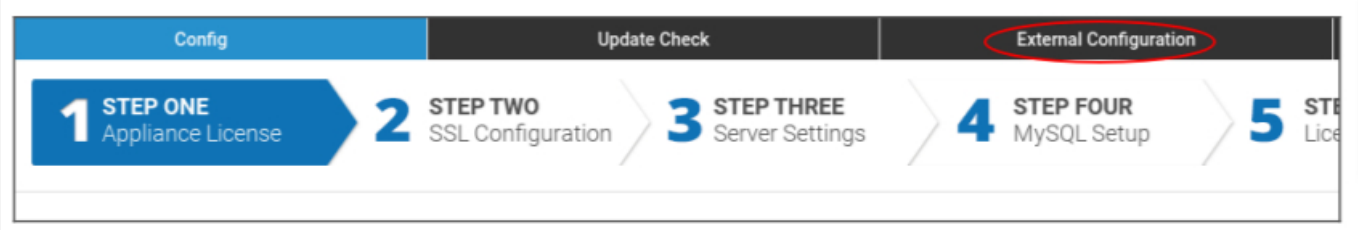


A palavra-passe só pode ser redefinida pelo Suporte da AppTec360, por isso certifica-te de que a depositas num local seguro e confirma o pop-up que vai surgir.



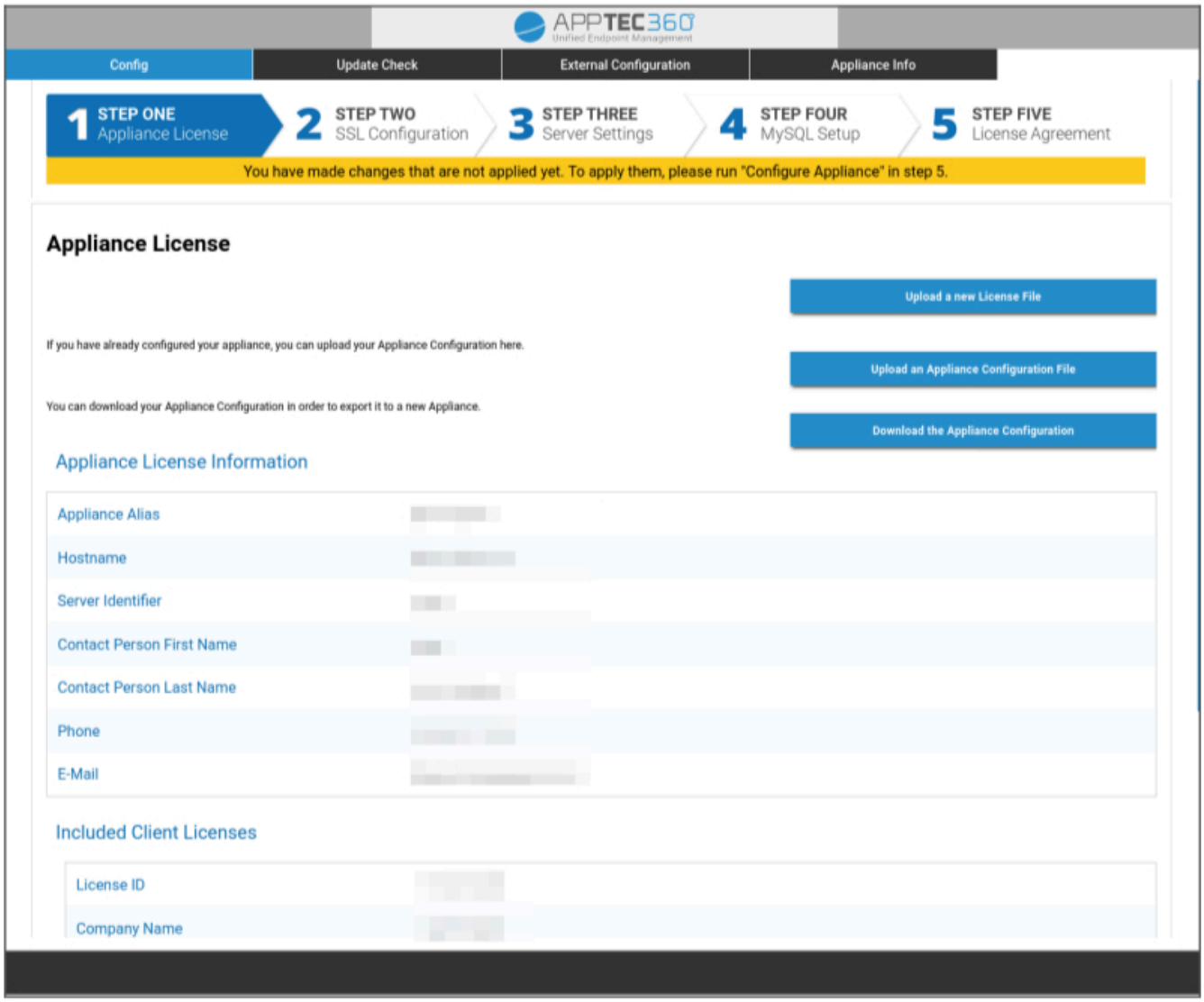
Configura a partir de um anfitrião externo

Para facilitar o processo de configuração, podes tornar a página de configuração acessível a partir do controlo remoto. Para o fazer, segue os passos em "Configurar a partir de um anfitrião externo".



Primeiro passo – Licença do aparelho

1. Carrega o ficheiro de licença que recebeste da AppTec.
2. Se o ficheiro de licença tiver sido carregado com sucesso, podes ver as informações da licença do aparelho como na imagem abaixo.



Segundo passo – Certificado SSL

Podes utilizar a configuração automática de certificados utilizando o Let's Encrypt ou fornecer os certificados tu mesmo (ver SSL-Certificate para mais informações).

Automático

O certificado será gerado automaticamente utilizando o serviço Let's Encrypt.

O AppTec360 EMM utiliza o desafio HTTP-01 para validação do domínio, o que significa que a porta HTTP tem de estar aberta a partir da Internet para o primeiro pedido de um certificado. Os pedidos de renovação subsequentes podem ser validados através de HTTPS.

Muda os botões de rádio para "Automático (Let's Encrypt)" e prime "GUARDAR VALORES". O certificado será automaticamente solicitado quando aplicares a configuração no Passo Cinco - Contrato de Licença. O certificado será renovado automaticamente, se necessário, e receberás um e-mail se o certificado estiver prestes a expirar (o que implica que a renovação pode ter falhado).

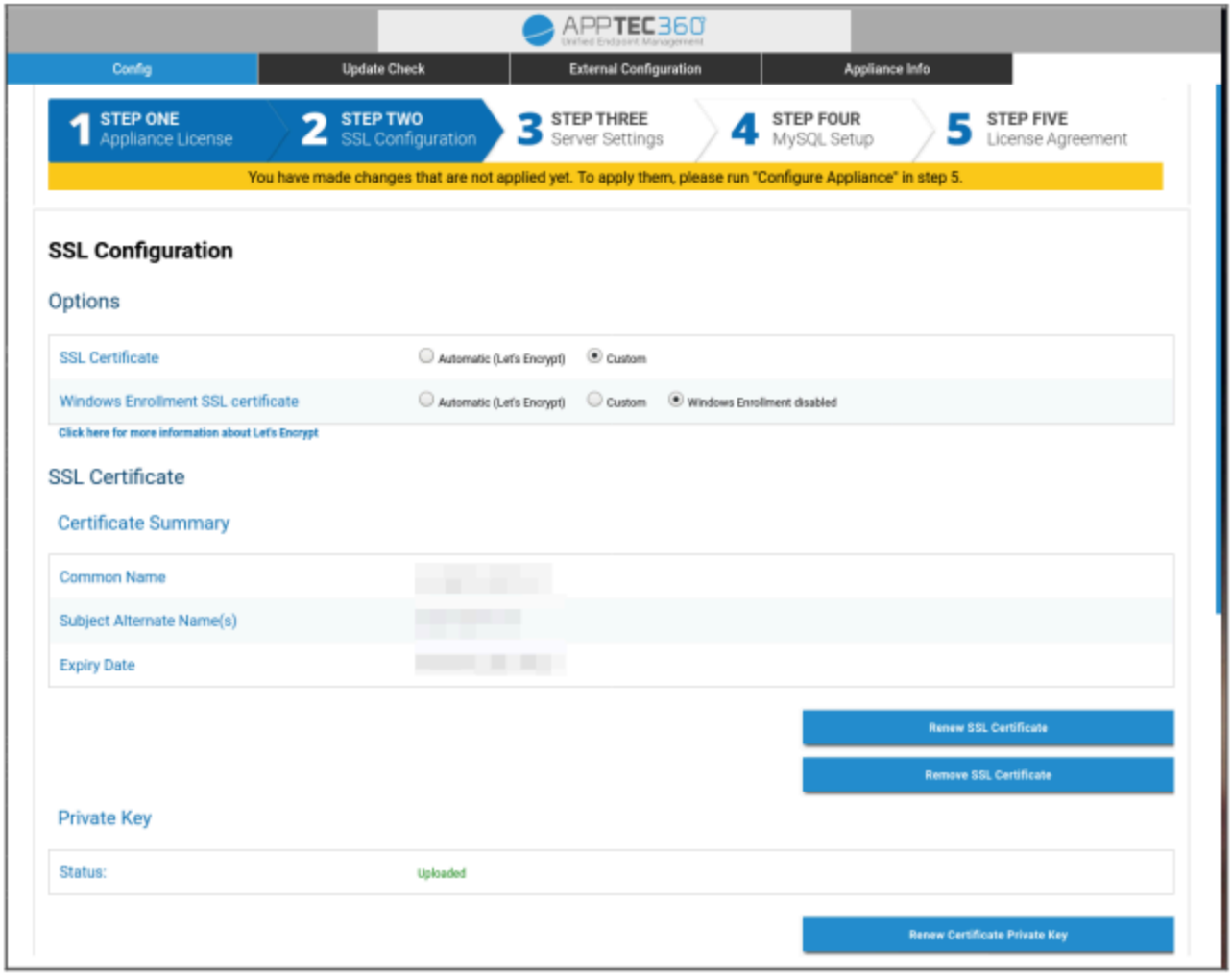
Personalizado

1. Carrega o certificado SSL para o teu nome de anfitrião licenciado. Podes ver o nome do anfitrião no Passo Um - Licença do aparelho.

2. Carrega também a chave privada do certificado e, se necessário, o certificado intermédio.

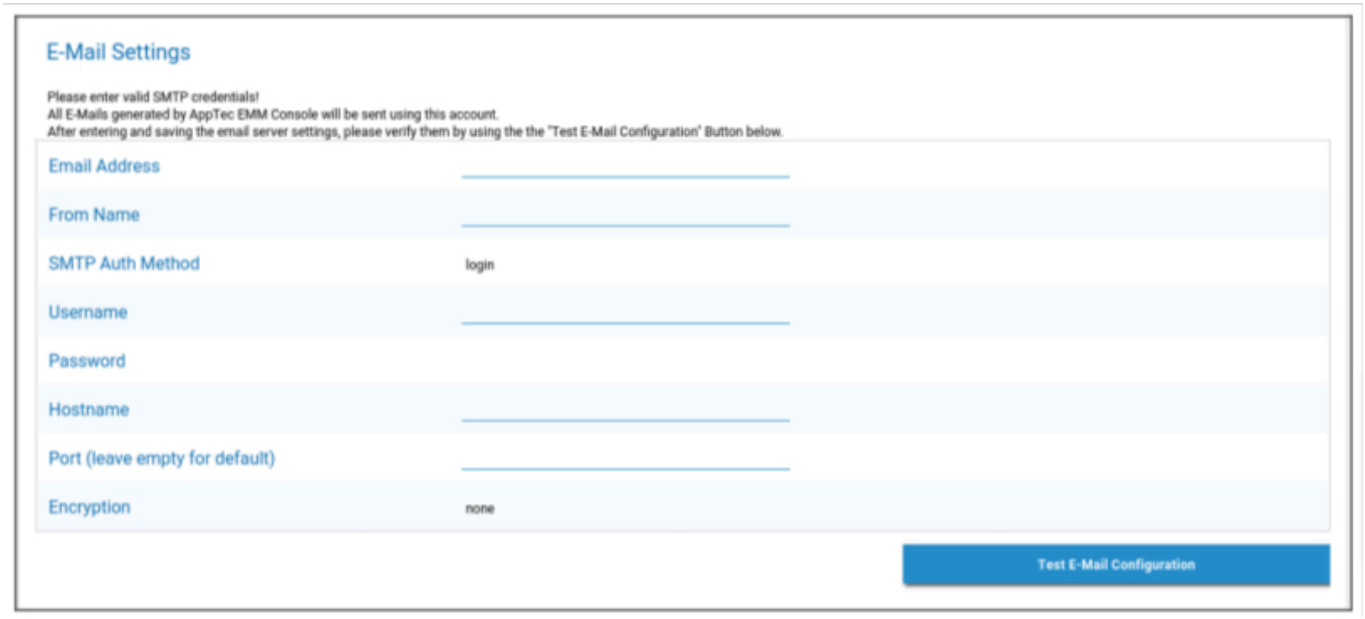
Importante: A chave não deve ser protegida por palavra-passe. Se for o caso, remove a palavra-passe antes de fazeres o upload.

Dica: Se também quiseres utilizar dispositivos Windows 10, tens de ativar "Certificado SSL de inscrição no Windows" e carregar o certificado, a chave privada e o certificado intermédio para o teu subdomínio (descrito em Endereço IP e Resolução DNS) no final da página.



Terceiro passo – Definições do servidor

1. Introduz um endereço de correio eletrónico de apoio global. Este endereço será utilizado nas mensagens de correio eletrónico enviadas aos teus utilizadores para que saibam quem contactar em caso de problemas com o seu dispositivo.
2. Fornece as definições de correio eletrónico que serão utilizadas pelo sistema para enviar mensagens de correio eletrónico. As definições serão utilizadas para enviar mensagens de correio eletrónico ao utilizador e também para enviar relatórios de erros e pedidos de funcionalidades para"support@apptec360.com". Depois de guardares as tuas definições de e-mail, tens de as verificar clicando em "Testar configuração de e-mail" e seguindo as instruções.



Quarto passo – Configuração do MySQL

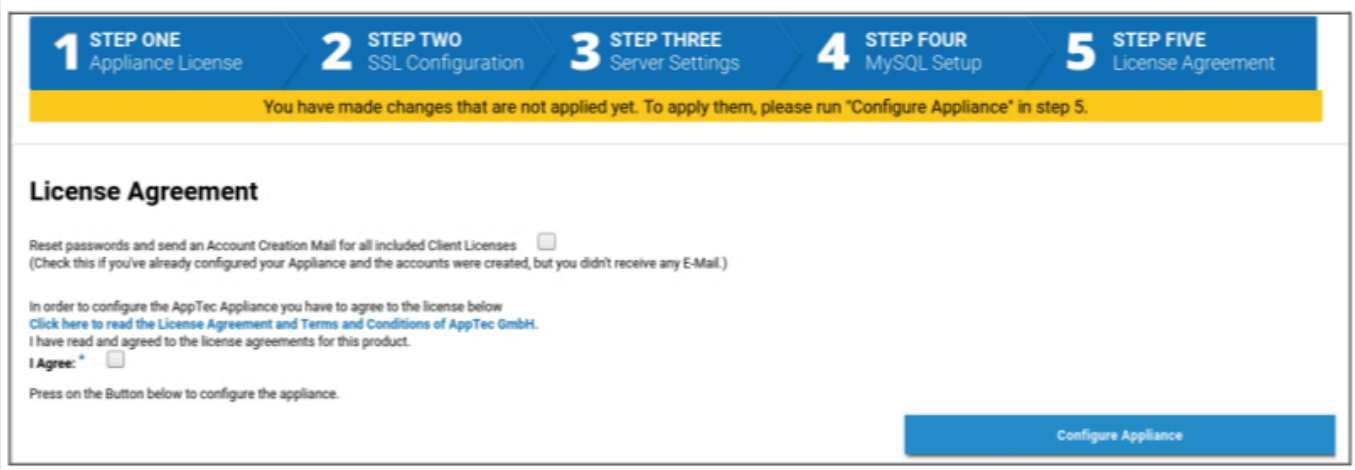
1. Se quiseres utilizar a base de dados interna, podes saltar este passo. Caso contrário, podes introduzir as informações de ligação para o teu servidor de base de dados externo.


1 STEP ONE
Appliance License
2 STEP TWO
SSL Configuration
3 STEP THREE
Server Settings
4 STEP FOUR
MySQL Setup
5 STEP FIVE
License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

Quinto passo – Contrato de licença

1. Não deixes de ler o contrato de licença.
2. Assinala "Concordo" e prime o botão "Configurar aparelho", para aplicar as definições.

Dica: Terás de executar "Configurar aparelho" sempre que alterares as definições nos 5 passos para aplicar as definições.



Parabéns!

Concluiu a configuração do dispositivo virtual.

Foi enviado um e-mail com a tua palavra-passe para o endereço que forneceste para a licença (visível em "Licenças de Cliente Incluídas" no Passo Um - Licença do Aparelho).

Agora podes entrar na consola utilizando esta palavra-passe e o endereço de e-mail que recebeste.

Para entrar na consola, introduz o nome do anfitrião da consola na barra de endereços do teu browser.

Podes encontrar o nome do anfitrião do teu aparelho no Passo Um - Licença do aparelho.

Resolução de problemas

1. Não recebeste um e-mail quando configuraste o aparelho no Passo Cinco - Contrato de Licença:

Certifica-te de que as definições de correio eletrónico no Passo Três - Definições do servidor estão correctas. Para reenviar a senha, marca a opção "Redefinir senhas e enviar um e-mail de criação de conta para todas as licenças de cliente incluídas" na Etapa Cinco - Contrato de Licença antes de executar "Configurar Aparelho" novamente.

2. Recebeste um erro em relação ao Let's Encrypt durante a configuração no Passo Cinco - Contrato de Licença:

Certifica-se de que o aparelho pode ser alcançado pelo seu nome de domínio na porta 80. Let's encrypt também escreve um log em "/var/log/letsencrypt" que pode ajudar na resolução de problemas.

Recomendações de segurança

Recomenda-se a execução dos seguintes passos para proteger a tua aplicação AppTec360.

Este não é um conjunto completo de instruções, é apenas uma recomendação para uma configuração básica.

- Altera a palavra-passe do utilizador da AppTec360
- Altera a palavra-passe dos utilizadores MySQL "root" e "AppTec" e actualiza o Passo Quatro - Configuração do MySQL em conformidade
- Altera a porta predefinida do servidor SSH
- Bloqueia a porta 80 na tua consola e não permite o tráfego HTTP de entrada, utiliza apenas HTTPS. Uma vez configurado, também é possível uma configuração externa através de HTTPS.
- Restringe o acesso à interface de gestão apenas a determinados Ips na parte inferior do Passo Três - Definições do Servidor
- Configura a firewall

Definições gerais

Visão geral da conta

Informações sobre a conta

Visão geral

Aqui, podes ver uma visão geral da tua conta AppTec360.

Nome da empresa	O nome da tua empresa
Data de criação	Data de criação da tua conta
Tipo de licença	Pago = licença paga Livre = licença não paga Nota: Por razões técnicas, as contas de um aparelho OnPremise serão sempre apresentadas como pagas
Identificador de cliente	Identificador da tua conta (NÃO é o teu número de cliente)
Data de expiração da licença	Data de expiração da tua licença AppTec360
Licença ContentBox	Free = licença gratuita para 25 dispositivos Pago = licença paga para x dispositivos
Lançador	Mostra se podes ou não utilizar o lançador personalizado para Android
Dispositivos	Número de licenças atualmente utilizadas / total de licenças
Pessoa de contacto	Pessoa de contacto fornecida
Telefone	Número de telefone fornecido
eMail*	Endereço de correio eletrónico fornecido
Utilizador raiz	Utilizadores raiz que podem iniciar sessão
Versão do software	Versão atual do software

**Nota: O endereço de e-mail apresentado aqui é o que introduziste para registar a Conta. Com base nisto, será criado um utilizador na árvore de utilizadores/dispositivos, que pode ser modificado. A edição deste utilizador irá alterar o endereço de e-mail que tens de utilizar para iniciar sessão, mas não as informações na visão geral da conta*.

Relatório de erros

Um relatório de erros pode ser enviado diretamente para o suporte para comunicar problemas ou erros e inclui informações e registos sobre a tua conta e configuração.

Assunto	O assunto do relatório de bug. Inclui um número de ticket se quiseres adicionar isto a um ticket de suporte existente.
Comportamento esperado	Descreve em pormenor o que fizeste e o que esperavas que acontecesse
Comportamento real	Descreve em pormenor o que aconteceu exatamente. Por favor, cita EXACTAMENTE as mensagens de erro. Também ajuda se acrescentares capturas de ecrã ao anexo.
Em que altura tiveste o problema?	Por favor, indica a hora exacta em que recebeste uma mensagem de erro/problema específico. Na melhor das hipóteses, inclui também os segundos, por exemplo, 18:55:27
O problema pode ser reproduzido? Em caso afirmativo, como (em pormenor)?	Descreve detalhadamente como podes reproduzir o problema.
Esta funcionalidade já funcionou como esperavas? Em caso afirmativo, até quando?	Deixa em branco se não souberes.
Fizeste alguma alteração específica ao sistema antes do aparecimento deste problema? Em caso afirmativo, que alterações (em pormenor)?	Refere sempre qual foi a tua última alteração ou ação antes do aparecimento da questão, mesmo que a consideres irrelevante.
Se aplicável: Que modelos de dispositivos e versões de SO são afectados?	Indica sempre a versão exacta do sistema operativo (por exemplo, iOS 14.7.1 ou Android 11)
Se aplicável: Qual é o endereço IP público e/ou o número de série do dispositivo?	Nomeia pelo menos um, mesmo que todos os dispositivos sejam afectados.
Inclui ficheiros de registo	Marca esta opção para enviar o ficheiro de registo com o relatório de erro. Recomenda-se que o faças.
Obtém o estado atual do VPP da Apple e inclui no relatório de erros	Inclui informações sobre atribuições de licenças VPP. Só ativa esta opção se o suporte te pedir para o fazeres ou se o teu problema estiver relacionado com o VPP.

Anexo	Anexa qualquer ficheiro que possa ser útil (por exemplo, capturas de ecrã de uma mensagem de erro)

Pedido de funcionalidades

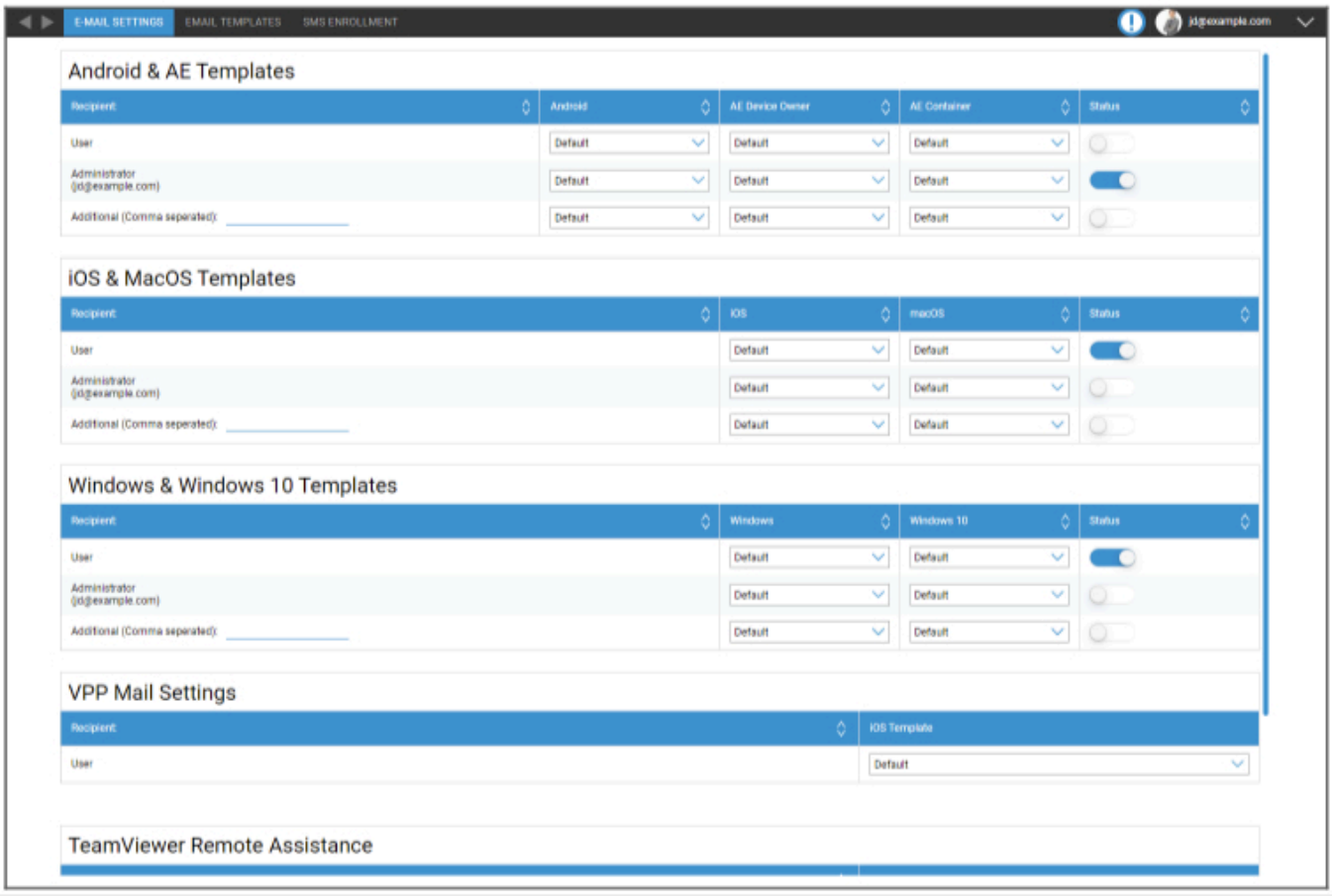
Um pedido de funcionalidade pode ser enviado diretamente para o suporte. Pode conter um pedido de uma caraterística específica ou uma melhoria para

Resumo	Uma breve sinopse do teu problema
Descrição	Uma descrição pormenorizada do teu problema, sendo o mais específico possível
Anexo	Anexa ficheiros ao relatório de bug

Configuração global

Definições de eMail

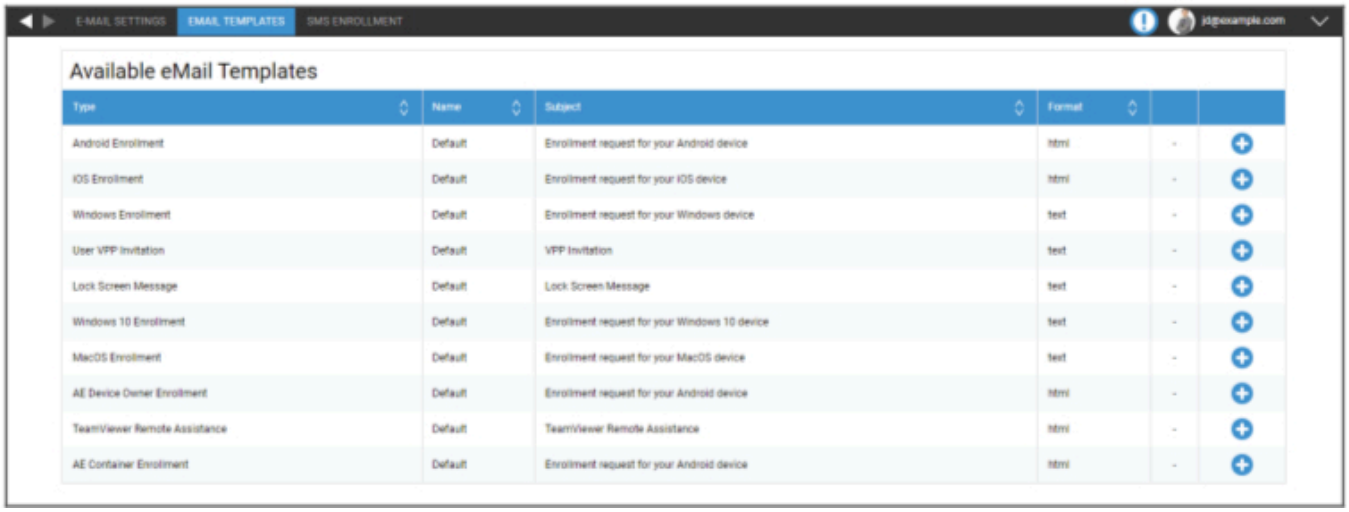
Aqui podes definir quem recebe um e-mail quando é gerado um pedido de inscrição e que modelo de texto é utilizado para esse e-mail.



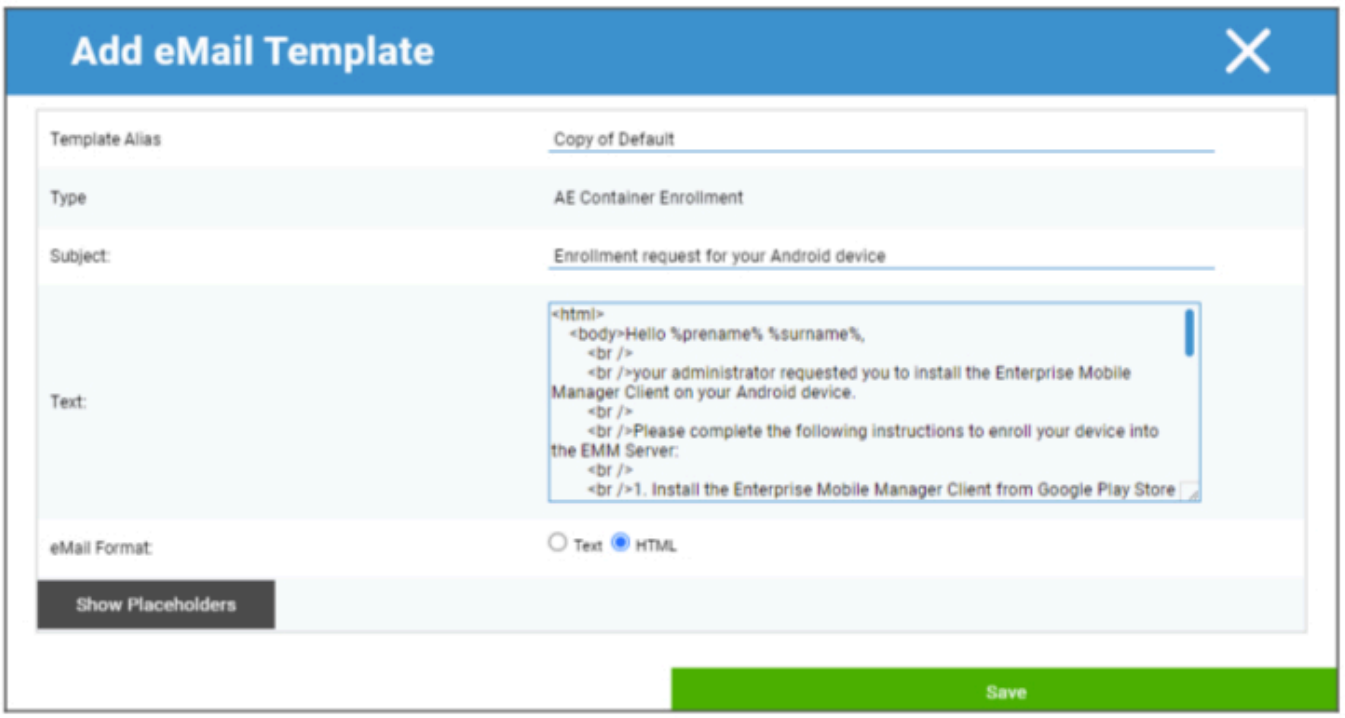
Modelos de eMail

Aqui podes gerar e editar os teus modelos para diferentes cenários. Estas podem ser em forma de texto normal ou em HTML. Com o HTML, podes controlar melhor a formatação do teu texto.

Os modelos predefinidos não podem ser editados ou apagados.



Também podes utilizar marcadores de posição como variáveis que serão automaticamente substituídas. Clica em "Mostrar marcadores de posição" durante a edição para veres os marcadores de posição disponíveis. Categorias diferentes têm marcadores de posição diferentes.



Inscrição no SMS

Aqui podes fazer/ativar o processo de inscrição no SMS.

(Predefinição: desativado)

Também verás um ecrã que indica quantos Créditos SMS ainda estão disponíveis.

Os Créditos SMS têm de ser adquiridos separadamente.

Privacidade

Acesso GPS

Aqui podes proteger a Vista GPS para cada dispositivo com 1 ou 2 palavras-passe (princípio dos quatro olhos). Ser-te-á pedido que introduzas a(s) tua(s) palavra(s)-passe sempre que tentares aceder à localização de um dispositivo.

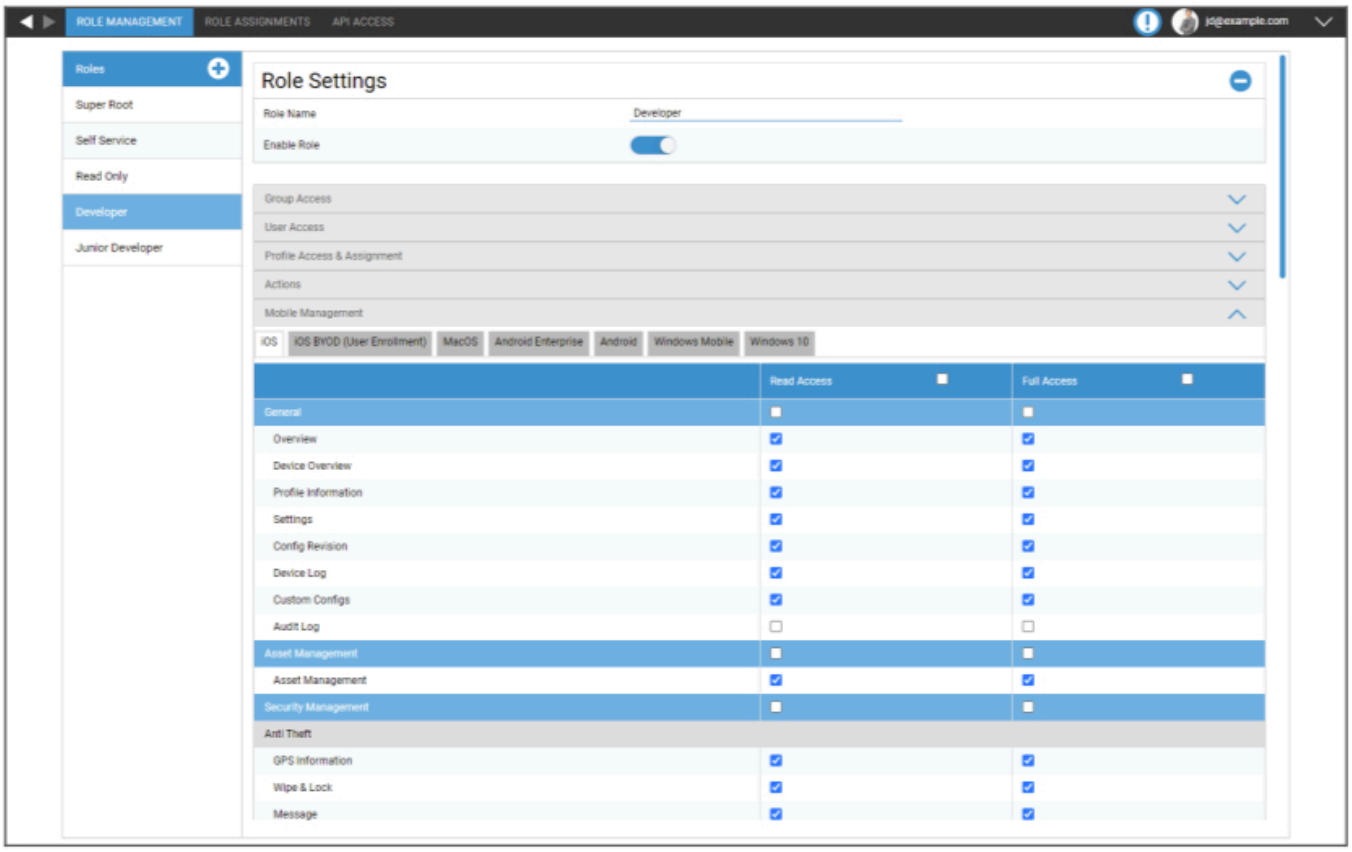
Restringe o acesso às definições de GPS	Desligado = a função está desligada e não é necessária nenhuma palavra-passe para a localização
	Ligado = a função está activada e é necessária uma palavra-passe para a localização
Método de proteção	Utilizar uma palavra-passe = utiliza uma palavra-passe para localizar
	Utilizar duas palavras-passe = utiliza duas palavras-passe para localizar
Introduzir palavra-passe (1)	Introduz a palavra-passe escolhida
Repete a palavra-passe (1)	Volta a introduzir a palavra-passe escolhida
opcional: Introduzir a palavra-passe 2	Introduz a segunda palavra-passe escolhida
opcional: Repete a palavra-passe 2	Volta a introduzir a segunda palavra-passe escolhida

Nota: Depois de definires o(s) teu(s) código(s) de acesso, tens de o(s) introduzir mais uma vez antes de ser(em) completamente ativado(s).

Acesso baseado em funções

Gestão de funções

As funções definem o que um utilizador pode ver e fazer quando inicia sessão na consola de gestão. Isto permite-te criar utilizadores que podem iniciar sessão mas que têm uma funcionalidade limitada.



A função Super Root é uma função predefinida que pode sempre ver e alterar tudo. Não pode ser alterado ou apagado. A função de autosserviço só pode ver os seus próprios utilizadores e dispositivos. Podes combinar o Self Service e uma função personalizada para, por exemplo, permitir que os utilizadores iniciem sessão e registem dispositivos por si próprios e apenas para o seu utilizador.

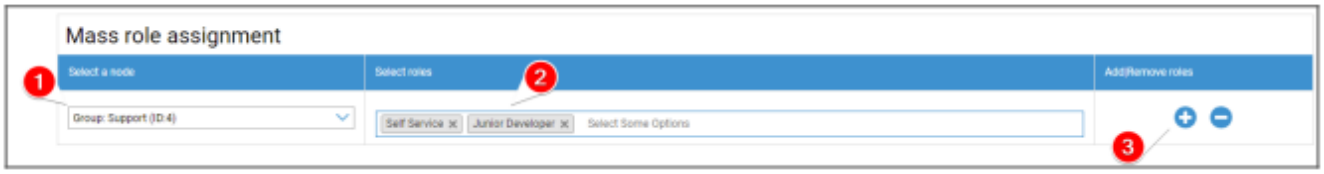
As funções personalizadas podem ser activadas ou desactivadas manualmente. As novas funções estão desactivadas por predefinição. Os utilizadores com uma função desactivada trabalham como se não tivessem essa função. Isto permite-te, por exemplo, restringir temporariamente uma determinada função das suas acções.

Todas as permissões estão divididas entre "Acesso de leitura" e "Acesso total". Dar acesso de leitura a uma função permite-lhe ver a parte específica da consola. Ao conceder-lhes acesso total, a função

pode ver e alterar a parte específica da consola.

Atribuições de funções

Aqui tens uma visão geral de todos os utilizadores que têm uma função e vês qual delas têm. Também podes atribuir uma função a utilizadores ou grupos inteiros aqui:

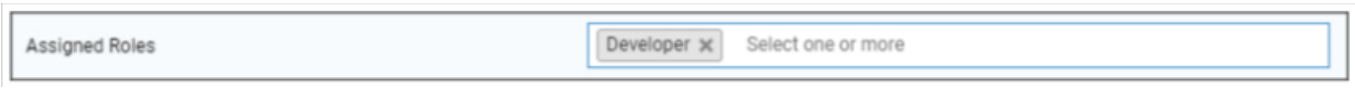


1. Selecciona para que grupo ou utilizador pretendes adicionar ou remover funções. Podes selecionar um único utilizador ou selecionar um grupo. Ao selecionar um grupo, a tua alteração afectará todos os utilizadores desse grupo e todos os utilizadores de subgrupos dentro do grupo selecionado.
2. Selecciona a função que pretendes adicionar ou remover. Podes selecionar uma ou várias funções.
3. . Selecciona a operação que pretende efetuar. Se clicares no "+", adicionas as funções seleccionadas se o(s) utilizador(es) ainda não as tiver(em). Ao clicar em "-", remove as funções seleccionadas do(s) utilizador(es). Se adicionares funções a um utilizador que ainda não tinha nenhuma função, será automaticamente activada a opção "Pode iniciar sessão" para o utilizador.
4. Guarda para terminar o processo. Os utilizadores que anteriormente não tinham qualquer função e tinham a opção "Pode iniciar sessão" desactivada receberão automaticamente um e-mail com uma ligação para definir uma palavra-passe.

Abaixo da atribuição de funções em massa, encontra-se a síntese das funções atribuídas. Também podes alterar manualmente as funções de utilizadores específicos.

Atribuição de uma função

Para atribuir uma função a um utilizador, tem de ir à Gestão móvel, onde encontra a árvore dos seus grupos, utilizadores e dispositivos. Edita o utilizador para atribuir uma função. Em alternativa, também podes utilizar o método acima mencionado apenas para utilizadores individuais.



Acesso à API

Acede à API REST da AppTec360

A API REST da AppTec360 requer um token de autenticação (chave da API) e uma chave privada que têm de ser gerados na Consola de gestão.

Para o fazer, inicia sessão no AppTec360 EMM e acede a

Definições gerais → Acesso baseado em funções → Acesso à API e adiciona uma nova chave.

Tens de selecionar um utilizador cujas permissões se apliquem à chave da API.

A chave privada só pode ser descarregada uma vez. Após o início da transferência, a chave é eliminada e o botão "Transferir" desaparece.

Se perderes a tua chave privada, terás de gerar uma nova chave API.

Regras gerais

- A API REST está disponível abaixo do URL de base:

/public/external/api

- Todos os pedidos têm de ser enviados através de POST.
- A API REST só suporta pedidos via HTTPS.
- Os pedidos devem conter os seguintes cabeçalhos:

Nome do cabeçalho	Valor do cabeçalho	Descrição
Tipo de conteúdo	aplicação/json	fixa
autenticação	123...xyz	Chave da API no separador "Acesso à API"
assinatura	Assinatura codificada em base64	Assinatura do payload gerado com o chave privada do separador "Acesso à API

- O corpo do pedido deve ser um objeto codificado em json que deve conter os seguintes valores:

Campo	Campo Exemplo Valor	Descrição
API	v2/dispositivo/lista de dispositivos	Nome da API
tempo	1529662725	Carimbo de data/hora Unix (UTC) da máquina cliente. A diferença de tempo máxima permitida entre o cliente e o servidor é de 30 minutos.

- Em caso de sucesso, a API devolve os dados solicitados (ver as consultas abaixo) e um código de estado HTTP 200.
- Se ocorrer um erro, o código de estado HTTP será entre 4xx e 5xx, dependendo do erro, e o objeto de resposta conterá uma matriz com a chave "errors", que contém uma lista de mensagens de erro legíveis por humanos.
- Se não existirem dados correspondentes para um dispositivo, é devolvido um conjunto vazio.
- Se um ID de dispositivo não existir, os dados de retorno serão nulos.

Exemplo de pedido

```
POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}
```

Consultas

Lista todos os dispositivos

Funcionalidade: Devolve uma lista de todos os dispositivos com a ID do dispositivo, IMEI e série
URI da API: v2/device/listdevices
Parâmetros obrigatórios: nenhum
Parâmetros opcionais: nenhum

Exemplo de corpo de pedido


```
{
"api": "v2/device/listdevices",
"time": 1529662725
}
```


Exemplo de corpo de resposta


```
{
"errors": [],
"list":[
{ "id":"10","serial":"987612345","imei":"899938455454"},
{ "id":"11","serial":"619723118","imei":"713032378599"}
]
}
```

Obtém uma lista de posições (GPS)

Funcionalidade: Devolve uma lista de todas as entradas de registo de posição armazenadas para ids de dispositivos
API URI: v2/device/listposition
Parâmetros obrigatórios: "ids" - Conjunto de IDs de dispositivos
Parâmetros opcionais: nenhum

Exemplo de corpo de pedido


```
{
"api": "device/listposition",
"params": {
"ids": [10, 11]
},
"time": 1529662725
}
```


Exemplo de corpo de resposta


```
{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}
```

Obter mapa de activos

Funcionamento:
Devolve uma lista de todos os possíveis activos armazenados a solicitar utilizando a opção Obter quaisquer dados de activos.
Podes utilizar o formulário legível por humanos ou a etiqueta do imobilizado para solicitar os dados.
URI da API: v2/device/getassetmap
Parâmetros obrigatórios: nenhum
Parâmetros opcionais: nenhum

Exemplo de corpo de pedido

{
"api": "v2/device/getassetmap",
"time": 1529662725
}

Exemplo de corpo de resposta

Esta resposta foi encurtada para facilitar a leitura.

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

Obtém quaisquer dados de activos

Funcionalidade: Devolve uma lista de dados de activos solicitados para ids de dispositivos
URI da API: v2/device/getassetdata
Parâmetros obrigatórios: "ids" - Conjunto de IDs de dispositivos
Parâmetros opcionais:
"assetkeys" - Chaves de dados do ativo a devolver. Se não for especificado, todos os dados de activos disponíveis serão
devolvido. Podes obter uma lista de chaves de activos utilizando Obter mapa de activos.

Exemplo de corpo de pedido

{
"api": "v2/device/getassetdata",
"time": 1529662725,
"params": {
"ids": [
26
],
"assetkeys": [
"imei"
]
}
}

Exemplo de corpo de resposta

{
"result": {
"26": {
"imei": "349157642516427”
}
},
"errors": []
}

Exemplo de código em Python3

```
! /usr/bin/python
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
applianceDomain = "YOURAPPLIANCE.COM"
apiURL = "https://"+applianceDomain+"/public/external/api"
privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
currentTimestamp = int(time.time())
# Get Devices
#requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}
# Get Positions
#requestData = {"api": "v2/device/listposition", "time": currentTimestamp,
"params":{"ids":[26]}}
# Get AssetData
requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp,
"params":{"ids":[26], "assetkeys": ["imei"]}}
# encode the request data to json
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
# Sign the request data json with the API private key
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
digest = SHA512.new()
digest.update(message)
```

```
# Read private key from file
with open(privateKeyPath, "r") as myKeyFile:
private_key = RSA.importKey(myKeyFile.read())
```

```
# Load private key and sign message
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
Base64EncodedSignature = base64.b64encode(
signatureOfRequestData).decode("utf-8")

headers = {"Content-type": "application/json",
"auth": apptecAPIAuthToken, "signature": Base64EncodedSignature}
print("Headers:", headers, "\n")

# Send request to Server
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

# Get answer
response = httpsClient.getresponse()
status = response.status
data = response.read()

if data == False:
print("Invalid answer from the server")
else:
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
if status != 200:
print("http error: lastReceivedHttpCode")
print(status)
```

Configuração da Apple

Certificado APNS

Aqui podes carregar um certificado APNS. Isto é necessário para gerir dispositivos iOS e MacOS.

Nota: O certificado APNS só é válido por um ano. Tens de o renovar antes de expirar. O processo de renovação é idêntico ao da criação (ver abaixo) e demora apenas alguns minutos.

Se te esqueceres de renovar a tempo, não podes fazer alterações nos dispositivos já registados **e tens de voltar a registar todos os aparelhos** .

Passo 1

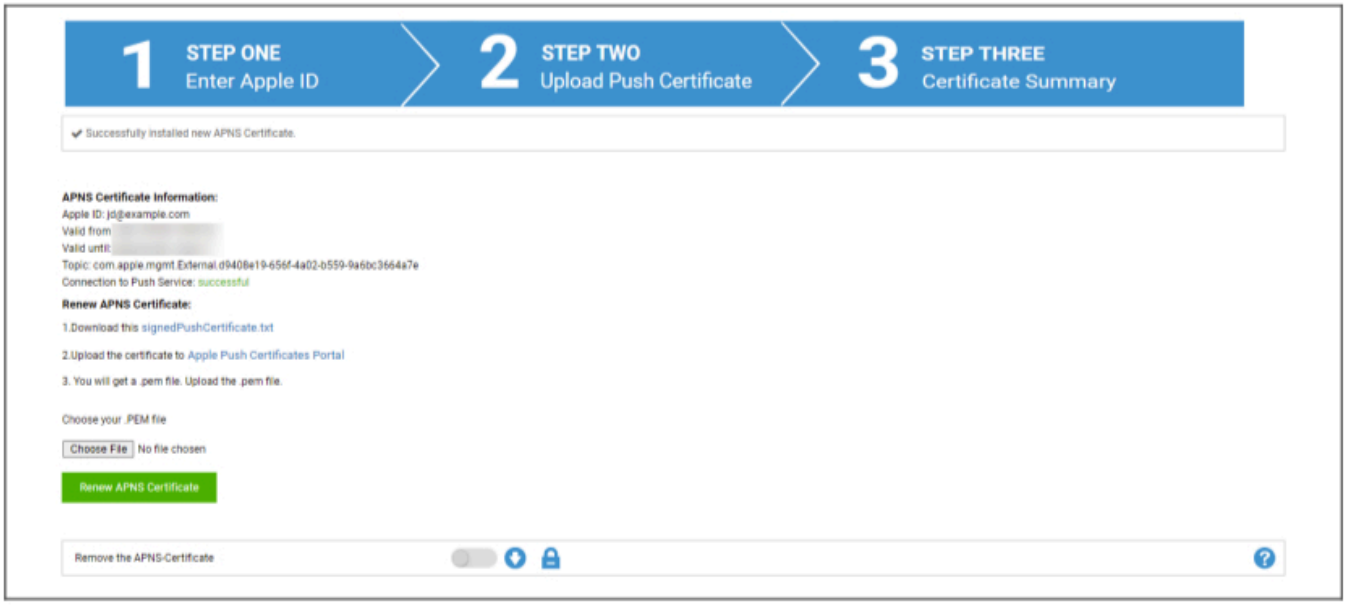
- Primeiro, introduz o ID Apple que pretendes utilizar para criar o Certificado APNS.

Nota: Este ID Apple só é utilizado para a criação do certificado APNS. Este ID Apple não tem nada a ver com os dispositivos e os dispositivos não terão conhecimento deste ID Apple. Além disso, também precisas de aceder a este ID Apple para renovar o Certificado APNS. Por isso, recomenda-se que utilizes um ID Apple genérico e documentes os dados de início de sessão. Envia um lembrete para o endereço de correio utilizado do ID Apple antes de o certificado APNS expirar.

- Clica em "Passo seguinte" para prosseguir.
- (opcional) Também podes recuperar o certificado APNS anteriormente eliminado se o tiveres eliminado por acidente

Passo 2

- Transfere o ficheiro signedPushCertificate.txt
- Acede a https://identity.apple.com/pushcert/ e inicia sessão com o ID Apple do Passo 1
- Clica em "Criar um certificado"
- (opcional) introduz uma Nota. Isto pode ser útil se gerires vários inquilinos para os identificares facilmente.
- Clica em "Choose File" (Escolher ficheiro) para selecionar o ficheiro signedPushCertificate.txt transferido anteriormente
- Clica em "Carregar".
- Verás agora a confirmação de que criaste um certificado APNS.
- Clica em "Transferir" e guarda-o.
- Volta à consola de gestão.
- Clica em "Escolher ficheiro" e selecciona o certificado APNS que pretendes carregar.
- Clica em "Carregar"



Passo 3

Configuraste com êxito o certificado APNS e podes agora gerir dispositivos iOS e MacOS.

No passo 3, verás uma visão geral do teu certificado APNS atualmente utilizado.

Também tens a opção de renovar o certificado APNS seguindo os passos apresentados no ecrã. Não te esqueças de o renovar antes de expirar.

Quando renovares o Certificado APNS, não te esqueças de iniciar sessão com o ID Apple apresentado no Passo 3 e também de renovar o certificado utilizado anteriormente e NÃO criar um novo. Verás o "tópico" do Certificado APNS no Passo 3 e quando clicares no "i" no Portal do Certificado Apple Push. Este é o ID único que identifica o certificado. Isto ajudar-te-á a identificar e a renovar a opção correcta.

Quando recebes a mensagem "Erro: O certificado push tem um tópico diferente!" durante a renovação, isso significa que renovaste outro certificado ou criaste um novo.

Se quiseres carregar um novo certificado, por exemplo, se já não conseguires aceder ao ID Apple utilizado anteriormente, primeiro tens de eliminar o certificado carregado atualmente.

De qualquer forma, apagar o certificado APNS significa que já não podes fazer alterações nos dispositivos atualmente registados até os registares novamente. Por isso, certifica-te de que estás preparado para esta situação e remove o certificado apenas se não houver outra forma.

Acesso gerido

Aqui podes ativar a inscrição de utilizadores para dispositivos iOS e o iPad partilhado para dispositivos iOS.

Inscrição de utilizadores

O "Registo de utilizadores" permite um modo especial para dispositivos BYOD.

Para cada utilizador, tem de ser criado um Apple-ID gerido no Apple Business Portal.

Durante o processo de registo, os utilizadores serão solicitados a fornecer as suas credenciais Apple-ID.

A "inscrição do utilizador" garante a máxima segurança para o utilizador, uma vez que apenas permite que um conjunto limitado de definições e restrições seja configurado pela MDM.

Domínio gerido:

O domínio utilizado para mapear o endereço de correio eletrónico do utilizador para o seu Apple-ID gerido (tem de estar no formato: '@appleid.company.com'). Por exemplo, john.doe@example.com será mapeado para john.doe@appleid.company.com

Consulta o Apple Business Manager para veres o teu domínio gerido

iPad partilhado

Um iPad partilhado é um dispositivo DEP configurado com um perfil DEP especial.

Isto permite que vários utilizadores iniciem sessão no dispositivo utilizando o seu ID Apple gerido.

O Apple-ID gerido tem de ser criado no Apple Business Portal ou no Apple School Manager.

Os utilizadores que iniciam sessão num iPad partilhado são solicitados a fornecer as suas credenciais Apple-ID geridas.

Domínio gerido:

O domínio utilizado para mapear o endereço de correio eletrónico do utilizador para o seu Apple-ID gerido (tem de estar no formato: '@appleid.company.com'). Por exemplo, john.doe@example.com será mapeado para john.doe@appleid.company.com

Consulta o Apple Business Manager para veres o teu domínio gerido

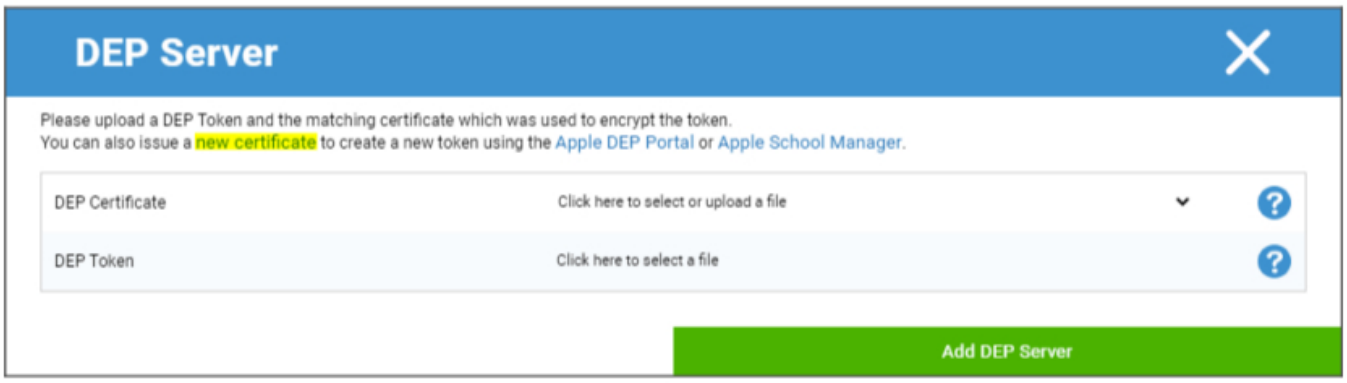
DEP

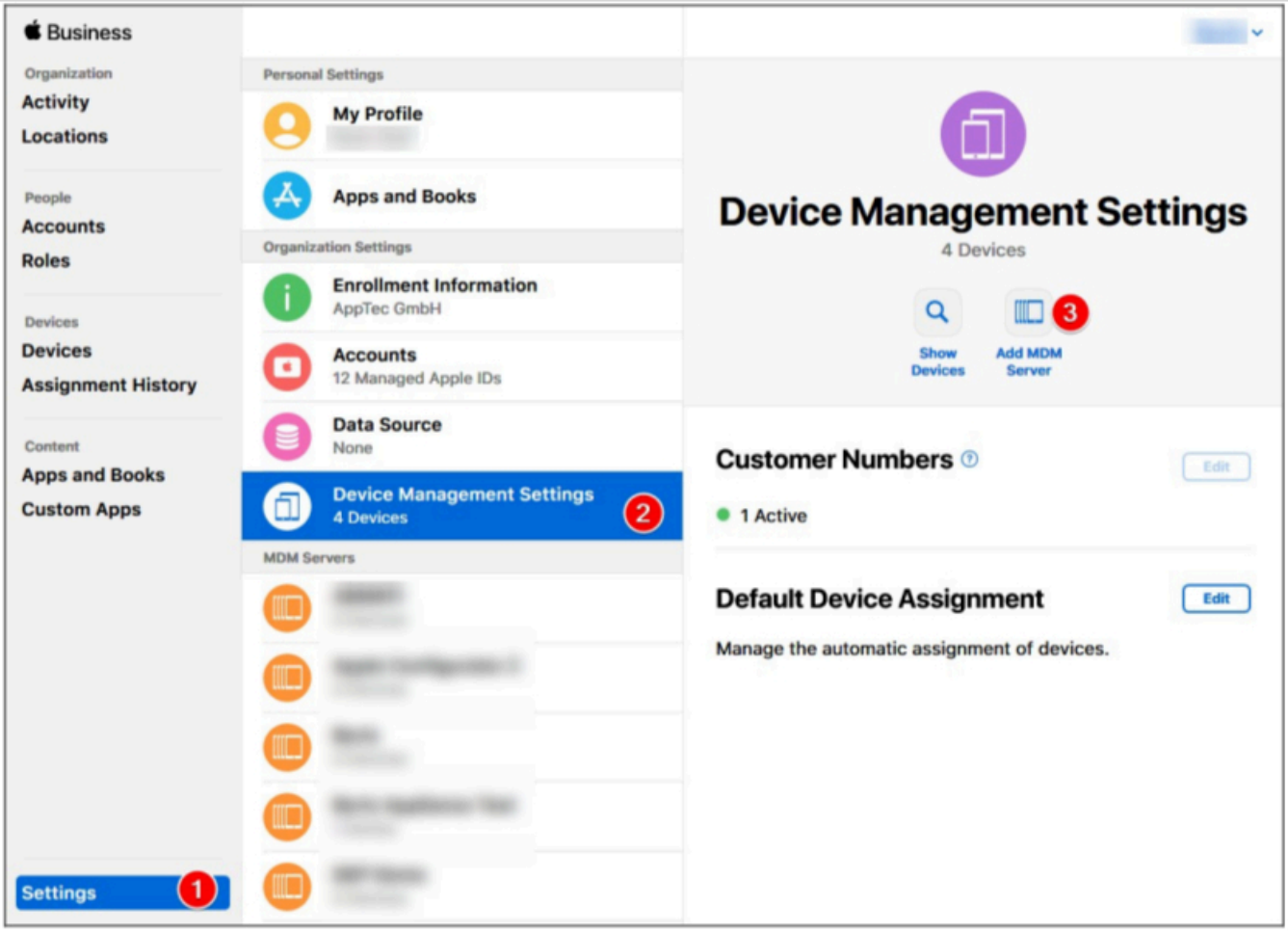
O DEP (Device Enrollment Program) permite-te registar facilmente os dispositivos na MDM. Se utilizares a DEP, os dispositivos serão automaticamente ligados à MDM quando configurares o dispositivo. Também podes saltar quase todos os passos de configuração que são normalmente obrigatórios no iOS.

Tem em atenção que tens de comprar os dispositivos a um revendedor que suporte a DEP. Para mais informações, contacta o teu revendedor ou a Apple.

Mais informações sobre o DEP: https://www.apple.com/business/dep/

Clica no "+" para adicionar um Token DEP. Na janela pop-up, clica em "novo certificado" no texto (marcado a amarelo na imagem abaixo). Isto irá gerar e descarregar um certificado DEP. Em seguida, acede ao Apple Business Manager(https://business.apple.com/) ou ao Apple School Manager(https://school.apple.com/).

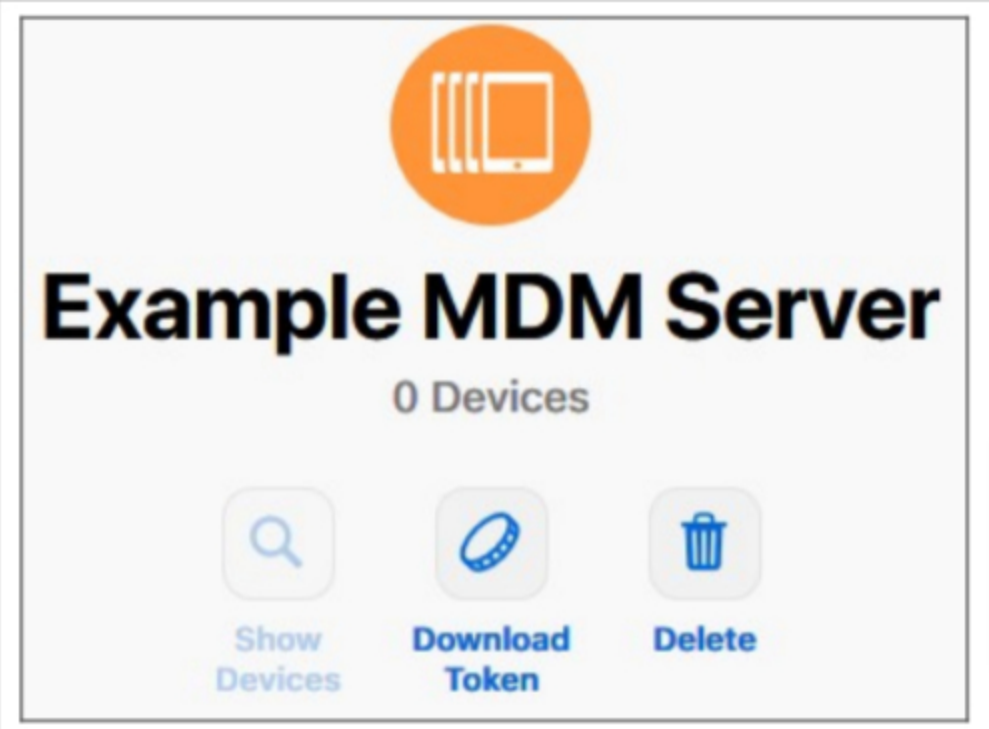




No Apple Business Manager, segue os passos indicados na imagem acima. Definições → Definições de gestão de dispositivos → Adicionar servidor MDM.

Dá ao servidor o nome que quiseres e carrega o certificado DEP transferido anteriormente em MDM Server Settings → Upload Public Key e clica em "Save".

Terás agora a opção "Transferir Token". Clica aqui e guarda-o. O Token só é válido por 1 ano. Mas basta clicares novamente em "Download Token" para obteres um novo, o que torna a renovação do token muito fácil.



Podes agora voltar à MDM, onde descarregaste anteriormente o certificado DEP. Se não fechaste o separador, a janela pop-up para adicionar um servidor DEP ainda deve estar aberta e o certificado DEP já deve estar selecionado. Podes agora carregar o teu Token no campo "DEP Token" e clicar em DEP Server.

Na coluna "**Devices**" (**Dispositivos**), verás a quantidade de dispositivos que estão atribuídos a este servidor DEP. Os dispositivos adicionados a este servidor DEP serão automaticamente criados no conjunto de DEP na Gestão de dispositivos móveis.

Podes clicar neste número para obteres uma visão geral de todos os teus dispositivos DEP e do seu estado.

Nota: Dependendo do teu fluxo de trabalho ou configuração no Business Manager, pode ser possível que tenhas de atribuir manualmente estes dispositivos ao servidor DEP. Também podes definir um servidor DEP predefinido no Apple Business Manager para novos dispositivos.

Na coluna "**Profiles**" (**Perfis**), vês a quantidade de perfis DEP que tens. Também podes clicar neste número para veres detalhes sobre os teus perfis DEP e podes apagar perfis antigos/não utilizados aqui. Atualmente, não é possível alterá-las. Se queres fazer uma mudança, tens de criar uma nova.

Na coluna "**Last Synchronization**" (**Última sincronização**), podes sincronizar manualmente o servidor DEP (por exemplo, se acabaste de adicionar um novo dispositivo ao DEP) e ver a data da última sincronização bem sucedida.

Na coluna "**Perfil automático**", podes definir um perfil DEP como predefinição automática. Este perfil será atribuído automaticamente aos novos dispositivos. Se não definires um perfil automático, terás de atribuir manualmente um perfil a novos dispositivos de cada vez.

Na coluna "**Adicionar perfil**" podes adicionar um novo perfil DEP. O aparelho recebe-o no início da configuração do aparelho. O perfil DEP define a forma como o dispositivo é configurado e quais os passos de configuração que serão ignorados.

Nota: depois de um dispositivo ser registado, estas definições só podem ser alteradas através de uma reposição de fábrica e do registo do dispositivo com um novo perfil. Isto é especialmente relevante para "**Removível**" e "**Permitir emparelhamento**". No caso de "**Allow pairing**" (**Permitir emparelhamento**), recomenda-se que o actives, uma vez que pode ser desativado através das restrições MDM, mas não pode ser ativado novamente se estiver desativado no perfil DEP.

Na coluna "**Editar**" podes carregar um novo token, por exemplo, quando renovas o Token.

Configurador e URL

URLs de inscrição na piscina

Aqui podes criar um URL de inscrição e um código QR de inscrição que é válido para um determinado número de inscrições e até uma determinada data. Isto permite-te registar vários dispositivos com apenas uma ligação ou código QR.

Os dispositivos registados com este URL ou código QR estarão na lista de dispositivos na Gestão de dispositivos móveis e, posteriormente, terás de os atribuir manualmente a um grupo ou utilizador.

Nota: isto é apenas para a inscrição manual. Não utilizes este URL se registares os dispositivos através do Apple Configurator

Perfil MDM – Configurador da Apple

Aqui podes obter o URL de que precisas para registar dispositivos através do Apple Configurator. Enquanto preparas os dispositivos com o Apple Configurator, podes adicionar os dispositivos à MDM no mesmo processo. O Apple Configurator requer este URL para o efeito.

Os dispositivos adicionados através do Apple Configurator estarão na lista de dispositivos na Gestão de dispositivos móveis e, posteriormente, terás de os atribuir manualmente a um grupo ou utilizador.

Também encontrarás aqui um ficheiro .mobileconfig que pode ser utilizado para registar os dispositivos através do Apple Configurator. De qualquer forma, recomenda-se que utilizes o URL.

Configuração do Android

Configuração do Android

Desinstalar a proteção	Se esta função estiver activada, o utilizador não pode desativar o administrador do dispositivo sem introduzir a palavra-passe definida pelo administrador da MDM. A palavra-passe é definida durante o registo, pelo que os dispositivos têm de ser novamente registados para atualizar a palavra-passe. Existem duas opções para remover os administradores de dispositivos: 1. Manualmente no dispositivo ◦ Abre a aplicação EMM no dispositivo ◦ Muda para o separador Estado ◦ Toca em "Desinstalar proteção" ◦ Introduzir a palavra-passe Podes utilizar a Revisão para obter a palavra-passe correcta a partir do "Histórico de palavras-passe" na consola. ◦ Desliza para baixo e toca no ponto recentemente adicionado, "Tap to uninstall AppTec360 MDM App" (tens 20 segundos para executar esta tarefa) ◦ Confirma a caixa de diálogo "Desinstalar a AppTec360 MDM App" com "ok". Isto irá anular a inscrição do dispositivo na consola. ◦ Para remover a aplicação do dispositivo, confirma a caixa de diálogo "A AppTec360 MDM será desinstalada" com "DESINSTALAR" 2. o automático (Consola) ◦ Selecciona o dispositivo na consola ◦ Clica no ícone de engrenagem azul e selecciona "Enterprise Wipe"

	Nota: Apenas disponível com Android 4.x e versões inferiores ou em dispositivos com a API KNOX (dispositivos Samsung)
Senha de desinstalação (Revisão x)	A palavra-passe estabelecida, com a qual o utilizador pode remover o administrador do dispositivo Revisão x = contador, quantas vezes a palavra-passe já foi alterada É importante saber qual a palavra-passe de que o utilizador necessita, porque é possível que o dispositivo não tenha comunicado com o AppTec360 Server e, por isso, a palavra-passe mais recente ainda não tenha sido transmitida
Histórico da palavra-passe	Quando clicas no botão azul ("Mostrar histórico"), podes ver as palavras-passe previamente estabelecidas
Proteção alargada contra desinstalação	Esta opção oferece proteção contra dispositivos não-SAFE Enquanto esta definição estiver activada, não é possível desativar facilmente o administrador do aparelho
Pede ao utilizador para desinstalar as aplicações bloqueadas?	Se possível, as aplicações bloqueadas não só serão bloqueadas como também desinstaladas automaticamente. O utilizador será solicitado a desinstalar as aplicações bloqueadas se não for possível uma desinstalação automática.
Sistema inteligente de bloqueio de aplicações	Se a lista branca estiver activada, o Cliente MDM Android bloqueia todas as aplicações instaladas pelo utilizador. Ativa esta definição para bloquear todas as aplicações de sistema que possam ser iniciadas no modo de lista branca.

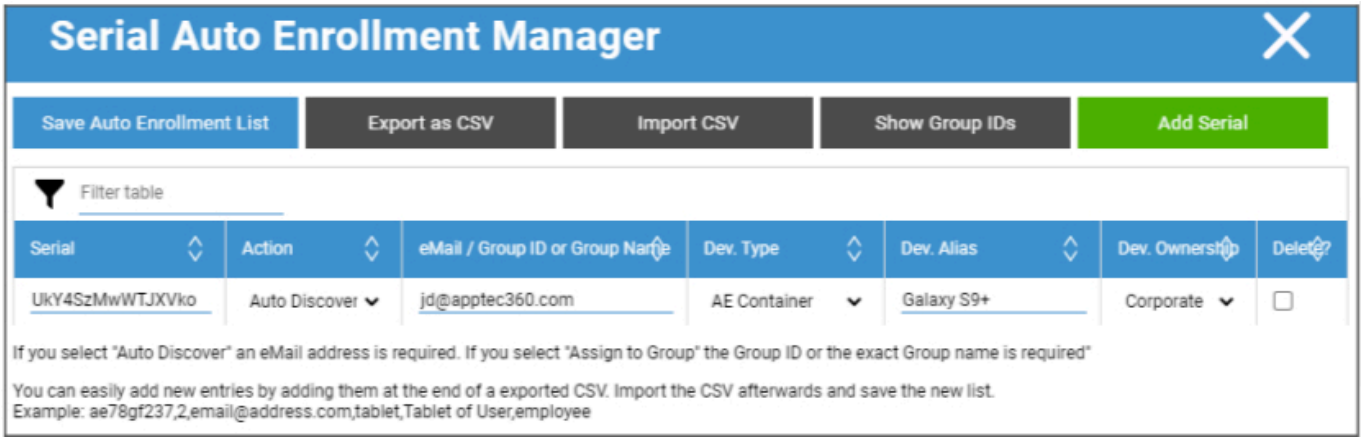
Inscrição automática

Aqui podes ativar a funcionalidade Auto Enrollment (Inscrição automática) para inscrever os teus dispositivos automaticamente quando o AppTec360 MDM Client é aberto no dispositivo.

Importante: este método de registo está obsoleto e já não funciona no Android 10 ou superior. De qualquer modo, quando utilizas o Android 7 ou superior, deves registar os dispositivos como Android Enterprise totalmente gerido. Se quiseres utilizar o contentor BYOD do Android Enterprise e tiveres o Android 10 ou superior, tens de registar manualmente o dispositivo através de credenciais, código QR ou SMS. De qualquer modo, a lista de inscrição automática continua a ser utilizada para automatizar o processo de inscrição, por exemplo, inscrição AE, inscrição Knox, etc.

De qualquer modo, a lista de inscrição automática continua a ser utilizada para automatizar o processo de inscrição, por exemplo, inscrição AE, inscrição Knox, etc.

Ao clicar em "Gestor de série" ou "Gestor de IMEI", podes adicionar a série ou o IMEI dos teus dispositivos, respetivamente. Não é necessário fazer as duas coisas para os teus dispositivos, apenas uma é suficiente.



A ação define se os dispositivos serão inscritos no agrupamento, num utilizador ou num grupo.

Também podes exportar e importar um ficheiro .csv e filtrar as tuas entradas por palavras-chave.

Android Enterprise

Aqui podes configurar o Android Enterprise. Isto é necessário para utilizares todas as funcionalidades do Android Enterprise.

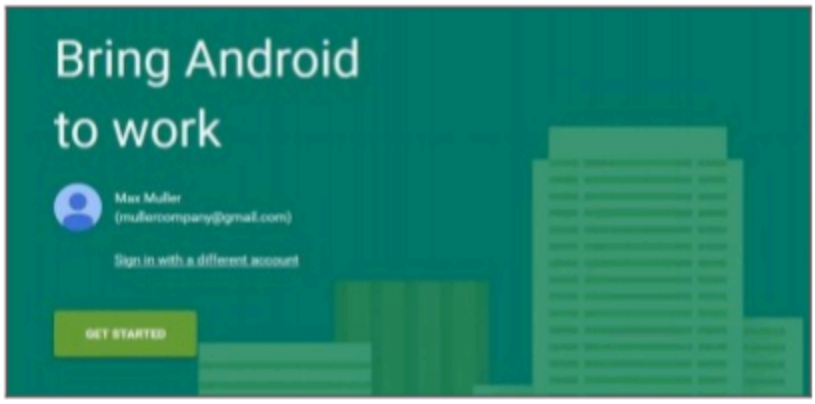
Primeiro método: Conta empresarial Android (Conta Google)

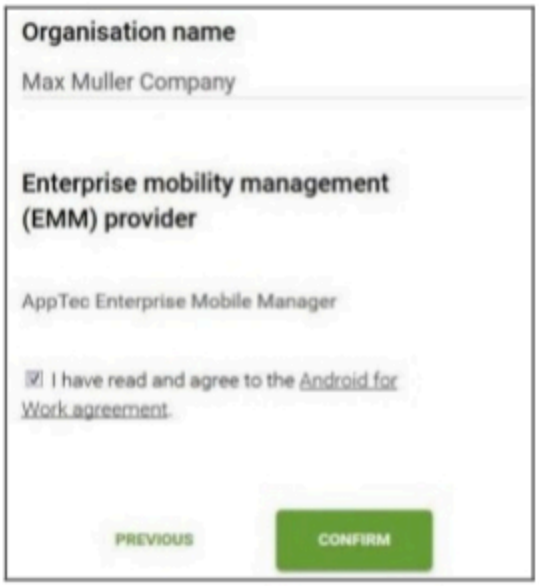
Primeiro carrega em "Preparar Configuração" e, após um breve momento, deve aparecer o botão "Iniciar Configuração".

Isto leva-te à página de configuração do Android Enterprise da Google.

Inicia sessão com a Conta Google que pretendes utilizar, se ainda não tiveres iniciado sessão, e prime "Começar".

Agora podes introduzir o nome da tua empresa. Depois de o fazer, marca a caixa de verificação e prime "Confirmar"





No último passo podes completar o teu registo e deves regressar à consola. Se tudo tiver funcionado, deves ter o seguinte aspeto:

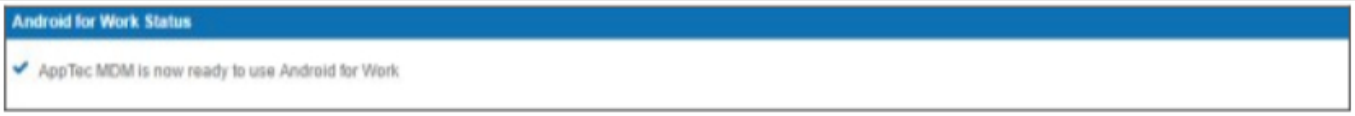
Agora podes começar a configurar o teu Android Enterprise Container.

Segundo método: Conta G-Suite

Carrega em "Utilizar o G-Suite" e inicia sessão na tua conta de administrador do Google. Aí vais a "Segurança" -> "Mostrar mais" -> "Gerir fornecedor EMM para Android" e gerar um Token. Nota: Se não vires as Definições empresariais do Android na tua conta G-Suite, tens de ir a "Obter mais aplicações e serviços" e adicionar a gestão de dispositivos Android. Agora, introduz o Token e o teu domínio principal na nossa consola e clica em "Guardar alterações". Quando tiveres terminado, clica em "Utilizar conta empresarial Android".

Agora, deves ver o botão "Criar conta de serviço". Clica nele. Este processo pode demorar alguns instantes.

Se tudo tiver funcionado, deves ter este aspeto:



Agora podes começar a configurar o teu Android Enterprise Container.

Proteção contra reposição de fábrica

Com a proteção de reposição de fábrica, podes associar o teu dispositivo a uma conta Google à tua escolha, o que também substitui qualquer associação existente a uma conta Google. Para utilizares a proteção contra reposição de fábrica, tens de a configurar aqui primeiro e depois activá-la nos teus perfis.

Para configurar a proteção de reposição de fábrica, clica em "FRP Setup" e segue as instruções no ecrã.

NOTA: Lê atentamente e executa os passos. Recomendamos que o faças numa nova janela incógnita do browser para evitar iniciar sessão automaticamente na conta Google errada. Podes bloquear-te completamente do dispositivo, se introduzires uma ID errada ou perderes o acesso à Conta Google utilizada!

Inscrição na AE

Aqui podes ativar o Android Enterprise Ernollment. A utilização deste método irá inscrever os teus dispositivos no modo de proprietário do dispositivo Android Enterprise. Neste modo, terás o controlo total sobre o dispositivo.

Ativar o registo AE	Ativa o Registo AE Atenção: Se desactivares a Inscrição AE, os Códigos QR existentes e os dispositivos programadores NFC já configurados deixarão de funcionar. Se voltares a ativar o Registo AE, terás de reenviar as configurações push NFC / gerar novos códigos QR.
Ativar a descoberta automática	Quando um dispositivo se inscreve através da "Inscrição AE", o sistema tenta atribuí-lo a um utilizador com base nas informações definidas na lista branca de série/IMEI ("Definições gerais" > "Configuração do Android" > "Inscrição automática").
Bloqueia dispositivos desconhecidos	Só os dispositivos que tenham sido incluídos na lista branca de série/IMEI ("Definições gerais" > "Configuração do Android" > "Inscrição automática") podem inscrever-se.

Nota sobre os métodos 1 e 2: "Ecrã de boas-vindas" refere-se ao primeiro ecrã que vês após a reposição de fábrica. Este aspeto pode ser diferente consoante a versão do Android e/ou o modelo do dispositivo que estás a utilizar.

Método 1: Inscrição no código QR

(requer Android 7.0 ou superior) Recomendamos que utilizes sempre este método se tiveres o Android 7 ou superior.

1. Repõe o dispositivo de fábrica
2. Gera o código QR para o registo utilizando um dos dois métodos seguintes:
    - Clica em "Definições gerais -> Configuração do Android -> Inscrição AE" em "Gerar código QR". Escolhe se pretendes saltar a encriptação do armazenamento e/ou se todas as aplicações do sistema devem ser removidas.
    - (em alternativa) Escolhe um dispositivo existente. Em "Visão geral do dispositivo", clica no código QR aí apresentado. Escolhe se pretendes saltar a encriptação do armazenamento e/ou se todas as aplicações do sistema devem ser removidas.
3. Agora toca 6 vezes no ecrã de boas-vindas do teu dispositivo. Isto deve iniciar o modo de registo QR.
4. Agora liga-te a uma rede sem fios e espera um pouco até que o leitor de código QR seja instalado
5. Agora lê o código QR
6. E pronto. O teu dispositivo está agora inscrito no modo de dispositivo Android Enterprise.

- a. Se utilizaste o código QR em "Definições gerais", podes encontrar o teu dispositivo em "Pool -> Dispositivos do proprietário do dispositivo AE". (Dica: é possível que tenhas de recarregar o site para veres os dispositivos). Se marcaste "Ativar a Descoberta Automática", encontrá-lo-ás no teu utilizador da Descoberta Automática.
- Se utilizaste o código QR de um perfil de dispositivo existente, o dispositivo será inscrito nesse perfil.

Método 2: Registo NFC

(requer NFC e Android 6.0 ou superior)

Prepara-te: Introduz as tuas informações WiFi em "Definições gerais -> Configuração do Android -> Registo AE -> Dados para aprovisionamento NFC". Agora usa "Dispositivo NFC" para procurar o dispositivo que será o programador. Este dispositivo será utilizado para enviar as informações de registo para os outros dispositivos através de NFC.

1. Reposição de fábrica do teu dispositivo
2. Abre a aplicação de emparelhamento NFC da AppTec360 no teu programador
3. Escolhe se pretendes saltar a encriptação do armazenamento e/ou se todas as aplicações do sistema devem ser removidas.
4. Segura os dois dispositivos de costas um para o outro
5. Agora, o Android Enterprise Enrollment deve ser o mais importante
6. Encontra agora o teu dispositivo na consola
    - a. No grupo, se não tiveres configurado a Descoberta Automática
    - b. No utilizador que configuraste para a Descoberta Automática
    - c. Dica: É possível que tenhas de recarregar o sítio para ver os dispositivos

Método 3: Conta Google

(requer Android 5.1 ou superior)

(Nota: Se estiveres a utilizar este método, o dispositivo não será automaticamente registado. Em vez disso, tens de o registar manualmente ou automatizar o processo utilizando o Registo automático).

1. Reposição de fábrica do teu dispositivo
2. Segue os passos de configuração até conseguires iniciar sessão com uma conta Google
3. Introduz "afw#apptec" como Nome de Utilizador/Mail
4. Toca em "Seguinte"
5. O teu dispositivo é agora um dispositivo Android Enterprise

KNOX Inscrição

Aqui podes ativar a Inscrição KNOX e encontrar as informações necessárias para criar um Perfil de Inscrição KNOX no Portal de Implementação KNOX. Precisas de uma conta no Portal de implementação KNOX para a configurar e utilizar.

(https://www.samsungknox.com/en/knox-deployment-program)

Ativar o registo KNOX	Ativa o registo KNOX. Tem cuidado: Se desactivares o Registo KNOX, os perfis MDM existentes deixarão de funcionar. Se activares o Registo KNOX novamente, terás de atualizar o campo "Dados JSON personalizados" do teu Perfil MDM
Ativar a descoberta automática	Quando um dispositivo se inscreve através da "Inscrição KNOX", o sistema tenta atribuí-lo a um utilizador com base nas informações definidas na lista branca de série/IMEI ("Definições gerais" > "Configuração do Android" > "Inscrição automática").

1. Inicia sessão no portal de registo móvel Samsung KNOX https://eukme.samsungknox.com/itadmin
2. Vai para "Perfis MDM"
3. Clica em "Adicionar"
4. Escolhe "Server URI not required for my MDM" e clica em "Next" (Seguinte)
5. Agora cria um perfil com as informações apresentadas na consola de gestão

Agora, este perfil de registo KNOX pode ser instalado diretamente no dispositivo pela Samsung, se adquirires os dispositivos diretamente à Samsung.

Em alternativa, podes descarregar a aplicação KNOX Deployment, iniciar sessão com a tua conta KNOX Deployment e enviar o perfil de inscrição KNOX através de NFC para outros dispositivos.

Se o dispositivo tiver um perfil de registo KNOX instalado, descarrega a nossa aplicação e regista o dispositivo, se tiver uma ligação à Internet em funcionamento.

A inscrição de dispositivos através da inscrição KNOX pode ser encontrada em "Pool -> KNOX Enrollment", ou no utilizador que especificaste na Auto Discover.

Zero-Touch

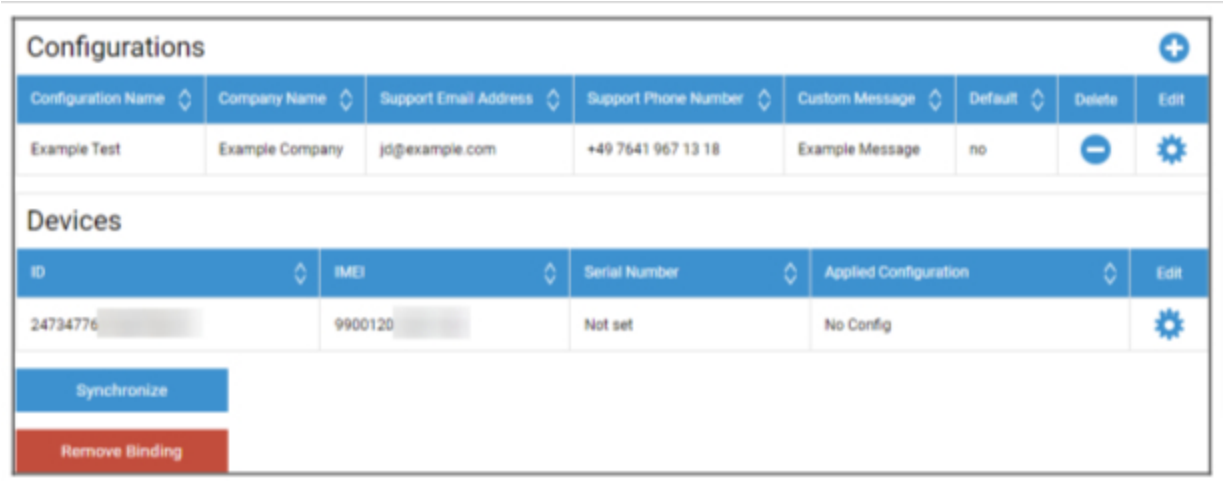
Com o Zero-Touch, podes registar facilmente os teus dispositivos sem teres de lhes tocar nem de configurar nada no próprio dispositivo. Só tens de o ligar, proceder à configuração normalmente e o dispositivo receberá todas as informações sobre como configurar e ligar ao MDM de forma totalmente automática.

Para utilizar o Zero-Touch, tens de comprar os teus dispositivos a um revendedor que suporte o Zero-Touch. O mesmo Revendedor também está a criar uma Conta para ti no Portal Zero-Touch. Contacta o teu Revendedor para obteres mais informações sobre o procedimento ou se tiveres problemas no acesso ao Portal Zero-Touch.

Clica em "Start Setup" para iniciar a configuração. Serás redireccionado para uma página de início de sessão onde tens de selecionar a tua Conta Google que tem acesso ao Portal Zero-Touch.

NOTA: É possível selecionar QUALQUER conta. Por isso, certifica-te de que seleccionas a conta correcta neste passo. Se não vires os teus dispositivos/configurações, é provável que tenhas utilizado a conta errada.

Depois de concluíres o início de sessão, terás o seguinte aspeto:



Clica no "+" para adicionar uma Configuração e preenche os campos apresentados no ecrã. Se activares a Configuração como Configuração predefinida, esta será atribuída automaticamente aos novos dispositivos. Criar ou definir uma configuração predefinida não a atribui a dispositivos já existentes.

Se um dispositivo não tiver nenhuma Configuração atribuída, será configurado como um dispositivo normal e não se ligará à MDM. Por isso, certifica-te de que os teus dispositivos têm uma configuração atribuída.

Depois de ligares a tua Conta, de os teus dispositivos estarem visíveis e de lhes teres atribuído uma Configuração, podes começar a configurar os dispositivos.

Podes adicionar os dispositivos à Lista de inscrição automática para que sejam inscritos automaticamente num grupo ou utilizador específico. Se não configuraste nada na lista Inscrição automática, os dispositivos serão inscritos no agrupamento.

Configuração do Windows

Configuração do Windows

Aqui tens a opção de ativar as seguintes configurações no teu PC com Windows 10:

Ligação DM instantânea	
Tempo de repetição inicial	Estabelece a primeira tentativa de ligação ao dispositivo, este valor aumenta exponencialmente
Tentativas de ligação	Indica quantas tentativas de ligação o cliente DM deve efetuar, durante um erro de ligação
Tempo máximo de sono	Indica o tempo máximo de espera após um erro de ligação
Primeiras tentativas de sincronização	Intervalos em que o dispositivo deve comunicar com o servidor, após a primeira ligação
Primeiro intervalo de repetição	Está relacionado com "Primeiras tentativas de sincronização" Aqui os tempos são indicados em minutos Por exemplo, em "First Sync Retries" (Primeiras tentativas de sincronização), é indicado o valor "2" e, em "First Retry Interval" (Primeiro intervalo de tentativas), é indicado o valor "4 Minutes" (4 minutos), para que o dispositivo comunique 2 vezes a cada 4 minutos, após a primeira ligação
Segunda tentativa de sincronização	Intervalos em que o dispositivo deve comunicar com o servidor, depois de completar as "Primeiras tentativas de sincronização"
Segundo intervalo de repetição	O mesmo princípio que para "First Retry Interval" - só que aqui, aplica-se a "Second Sync Retries"
Tentativas de sincronização regulares	Intervalos, com que frequência o dispositivo deve comunicar com o servidor no futuro Predefinição: "Infinito" Recomendamos que não alteres este valor, porque se introduzires "10", o dispositivo comunica com o servidor 10 vezes e depois pára.
Intervalo de repetição regular	O mesmo princípio que para "First/Second Retry Interval" - só que aqui, aplica as definições para o futuro
Intervalo de repetição regular	O mesmo princípio que para "First/Second Retry Interval" - só que aqui, aplica as definições para o futuro

ContentBox

Configuração

Aqui podes configurar a ContentBox. Podes colocar ficheiros para grupos na ContentBox que podem ser acedidos com a aplicação ContentBox no dispositivo.

Ativar ContentBox	Ativar ContentBox. Se não utilizares a ContentBox, podes poupar recursos nas máquinas OnPremise.
Utiliza a instalação externa da ContentBox	A ContentBox também pode ser operada com a tua própria Nextcloud.
URL	URL completo da entidade Nextcloud
Utilizador raiz	Utilizador raiz da conta Nextcloud
Palavra-passe de raiz	Palavra-passe de raiz da conta Nextcloud
Permissões de pasta de grupo predefinidas	Permissões de pastas de grupo predefinidas, que podem ser modificadas individualmente por grupo (em Gestão móvel)
Partilha a pasta do grupo com subgrupos	Se estiver ativo, cada subgrupo pode ler todas as pastas do grupo principal, podendo também ser configurado individualmente para cada grupo (Gestão móvel)
Permissões para subgrupos	Permissões para subgrupos pode ser configurado individualmente para cada grupo (Gestão móvel)
Permitir a partilha	Permite ao utilizador partilhar o conteúdo através de Ligações, podendo ser configurado individualmente para cada grupo
Tamanho máximo de carregamento de ficheiros em MB	Tamanho máximo de um ficheiro Padrão: 512 MB Configuração máxima: 2048
Credenciais WebDAV	
URL WebDAV	Também podes abrir a ContentBox com WebDAV. Não elimines as seguintes pastas, em circunstância alguma: /apptecgroups /apptecgroups/AppTecGroup-X
Utilizador raiz	Nome dos utilizadores raiz
Palavra-passe	Palavra-passe dos utilizadores raiz

A sincronização com a ContentBox ocorre automaticamente. Podes, no entanto, efetuar uma sincronização manual com "Synchronize ContentBox".

Além disso, aqui podes ativar/desativar a ContentBox em cada dispositivo individual.

Isto só é relevante, se não tiveres licenciado adicionalmente a ContentBox, então ainda tens acesso a 25 dispositivos com os quais podes testar a ContentBox - aqui podes ativar isto para os respectivos dispositivos.

Configuração LDAP

Visão geral do LDAP

Aqui podes estabelecer uma ligação ao teu Active Directory através de LDAP para importar em massa utilizadores e grupos. A sincronização tem de ser efectuada manualmente. Podes configurar várias ligações LDAP a diferentes sistemas ou com diferentes configurações/filtros.

Nome do servidor	O nome de exibição do servidor
Tipo	Atualmente, apenas são suportadas as Active Directories que suportam LDAP
Domínio LDAP	O domínio LDAP primário (por exemplo, exemplo.com)
Anfitrião LDAP	Só é necessário se o anfitrião LDAP não for acessível no domínio LDAP fornecido.
Porto	Deixa em branco para utilizar a porta padrão (389 ou 636 para SSL)
Nome de utilizador	Por exemplo, CN=John,OU=Users,DC=EXAMPLE,DC=COM Nota: A maioria dos sistemas exige o nome de utilizador neste formato e não aceita "John" como nome de utilizador
Palavra-passe	
Confirma a palavra-passe	
Segurança da ligação	Nota: quando utilizares SSL ou TLS, o certificado do Active Directory será verificado. Se for auto-assinado, tens de adicionar a CA de raiz ao armazenamento de confiança da máquina no local. Se estiveres na nuvem, o Active Directory tem de fornecer um certificado de confiança ou a ligação só funcionará sem encriptação
Sincronização automática.	Ativa a sincronização automática do diretório LDAP no intervalo de tempo especificado nas definições gerais de LDAP.
Base DN	Se não quiseres sincronizar todo o diretório, podes especificar uma OU aqui, por exemplo, OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Membro de	Todos os utilizadores importados serão adicionados ao grupo selecionado
Apenas utilizadores activados?	Quando ativado, o atributo userAccountControl será considerado, os utilizadores sem esse atributo não serão importados.
Filtro LDAP	Podes utilizar o Filtro LDAP para filtrar os utilizadores que são importados
Filtro Regex	Podes utilizar o filtro Regex para filtrar os utilizadores que são importados

Teste a ligação	Testa a ligação quando guarda a configuração
Repor a estrutura de directórios na sincronização?	Se for verdadeiro, todas as entradas LDAP serão movidas de volta para a sua localização original na árvore LDAP. Recomenda a ativação.
Reimportar utilizadores e grupos eliminados?	Quando ativado, os utilizadores e grupos que foram eliminados serão recriados. Recomenda a ativação.
Sincroniza as eliminações?	Quando ativado, os grupos e os utilizadores serão eliminados quando forem eliminados no servidor LDAP. Os dispositivos dos utilizadores eliminados também serão eliminados.

Abaixo da lista das tuas Configurações LDAP podes definir o período em que o sistema sincroniza automaticamente. Utiliza apenas as Configurações LDAP para sincronização automática que tenham a opção correspondente activada.

Gestão de aplicações

BD de aplicações internas

Android

Aqui podes carregar as aplicações Android que a tua empresa desenvolveu e distribuí-las posteriormente na Gestão Móvel em perfis de dispositivos ou grupos.

Tem em atenção que aconselhamos apenas a distribuição de aplicações desta forma, que não estejam disponíveis na Google Play Store.

Clica no "+" para carregar o APK de uma aplicação que queiras carregar. Atualmente, apenas o formato APK é suportado.

O limite de carregamento nos Aparelhos no Local pode ser aumentado no Passo 3 da Configuração do Aparelho. Se quiseres aumentar o limite de carregamento na nuvem, contacta o suporte para obteres mais informações.

Tem em atenção que, normalmente, os APKs são um pouco mais pequenos do que o seu conteúdo. É possível que um carregamento falhe devido a isto, uma vez que o APK é descompactado no processo. Por exemplo, é possível que um APK de 95 MB falhe com um limite de carregamento de 100 MB. Neste caso, aumenta o limite de carregamento como mencionado acima.

Aconselhamos também que primeiro movas manualmente o APK para um dispositivo de teste (por exemplo, através de USB) e tentes instalá-lo manualmente com a aplicação Ficheiros do dispositivo. Se isto não funcionar por qualquer razão, também falhará através da MDM.

Atualizar o objetivo

Com a funcionalidade "Atualizar destino" podes escolher a versão de uma aplicação que deve ser instalada ou a versão para a qual uma aplicação deve ser actualizada se activaste "Manter atualizado" para uma aplicação.

Se não tiveres selecionado um destino de atualização, será utilizada a versão mais elevada.

Tem em atenção que o Android não pode fazer o downgrade de aplicações. Tem também em atenção que o "Código da versão" determina se uma versão é superior, inferior ou igual. Por isso, certifica-te de que aumentas corretamente esta versão na tua aplicação quando crias uma atualização.

iOS

Aqui podes carregar as aplicações iOS que desenvolveste e distribuí-las mais tarde na Gestão Móvel, no teu dispositivo ou perfil de grupo.

Clica no "+" para carregar o IPA de uma aplicação que queiras carregar. De momento, apenas o formato IPA é suportado.

O limite de carregamento nos Aparelhos no Local pode ser aumentado no Passo 3 da Configuração do Aparelho. Se quiseres aumentar o limite de carregamento na nuvem, contacta o suporte para obteres mais informações.

Atualizar o objetivo

Com a funcionalidade "Atualizar destino" podes escolher a versão de uma aplicação que deve ser instalada ou a versão para a qual uma aplicação deve ser actualizada se activaste "Manter atualizado" para uma aplicação.

Se não tiveres selecionado um destino de atualização, será utilizada a versão mais elevada.

MacOS

Aqui podes carregar as MacOS Apps que desenvolveste e distribuí-las mais tarde na Gestão Móvel no teu dispositivo ou perfil de grupo.

Clica no "+" para carregar o PKG de uma aplicação que queiras carregar. Atualmente, apenas o formato PKG é suportado.

O limite de carregamento nos Aparelhos no Local pode ser aumentado no Passo 3 da Configuração do Aparelho. Se quiseres aumentar o limite de carregamento na nuvem, contacta o suporte para obteres mais informações.

Atualizar o objetivo

Com a função "Atualizar destino" podes escolher a versão de uma aplicação que deve ser instalada ou a versão para a qual uma aplicação deve ser actualizada se activaste "Manter atualizado" para uma aplicação.

Se não tiveres selecionado um destino de atualização, será utilizada a versão mais elevada.

Windows 10

Aqui podes carregar as aplicações do Windows 10 e distribuí-las mais tarde na Gestão Móvel no teu dispositivo ou perfil de grupo.

Clica no "+" para carregar a APPX, APPXBUNDLE ou MSI de uma aplicação que queiras carregar. De momento, só é suportado o formato APPX, APPXBUNDLE ou MSI.

Também podes carregar e definir dependências para uma aplicação, que serão automaticamente distribuídas e instaladas antes de instalar a aplicação desejada.

O limite de carregamento nos Aparelhos no Local pode ser aumentado no Passo 3 da Configuração do Aparelho. Se quiseres aumentar o limite de carregamento na nuvem, contacta o suporte para obteres mais informações.

Atualizar o objetivo

Com a função "Atualizar destino" podes escolher a versão de uma aplicação que deve ser instalada ou a versão para a qual uma aplicação deve ser actualizada se activaste "Manter atualizado" para uma aplicação.

Se não tiveres selecionado um destino de atualização, será utilizada a versão mais elevada.

Pacote Win32 (.exe)

Também podes distribuir ficheiros .exe/instaladores pelos teus dispositivos.

Nome do pacote	O nome que será apresentado na MDM
Descrição	Descrição apresentada na MDM
Arquivo de pacote	Só são permitidos ficheiros .zip. Coloca os ficheiros que pretendes implementar neste ficheiro zip.
Contexto de implantação	**Sistema**: O comando de instalação é executado com privilégios de sistema que são superiores aos de "Utilizador". Além disso, quando utiliza "System" (Sistema), o processo não tem IU, pelo que será silencioso e o perfil do utilizador, por exemplo, variáveis de ambiente como o %AppDat%, não está acessível. **Utilizador**: O comando de instalação tem acesso ao perfil do utilizador e pode apresentar a interface do utilizador, se necessário. Nota: Alguns processos podem estar a funcionar apenas num contexto. Por exemplo, se um software se instalar na AppData, só funcionará se seleccionares "Utilizador"
Instalar o comando	O comando utilizado para instalar o programa. Por exemplo, o comando de instalação para um ficheiro zip que contém "setup.exe" na sua raiz, que suporta o parâmetro "/s" para uma instalação silenciosa, o comando de instalação seria "setup.exe /s". Tem em atenção que um software diferente pode ter parâmetros diferentes.
Comando de desinstalação	O comando a executar para desinstalar o software através da MDM. Normalmente, aponta para o desinstalador. Por exemplo, "C:\Program Files\ExampleSoftware\uninstall.exe".
Requisitos	
Nota: Todos os requisitos definidos têm de ser cumpridos para que o software seja instalado. Caso contrário, não será instalado. Alguns campos podem ser obrigatórios. Se não for definido qualquer valor para um requisito, este será ignorado.	
Arquitetura do SO	Arquitetura do SO
Versão mínima do SO	Versão mínima do SO
Espaço livre mínimo no disco (MB)	Espaço livre mínimo no disco (MB)
Memória física mínima (MB)	Memória física mínima (MB)

Número mínimo de processadores lógicos	Número mínimo de processadores lógicos
Velocidade mínima da CPU (MHz)	Velocidade mínima da CPU (MHz)
Requisitos adicionais	Também podes definir regras manualmente ou carregar um script aqui para executar verificações de requisitos adicionais, se quiseres.
Regras de deteção	
Método de deteção	Aqui podes definir como detetar se a aplicação está instalada no dispositivo. Os comandos de instalação só serão executados quando estas regras detectarem que a aplicação NÃO está instalada. Os comandos de desinstalação só são executados quando estas regras detectam que a aplicação não está instalada. **Define regras manualmente**: Permite-te definir manualmente uma ou mais regras para verificar, por exemplo, se um determinado ficheiro, pasta, MSI ou chave de registo está presente. Se todas as regras de deteção fornecidas forem verdadeiras, a aplicação será considerada presente. **Usa o script**: Carrega o teu próprio script com as tuas próprias verificações. Se o script devolver "$TRUE", a aplicação será considerada presente.
Regras de deteção	

Definições da aplicação

Definições da aplicação iOS

Aqui podes definir as definições predefinidas para adicionar uma aplicação às aplicações obrigatórias ou à loja de aplicações empresariais.

Nota: Isto apenas define o que é selecionado por predefinição ao adicionar aplicações. Isto NÃO altera as definições existentes para as aplicações que já foram adicionadas às aplicações obrigatórias ou à loja de aplicações empresariais.

Mantém-te atualizado	Mantém automaticamente a aplicação actualizada. Tem em atenção que pode demorar até 7 dias após o lançamento de uma atualização até que a aplicação seja actualizada.
Ultrapassa quando não é gerido	Se uma aplicação já estiver instalada como não gerida (pelo utilizador), a aplicação será ultrapassada e gerida pela MDM.
Remove a aplicação quando o perfil MDM é removido	Desinstala a aplicação quando a MDM é removida.
Evita a cópia de segurança dos dados da aplicação	Impede a cópia de segurança dos dados da aplicação.

Definições da aplicação Android

Aqui podes definir as definições predefinidas para adicionar uma aplicação às aplicações obrigatórias ou à loja de aplicações empresariais.

Nota: Isto só define o que está selecionado por defeito quando adicionas. Isto NÃO altera as definições das aplicações que já foram adicionadas às aplicações obrigatórias ou à loja de aplicações empresariais.

Mantém-te atualizado	Mantém automaticamente a aplicação actualizada. Apenas disponível para aplicações internas.
Atualização do cliente EMM do Controlled AppTec360	Se estiver ativado, os administradores podem especificar o destino da atualização para o AppTec360 EMM Client. Uma lista de todas as versões disponíveis do Cliente EMM AppTec360 será apresentada em "Definições Gerais" → "Gestão de Aplicações" → "BD de Aplicações Internas" → "Android".

Aplicações de terceiros

Android

Aqui podes definir o teu código de ativação para o Ikarus.

Define esta opção como "Utilizar código de ativação" e introduz o teu código de ativação aqui.

Nota: Depois de introduzires o Código e guardares, o Código ainda não é adicionado ao perfil que é enviado para o dispositivo. Tens de efetuar qualquer alteração no teu perfil para que o código seja adicionado ao perfil. Por exemplo, altera qualquer interrutor no perfil de desligado → ligado → desligado - Guardar → Atribuir agora.

iOS

Aqui podes introduzir a tua licença SecurePIM. Depois de introduzir a licença, prime "Save Changes" (Guardar alterações) e podes utilizar as opções do SecurePIM.

VPP / KNOX Premium

O Programa de Compra em Volume (VPP) da Apple permite-te distribuir facilmente aplicações pagas e gratuitas para os teus dispositivos. Isto é altamente recomendado, uma vez que não precisas de um ID da Apple nos dispositivos, os utilizadores não têm de confirmar a instalação (supervisionada), os utilizadores não terão de introduzir a palavra-passe do ID da Apple e podes facilmente distribuir aplicações pagas sem as comprar novamente em cada dispositivo.

Para utilizar o VPP, tens de te registar no Apple Business Manager.

Licenças VPP

Aqui podes ter uma visão geral das tuas aplicações VPP, quantas licenças são utilizadas e quantas estão disponíveis.

Clicando na Roda, poderás ver quais os dispositivos que têm uma Licença atribuída e qual o Estado dessa Atribuição.

Clicando em actualiza a Cache VPP que compara as Licenças atribuídas no MDM com as Licenças atribuídas no lado da Apples. Isto pode resolver problemas de licença em alguns casos.

Token VPP

Aqui podes carregar o teu Token VPP, que pode ser encontrado no Apple Business Manager em Definições → Apps & Books. Podes carregar vários Tokens VPP.

Para renovar um Token, basta descarregar um novo no Apple Business Manager, clicar na roda "Editar" e carregar o novo Token.

O "Modo VPP" decide como é tratada a atribuição de licenças. Dependendo do teu cenário, tens de utilizar modos diferentes:

A opção "Device based" tem de ser utilizada ao registar os dispositivos através de código QR, ligação, Apple Configurator ou DEP.

"Baseado no utilizador" é necessário se os Dispositivos estiverem inscritos com a Inscrição de utilizador ou como iPad partilhado.

Se activares a "Gestão automatizada de licenças", os utilizadores que forem movidos de um grupo para outro serão automaticamente atribuídos a licenças Apple VPP com base no perfil de grupo para o qual são movidos.

As licenças Apple VPP existentes do grupo de onde foram transferidas não serão revogadas.

Aos novos utilizadores adicionados a um grupo serão automaticamente atribuídas licenças Apple VPP com base no respetivo perfil de grupo.

KNOX Premium Key

Aqui podes introduzir a tua chave KNOX Premium para utilizar o Samsung KNOX Container.

Tem em atenção que isto já não é suportado desde o Android 10. Em vez disso, utiliza o Android Enterprise Container.

Definições da App Store

Região e língua

Aqui podes definir o idioma e a região predefinidos para a Pesquisa de aplicações na Gestão de aplicações.

Tem em atenção que a definição para o iTunes também define a forma como o sistema obtém informações sobre determinadas aplicações. Se encontrares aplicações nas tuas listas que são apresentadas de uma forma estranha (por exemplo, ícone em falta), talvez tenhas definido uma região onde a aplicação específica não está disponível.

AE Play Store

Aqui podes encontrar todas as opções da Play Store para dispositivos Android Enterprise para aprovar aplicações, carregar as tuas próprias aplicações na Play Store ou criar as tuas próprias aplicações Web.

Aplicações aprovadas

Aqui podes ter uma visão geral de todas as aplicações que aprovaste.

Aplicações da Play Store

Isto irá carregar um iFrame que mostra a Play Store. Procura a aplicação que quiseres, clica nela e aprova-a. Ao aprovares a aplicação, também podes definir que a aprovação seja revogada se as permissões necessárias forem alteradas. Recomendamos que deixes estas definições por defeito quando aprovares as aplicações.

Depois de uma aplicação ter sido aprovada, podes adicioná-la aos teus perfis.

O botão "Aprovar" mudará para "Revogar aprovação" após a aprovação, para que possas sempre remover as aplicações se já não precisares delas.

Aplicações privadas

Aqui podes carregar a tua própria aplicação como uma aplicação privada para a Google Play Store. Isto permite-te distribuir a aplicação através dos Serviços da Google e actualizá-la através deles. Isto também tem a vantagem de as tuas próprias aplicações poderem ser instaladas sem a confirmação do utilizador, que normalmente é necessária.

Aplicações Web

Aqui podes criar Web Apps, que são ligações a determinadas páginas Web que podem ser atribuídas como Apps.

Também podes atribuir-lhe um ícone personalizado e definir melhor a forma como é apresentado.

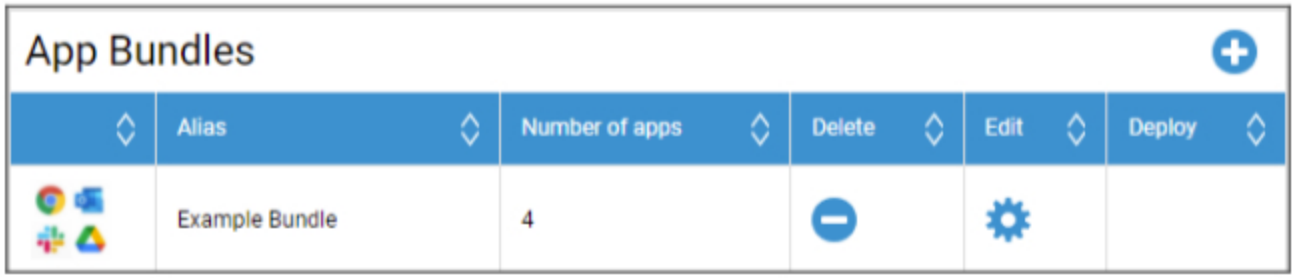
Layout da loja

O esquema da loja define a forma como as aplicações são apresentadas na Play Store ou se são de todo apresentadas.

Tem em atenção que, se quiseres mostrar aplicações na Play Store para o utilizador instalar manualmente, estas têm de ser adicionadas aqui no Layout **E** no perfil para a Play Store da empresa. Se adicionares uma aplicação apenas a uma delas, esta não será apresentada.

Pacote de aplicações

Com os pacotes de aplicações, podes definir grupos de aplicações que podem ser atribuídos a perfis de dispositivos ou de grupos com um clique.



Clica no "+" para criar um novo Pacote de aplicações. Depois de criares um Pacote de aplicações, podes clicar em "Editar" para adicionar aplicações de várias origens ao Pacote.

Podes adicionar um pacote aos perfis como qualquer outra aplicação. Ao adicionares aplicações, terás um separador extra chamado "Pacotes de aplicações" onde tens os teus pacotes.

Se fizeres alguma alteração a um pacote de aplicações, aparece um botão na coluna "Implementar". Isto permitir-te-á enviar estas alterações para todos os perfis que contenham este pacote. Por isso, não te esqueças de que tens de fazer isto manualmente depois de adicionares ou removeres aplicações de um pacote.

Controlo remoto

TeamViewer

Conector TeamViewer

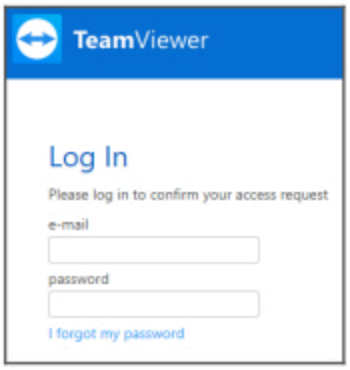
Nota: Na versão de avaliação gratuita da nossa versão na nuvem, não podes ligar a tua conta TeamViewer. Em vez disso, terás uma conta de demonstração gratuita ligada automaticamente.

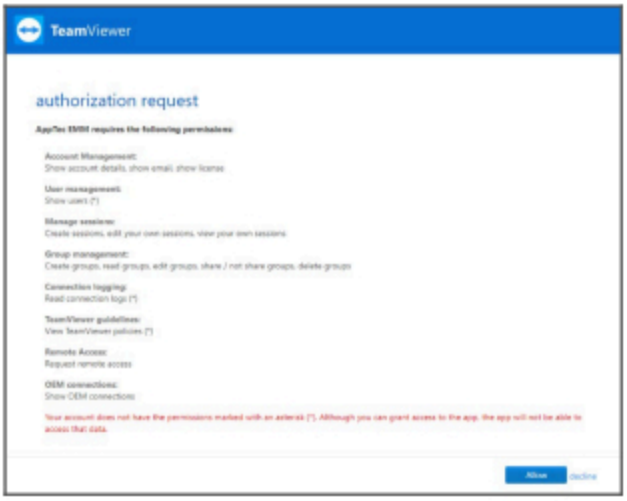
Vai a Definições Gerais -> Controlo Remoto -> TeamViewer. Aqui podes associar a tua conta TeamViewer à consola ou ver informações sobre a tua conta atualmente ligada. Também podes ver todas as sessões atualmente activas se fores a "Sessões activas".

Para associar a tua conta, clica em "Iniciar configuração".

Se o fizeres, serás encaminhado para uma nova página onde terás de iniciar sessão com a tua conta TeamViewer.

Depois de iniciares a sessão, autorizaste a AppTec360 MDM a utilizar esta conta. Depois de confirmares, tens de esperar alguns segundos e a conta fica ligada.


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password


TeamViewer
authorization request

Instalar o TeamViewer QuickSupport

Adiciona a aplicação "TeamViewer QuickSupport" às aplicações obrigatórias do perfil do teu dispositivo ou do perfil do grupo e clica em "Atribuir agora". Espera até a aplicação estar instalada no dispositivo.

Se tentares aceder a um dispositivo no qual a aplicação não está instalada, esta será instalada ou ser-te-á pedido que a instales, dependendo da configuração do dispositivo.

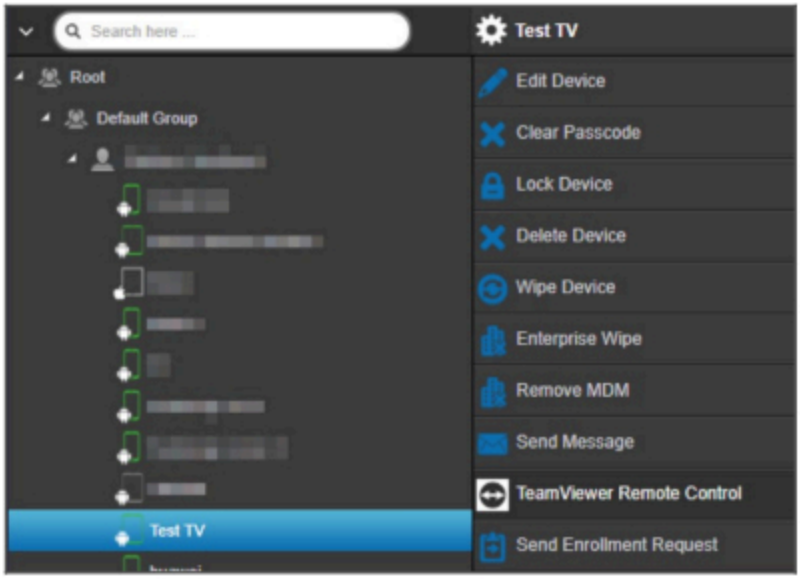
Controla o teu dispositivo à distância

Para controlar remotamente o teu dispositivo, selecciona o dispositivo, clica na roda e escolhe "TeamViewer Remote Control"

Se já existir uma sessão ativa, podes utilizar a sessão antiga ou criar uma nova.

Confirma que pretendes criar uma nova sessão do TeamViewer.

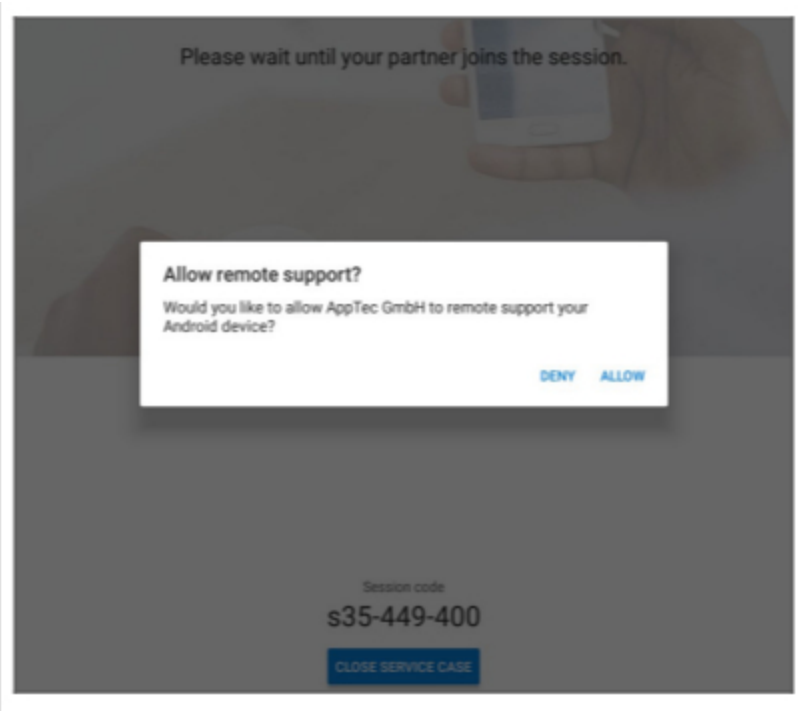
Passados alguns segundos, receberás uma ligação para a tua sessão TeamViewer. Podes clicar em "Iniciar" para abrir esta ligação numa nova janela.


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

Esta ligação abrirá o TeamViewer instalado e ligar-te-á ao teu dispositivo.

Agora tens de confirmar a ligação no próprio dispositivo para o controlares à distância.

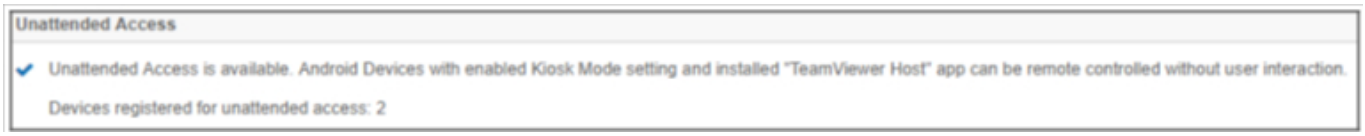


Se estiveres a utilizar o iOS, receberás uma mensagem no Cliente MDM AppTec360. Com essa ligação, o dispositivo entra na sessão remota. Dependendo das definições de notificação do dispositivo, é possível que não recebas uma notificação e tenhas de abrir manualmente o Cliente MDM AppTec360.

Em alguns dispositivos Android (por exemplo, Samsung), é necessário instalar uma aplicação adicional como complemento. A aplicação TeamViewer no dispositivo informa-te sobre isso, se tal for necessário no teu dispositivo.

Acesso sem vigilância

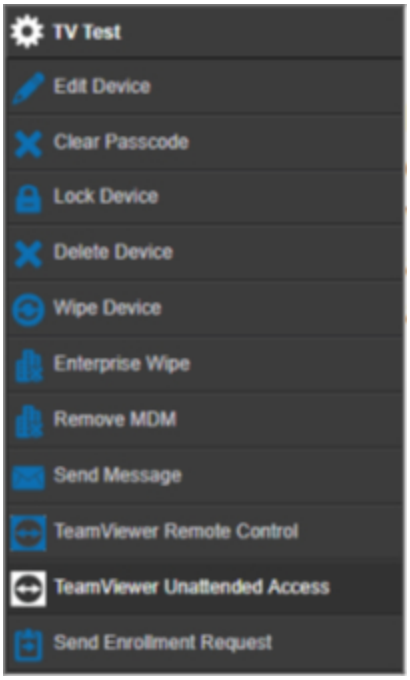
Nota: O acesso não assistido só é possível em dispositivos Android.



Só podes ligar aos teus dispositivos, sem aceitar a ligação no dispositivo, se a tua conta TeamViewer estiver a utilizar uma licença "Tensor" ou "Corporate".

Podes verificar isto, depois de associares a tua conta, em "Definições gerais"

Para utilizares o acesso não assistido, tens de instalar a aplicação "TeamViewer Host" e ativar "Enable Unattended Access" (Ativar acesso não assistido) em "Kiosk Mode & Launcher" (Modo de quiosque e iniciador) no teu perfil. Tem em atenção que isto só é possível se estiveres a utilizar o Modo Quiosque.



Agora podes selecionar o acesso não assistido se seleccionares o teu dispositivo e clicares na roda. Isto irá ligar-te ao teu dispositivo sem qualquer necessidade de confirmação no próprio dispositivo. Tem em atenção que pode demorar alguns momentos até obteres a ligação para acederes ao teu dispositivo.

Splashtop

Se activares a opção Splashtop, verás as opções de configuração do Splashtop nos teus perfis.

Para utilizares o Splashtop, tens de definir o Splashtop Streamer (com.splashtop.streamer.csrs) como aplicação obrigatória no teu perfil. Depois disso, podes ativar a configuração do Splashtop no teu perfil em "Controlo Remoto". Ao ativar esta opção, configura a aplicação Splashtop Streamer. Se estiveres a utilizar o Splashtop Streamer mas não em combinação com o MDM, deves deixar esta opção desligada.

No teu perfil, em "Controlo remoto", também tens de definir um código de implementação. Vai a https://my.splashtop.com e entra na tua conta Splashtop. Clica em "Adicionar computador" e copia o código de implantação de 12 dígitos da página resultante.

Sem o código de implantação, o controlo remoto NÃO é possível.

Depois de o fazeres, podes clicar com o botão direito do rato no teu dispositivo e iniciar uma sessão remota clicando em "Splashtop Remote Control"

Gestão de cartões SIM

Importação em massa de CSV

Mostra uma visão geral dos teus Sim Cards atribuídos e todas as informações sobre eles. Isto ajuda-te a ter toda a informação, não só sobre os teus dispositivos, mas também sobre os teus Sim Cards num único sistema.

OBSERVAÇÃO: Trata-se de uma gestão/documentação manual. Não é possível obter estes dados automaticamente dos dispositivos devido aos mecanismos de privacidade/segurança dos sistemas operativos.

Também podes exportar e importar esta lista como CSV.

Transportadora e tarifa

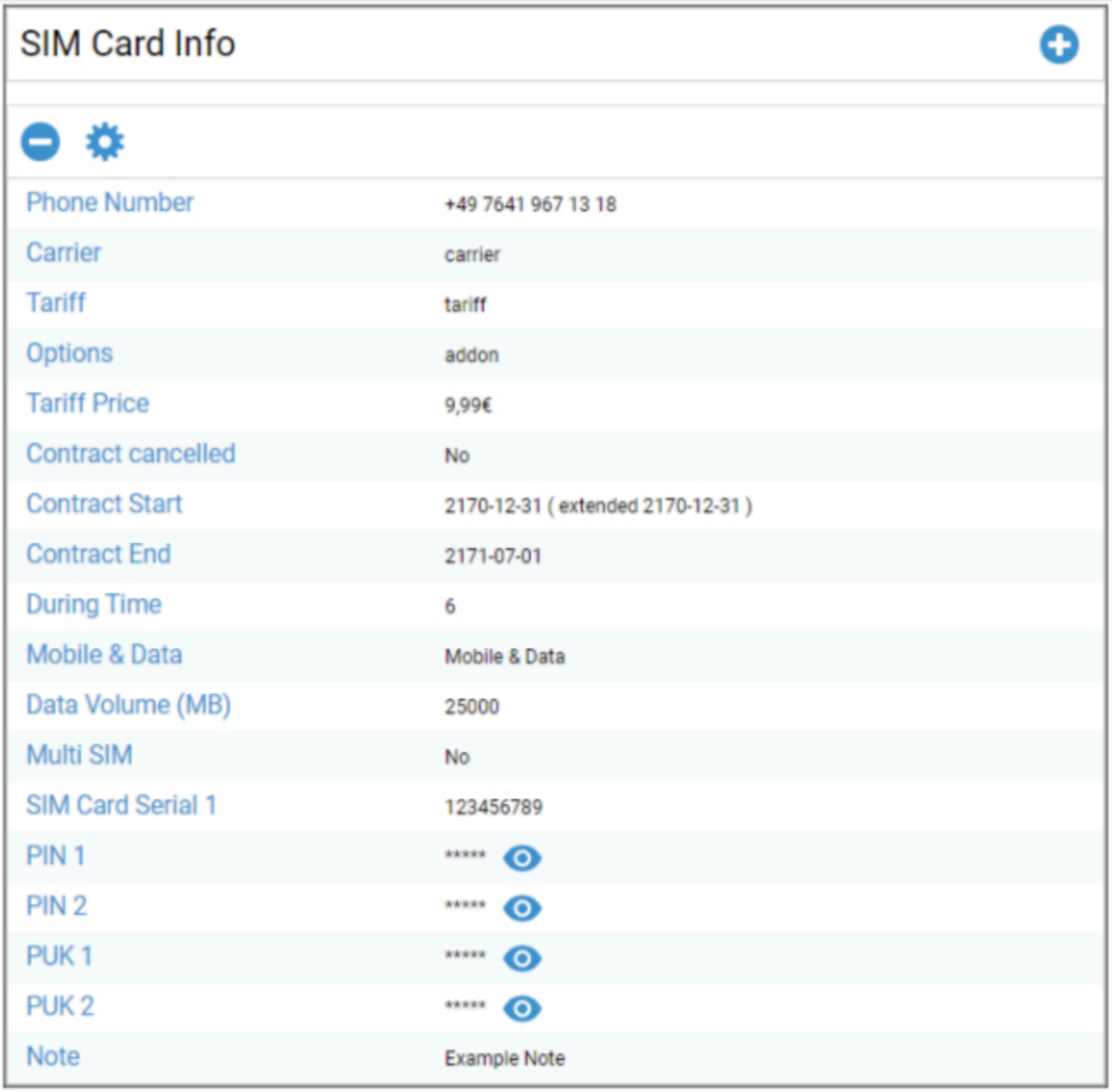
Para adicionar um cartão SIM, clica primeiro no botão para adicionar uma ou várias operadoras.

Depois, clica no "+" em "Informações tarifárias" para adicionar uma tarifa a uma transportadora.

Opcionalmente, podes adicionar Add-Ons opcionais abaixo se tiveres algo deste género.

Isto preparou tudo o que precisas para adicionar um cartão SIM real. Os cartões SIM estão atualmente atribuídos a um utilizador. Por isso, vai à Gestão de telemóveis, selecciona um utilizador e vai a "Visão geral do cartão SIM".

Aqui podes ver os cartões SIM destes utilizadores. Se houver um, podes editá-lo ou removê-lo. Os utilizadores podem ter vários cartões SIM.

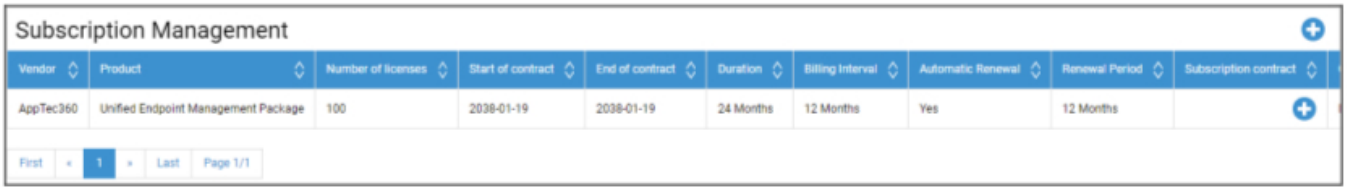


Clica no "+" para adicionar um Sim Card e adiciona todas as informações de que necessitas. Estes Cartões Sim também serão listados na lista de todos os teus Cartões Sim em Definições Gerais → Gestão de Cartões Sim.

Gestão de assinaturas

Gestão de assinaturas

Aqui podes documentar as assinaturas em curso, os seus detalhes e também armazenar diferentes ficheiros, por exemplo, o contrato assinado, a carta de rescisão, etc. Também podes definir lembretes que te recordam por correio antes de a subscrição terminar e que talvez se prolongue automaticamente.



Clica no "+" na parte superior para adicionar uma subscrição. Podes adicionar o número de subscrições que quiseres.

Clica no "+" nos diferentes campos para carregar ficheiros relativos a esta Assinatura. Tecnicamente, podes carregar qualquer tipo de ficheiro, mas tem em atenção que nem todos os tipos de ficheiros podem ser pré-visualizados no browser.

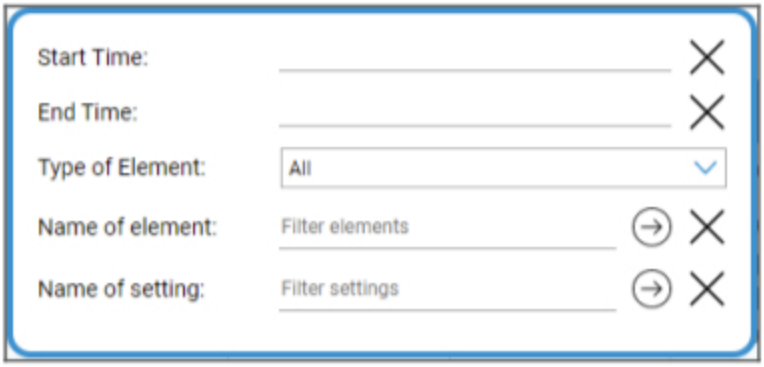
Registo geral de auditoria

Registo de auditoria

Aqui tens um registo de auditoria geral que mostra todas as alterações feitas. Enquanto o Registo de Auditoria de um utilizador ou grupo mostra apenas as alterações efectuadas por esse utilizador ou grupo, este mostra TODAS as alterações efectuadas em qualquer parte da consola.

Podes ver o que foi alterado, por quem, quando e onde. Em alguns casos, também podes alargar a Entrada para veres mais pormenores.

É possível clicar no utilizador ou na entrada em "Caminho / Tipo" para chegar ao local onde foi feita a alteração.



No canto superior direito, também podes definir um filtro que pode ajudar a encontrar determinadas alterações num ambiente onde estão a ocorrer muitas alterações.

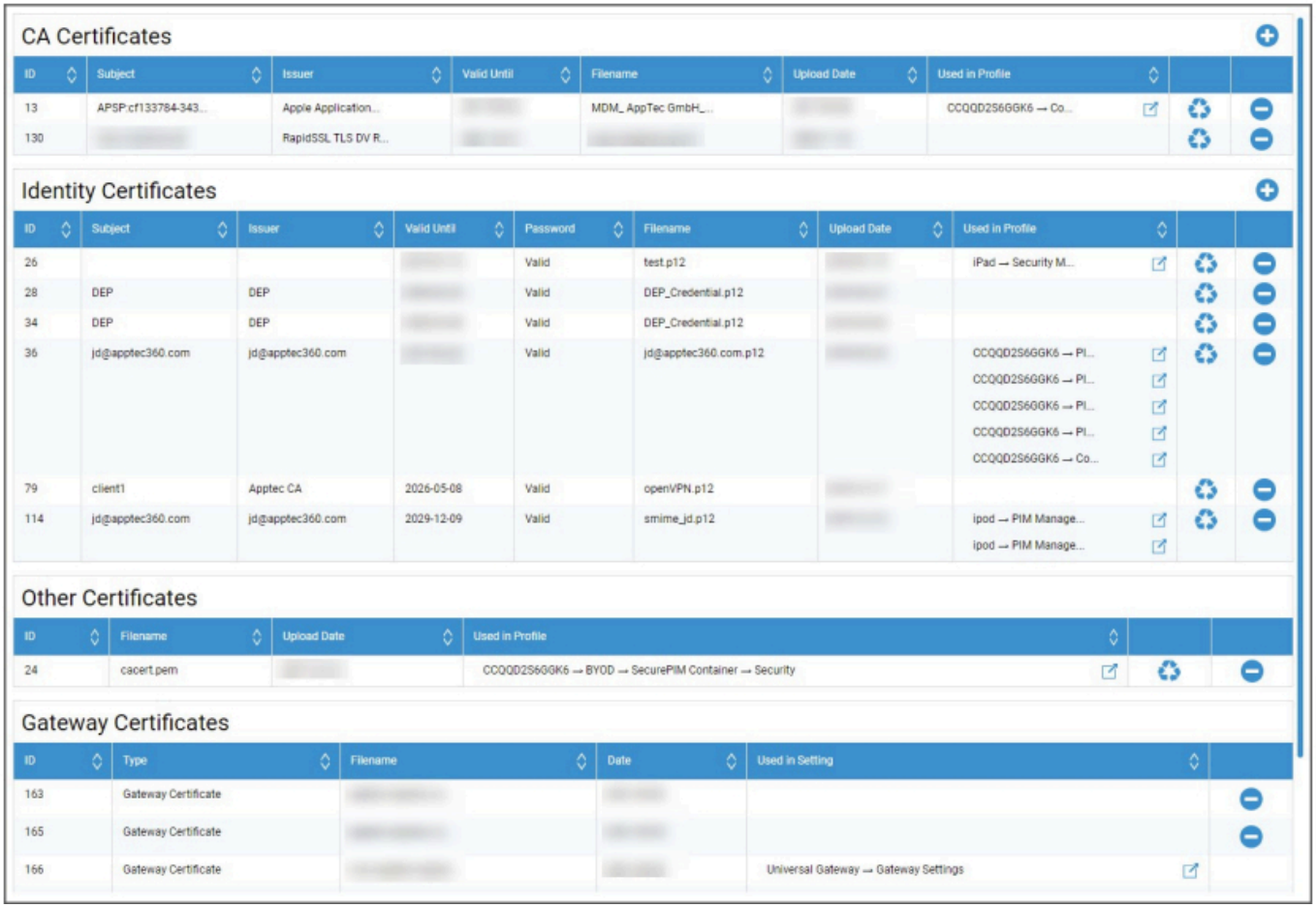
Definições do registo de auditoria

"Período de retenção do registo de auditoria" define durante quanto tempo os registos de auditoria devem ser retidos antes de serem eliminados.

Gestão de certificados

Aqui terás uma visão geral de todos os certificados carregados e utilizados na Consola. Esta é apenas uma visão geral. A configuração real, por exemplo, dos certificados Wi-Fi, continua a ser feita no perfil, no local correspondente.

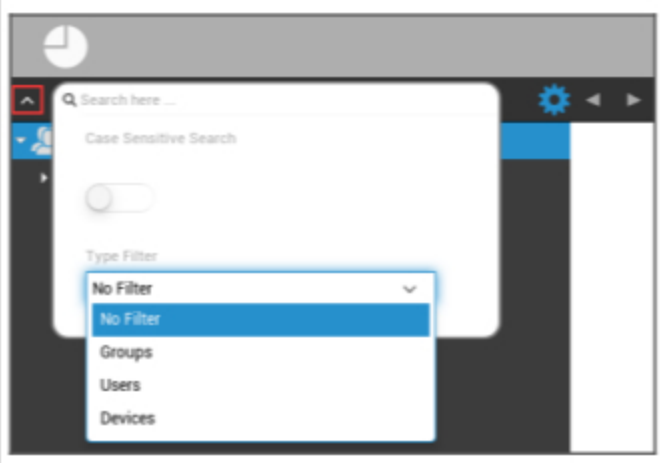
Aqui também podes remover ou atualizar certificados, o que se reflectirá automaticamente nos perfis afectados. Clica nas informações em "Utilizado no perfil" para veres onde é que um certificado ainda está atribuído.



Gestão móvel

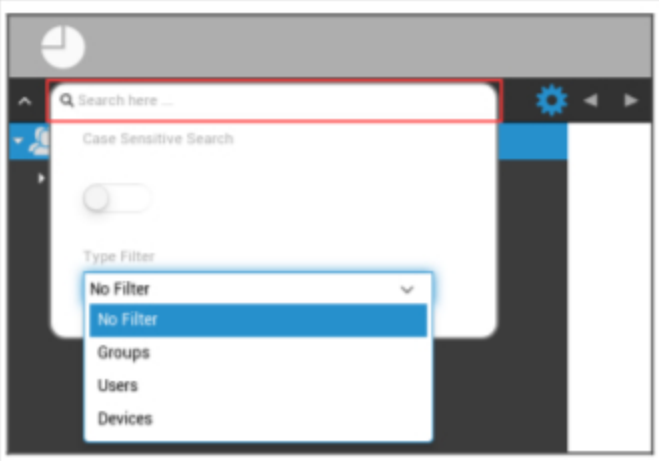
Ecrã de gestão móvel

Filtro do dispositivo



Com um clique no canto superior esquerdo do ecrã, podes encontrar uma variedade de filtros para a apresentação de dispositivos.

Janela de pesquisa



A janela de pesquisa permite-te pesquisar todos os dispositivos e/ou utilizadores com uma palavra-chave específica.

Opções de engrenagem

Depois de clicares no respetivo símbolo, é apresentada uma lista de opções que estão disponíveis.

Estes mudam com cada janela atual e são explicados nos respectivos capítulos.

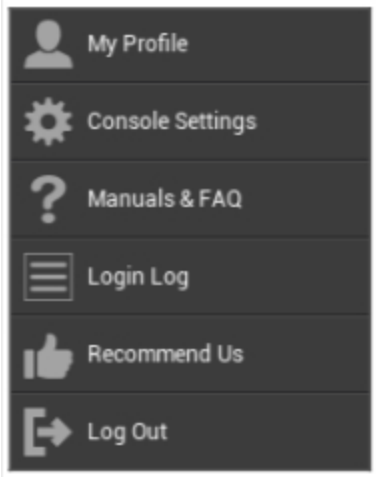
Setas de navegação

Com um clique na seta para a esquerda, serás levado para a página anterior.

Depois, com um clique na seta para a direita, serás levado para a página que acabaste de deixar.

Definições da conta de administração

Se clicares no endereço de correio eletrónico, como se vê acima, aparece o seguinte menu:



O meu perfil	Edita os detalhes da conta de administrador
Definições da consola	Configura as definições da consola para a conta Admins
Manuais e FAQs	Vê a página "Manuais e FAQ" em "Definições gerais"
Registo de início de sessão	Acede ao "Registo de acesso"
Recomenda-nos	Vê a página "Recomenda-nos" em "Definições gerais"
Terminar sessão	Termina a sessão na consola MDM

Informações do utilizador

Aqui podes editar os detalhes da conta do administrador atualmente com sessão iniciada.

Nome de utilizador	Nome de utilizador e/ou endereço de correio eletrónico da conta
Nome	Nome próprio do administrador
Último nome	Apelido dos administradores
Nome de utilizador	Nome de login dos administradores
Endereço de correio eletrónico	Endereço de correio eletrónico dos administradores
Endereço de correio eletrónico alternativo	Endereço de correio eletrónico alternativo dos administradores
Imagem	Foto do perfil
Número de telefone	Número de telefone do administrador
Número de telemóvel	Número de telemóvel do administrador
Extensão do telefone	Extensão do telefone
Localização	Localização
Posição	Posição na empresa
Grupo de utilizadores	Selecciona o grupo de utilizadores ao qual pretendes atribuir a conta de administrador
Comenta	Introduzir um comentário
Introduzir a nova palavra-passe	Introduz a palavra-passe para uma alteração da palavra-passe
Repete a nova palavra-passe	Repete a nova palavra-passe para confirmar

Tem em atenção que o acesso de administração também pode ser arquivado como uma conta de utilizador local na estrutura hierárquica. Sem o estabelecimento de um administrador adicional, este não deve ser suprimido!

Definições da consola

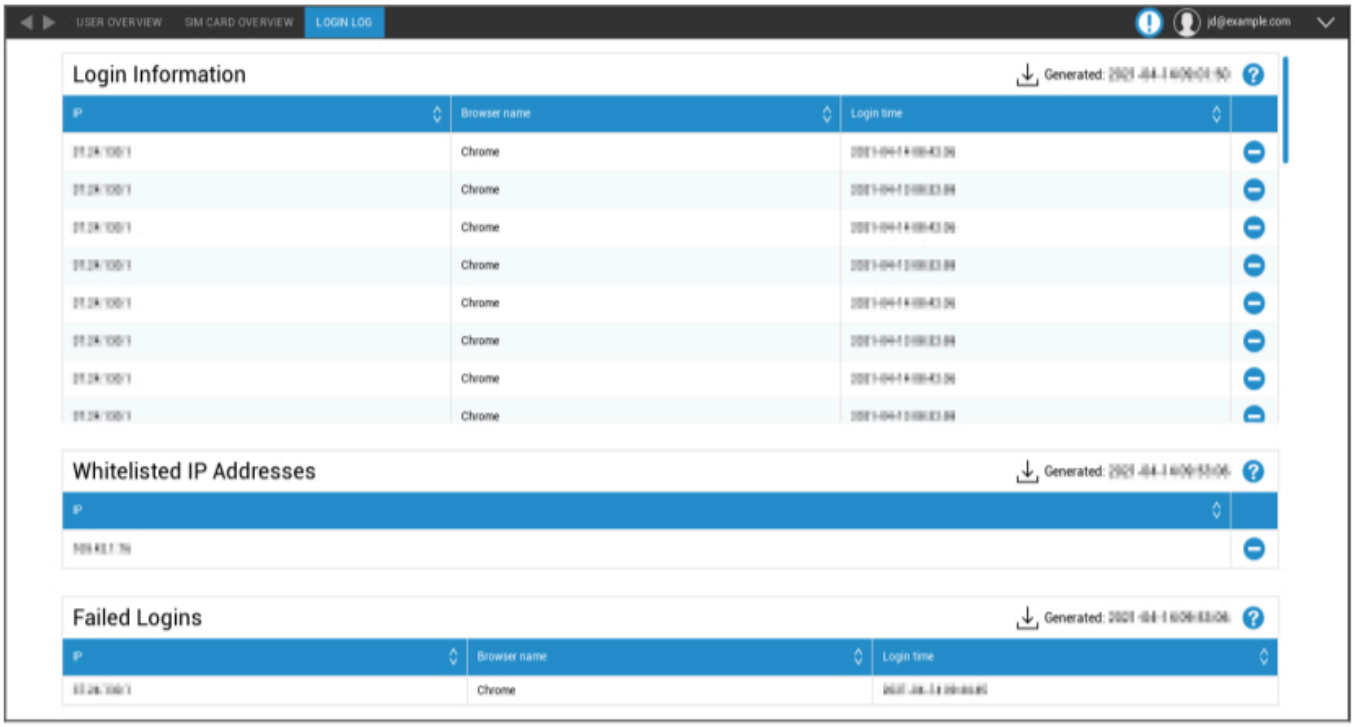
Aqui podes configurar as seguintes definições da consola para a conta Admins:

Opções de visualização do utilizador do diretório	Define como os utilizadores devem ser etiquetados na árvore
Opções de visualização do dispositivo de diretório	Define como os dispositivos devem ser etiquetados na árvore
Tempo limite da sessão	Se o utilizador não fizer nada durante o tempo especificado, o utilizador será desconectado. O valor predefinido é 60 minutos. Termina a sessão e volta a iniciar sessão depois de alterares esta definição.
Fuso horário	Escolhe o fuso horário que é utilizado
Formato da hora	Escolhe a forma como os carimbos de data/hora devem ser apresentados
Idioma da consola	Escolhe o idioma em que a consola deve ser apresentada. Podes consultar o inglês e o alemão.
Cor principal	Podes definir uma cor que será utilizada como base para o esquema de cores da consola. Podes utilizar o seletor de cores ou introduzir uma cor em notação HTML HEX. Os formadores RGB como "rosa", "amarelo" também funcionam.
Guardar comando	A combinação de teclas para ativar uma gravação sem premir o botão "Gravar".
Utiliza a autenticação de dois factores	Ativa a utilização da autenticação de dois factores ao iniciar sessão. Receberás um e-mail após o início de sessão com um código que terás de introduzir para iniciar sessão.
Tempo limite da autenticação de dois factores	Define um período de tempo durante o qual não te será pedida uma autenticação de dois factores após uma autenticação bem sucedida.
Envia o código de verificação através de	O código de verificação será enviado para as opções seleccionadas. A mensagem do dispositivo será mostrada na AppTec360 MDM App em todos os dispositivos Android e iOS que te pertencem.
Envia uma mensagem de início de sessão após o início de sessão	Se ativado, será enviado um e-mail para cada início de sessão de um endereço IP que não esteja na lista branca.

	O e-mail contém informações sobre o início de sessão (por exemplo, IP, Browser).

Registo de início de sessão

Aqui podes ver informações sobre os logins da conta de administrador atualmente iniciada.



Informações de início de sessão	Uma lista que contém os logins da conta de administrador atualmente iniciada que foi registada pela consola. Esta lista mostra todos os teus inícios de sessão bem sucedidos nos últimos 30 dias.
Endereços IP da lista branca	Esta é a lista de todos os teus endereços IP da lista branca. Se iniciares sessão a partir de um IP que esteja listado aqui, não receberás a mensagem de início de sessão. Podes adicionar um endereço IP a esta lista clicando no botão junto a uma entrada na lista "Informações de início de sessão" acima. Podes remover um endereço IP desta lista clicando no botão junto a uma entrada nesta lista ou na lista "Informações de início de sessão" acima.
Logins falhados	Esta é uma lista de todas as tentativas de início de sessão falhadas nos últimos 30 dias. Se não conseguires introduzir a palavra-passe correcta pelo menos 3 vezes em 20 minutos, aparecerá uma entrada nesta lista. Também serás informado por e-mail das tentativas de início de sessão falhadas.

Administração da empresa (nó-raiz) na gestão móvel

Quando chegares ao Root-Node (primeiro grupo), podes efetuar uma série de configurações para a tua empresa, no que diz respeito ao Mobile Management.

Criar um subgrupo	Cria um subgrupo
Renomear o nó raiz	Renomear o nó-raiz (por exemplo, o nome da tua empresa)
Inscrição em massa	Inscreve vários dispositivos/utilizadores ao mesmo tempo
Atribuição de massa	Atribui um perfil para os respectivos grupos, com um só olhar
Administração rápida de aplicações	Envia pedidos de (des)instalação de uma aplicação para os dispositivos dos respectivos grupos
Importação de utilizadores CSV	Importar utilizadores do CSV para o respetivo grupo

Criar um subgrupo

Com "Criar um subgrupo" podes criar um subgrupo adicional.

Podes estabelecer em que grupo o subgrupo deve ser atribuído.

(Por defeito, é criado um novo grupo que é atribuído como um subgrupo no nó raiz)

Renomear o nó raiz

Aqui podes mudar o nome da tua raiz. É comum, neste caso, utilizar-se o nome da empresa.

Inscrição em massa

Com o "Registo em massa" podes registar vários dispositivos e utilizadores.

Podes selecionar diretamente a forma como o utilizador deve receber a inscrição (eMail; eMail alternativo; SMS)

Dependendo do dispositivo que o utilizador vai receber (iOS, Android, Windows Phone), podes marcá-lo diretamente aqui.

A distinção entre um Smartphone ou um Tablet também pode ser configurada aqui, que terás de selecionar corretamente, com uma marca de verificação.

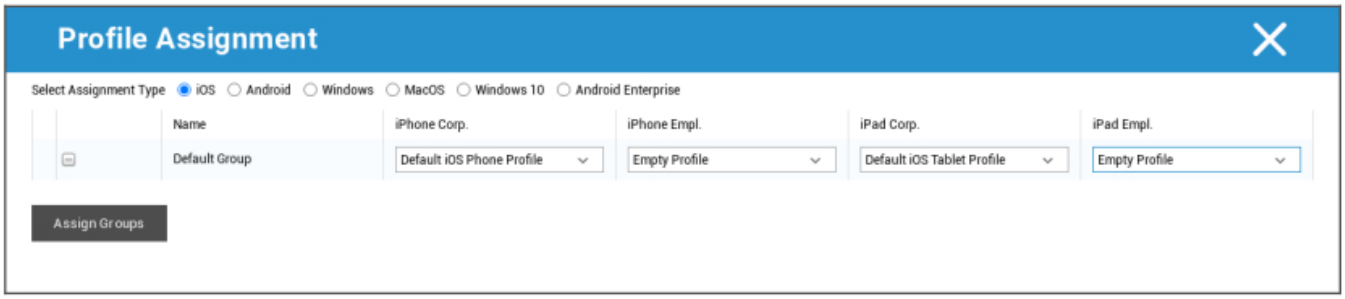
Como passo final, podes determinar se o respetivo dispositivo é empresarial ou privado (BYOD).

Com a opção "Exportar como CSV", podes exportar as informações como um ficheiro de dados CSV. Em contrapartida, também podes importar o ficheiro de dados CSV com "Importar CSV", o ficheiro deve ser parecido com o exemplo abaixo:

Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;

Atribuição de massa

Em Atribuição em massa, podes atribuir um perfil a todos os grupos, que estão divididos em iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

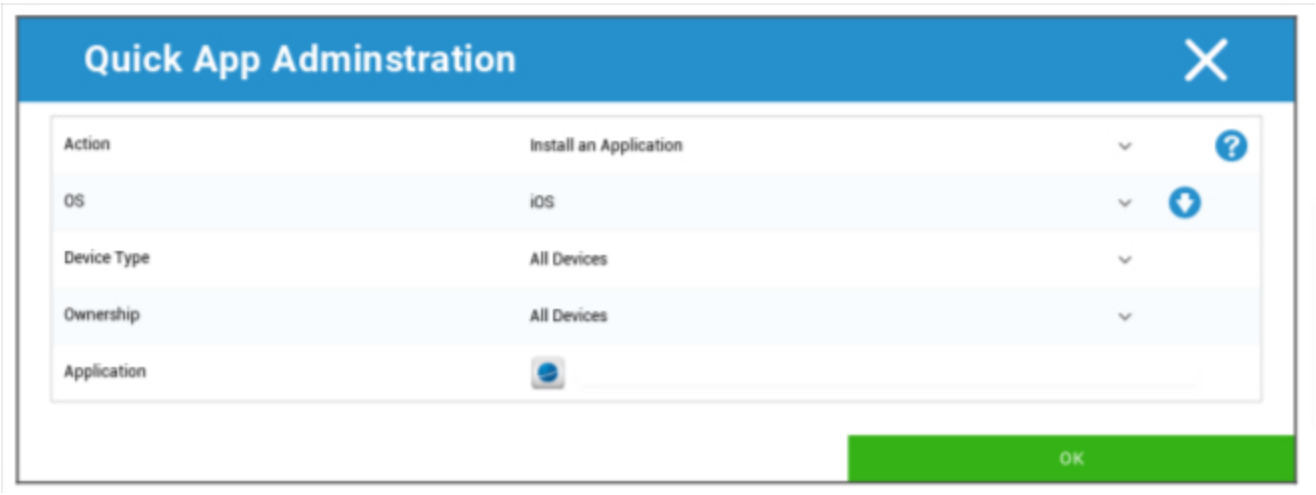


Windows - MacOS - Windows 10 - Android Enterprise

Administração rápida de aplicações

Em Administração rápida de aplicações, podes enviar pedidos de instalação ou desinstalação de uma aplicação específica para um SO à tua escolha.

Também podes definir se o pedido deve ser enviado para todos os tipos de dispositivos do SO selecionado ou apenas para um tipo de dispositivo específico.



Importação de utilizadores CSV

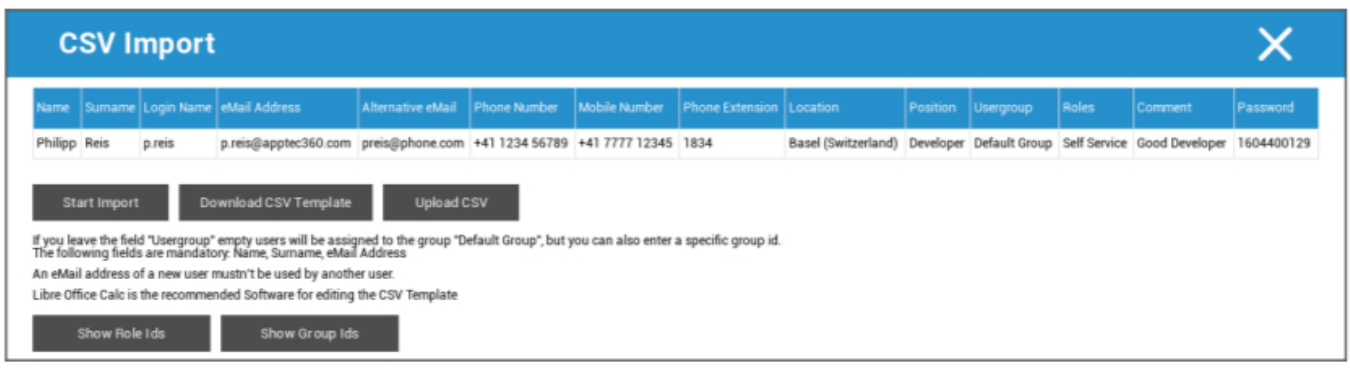
Importa utilizadores do CSV para o respetivo grupo.

Com "Descarregar modelo CSV", podes exportar um ficheiro de modelo CSV, que pode ser preenchido (ou pode ser utilizado como referência).

Também podes usar as opções "Show Role Ids" e "Show Group Ids" como referência para criar o teu próprio ficheiro CSV.

O ficheiro CSV pode ser carregado para a MDM com "Upload CSV".

Como passo final, podes iniciar a importação clicando em "Iniciar importação".



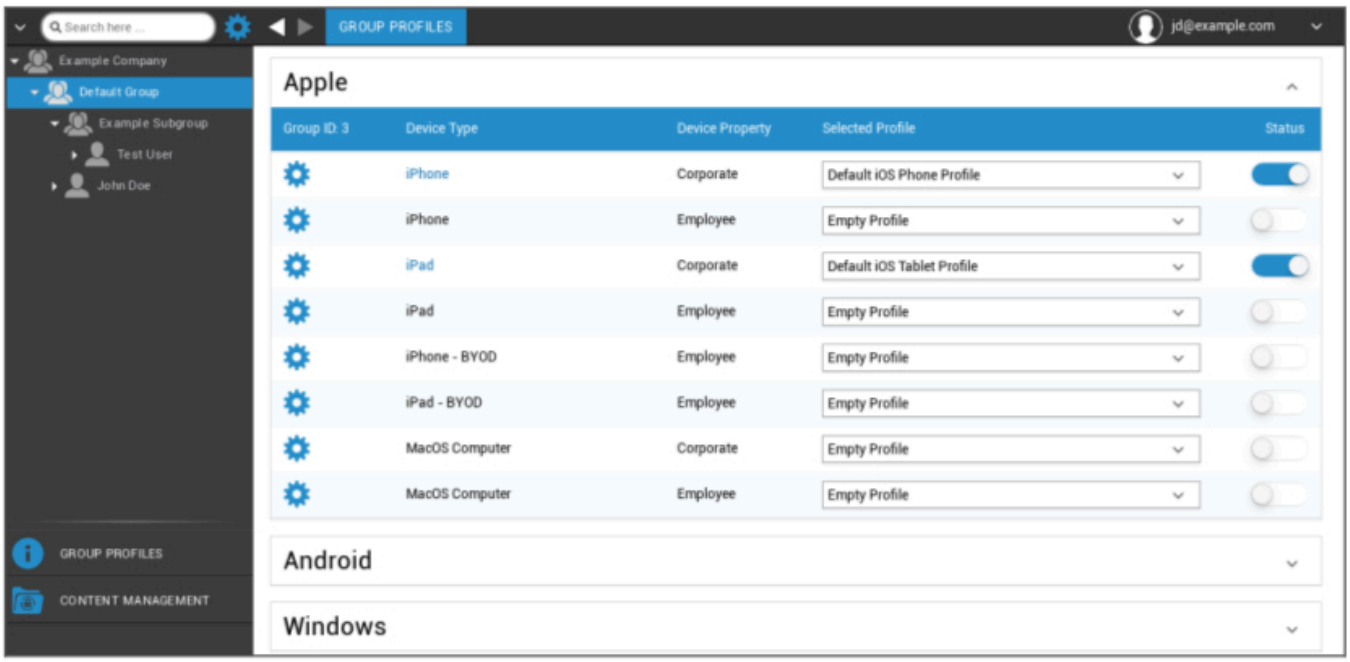
Gestão de grupos na gestão móvel

Um clique na visão geral mostra os diferentes perfis de configuração para as respectivas plataformas.

Um perfil contém todas as opções de configuração que podem ser previamente estabelecidas com a AppTec360 no dispositivo do utilizador final. Em cada plataforma, podes criar perfis para dispositivos empresariais (Corporate) ou para dispositivos "Bring-Your-Own-Device" (Employee).

Para diferenciar as configurações dos grupos de aparelhos, por exemplo, com base na localização ou na função, é aconselhável criar vários subgrupos.

Tem em atenção a Gestão de perfis em Gestão móvel



Com o menu de engrenagens, define uma variedade de configurações para o respetivo (sub)grupo.

Criar um subgrupo	Cria um subgrupo para o respetivo (sub)grupo
Edita o grupo selecionado	Edita o grupo selecionado
Elimina o grupo selecionado	Elimina o grupo selecionado
Inscrição em massa	Inscreve muitos dispositivos/utilizadores de uma só vez para o perfil selecionado
Atribuição de massa	Atribui perfis ao grupo que está atualmente selecionado
Criar um subgrupo	Cria um subgrupo para o respetivo (sub)grupo

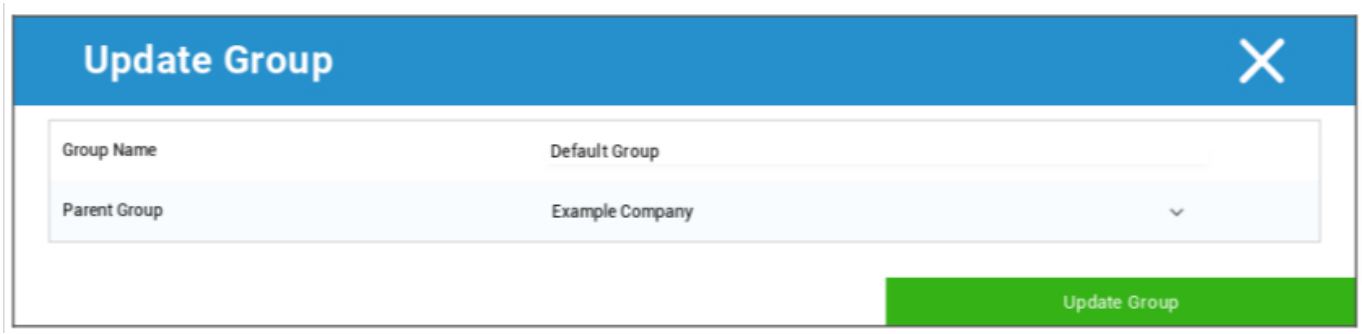
Criar um utilizador	Cria um utilizador para o respetivo (sub)grupo

Criar um subgrupo

Com "Criar um subgrupo", podes criar um subgrupo adicional.

É possível estabelecer em que grupo o subgrupo deve ser atribuído (como padrão, o subgrupo é atribuído ao grupo que está selecionado no momento).

Edita o grupo selecionado



Aqui podes editar o perfil - aqui, são possíveis as seguintes definições:

- O nome do grupo pode ser alterado
- O grupo parental pode ser alterado

Elimina o grupo selecionado

Em "apagar o grupo selecionado" são listados todos os utilizadores e dispositivos que estão no respetivo grupo. Aqui, tens a opção de os apagar.

Para um utilizador, podes executar os seguintes comandos de eliminação:

Eliminar utilizador	O utilizador é eliminado
Move o utilizador para o grupo:	Podes mover o utilizador para outro grupo (coluna seguinte, ex. "Admins)

Para um dispositivo, podes executar os seguintes comandos de eliminação:

Limpar e apagar	Limpa e elimina o dispositivo
Elimina do sistema	Remove o dispositivo apenas da AppTec

Referência: Inscrição em massa

Referência: Atribuição de massa

Criar um utilizador

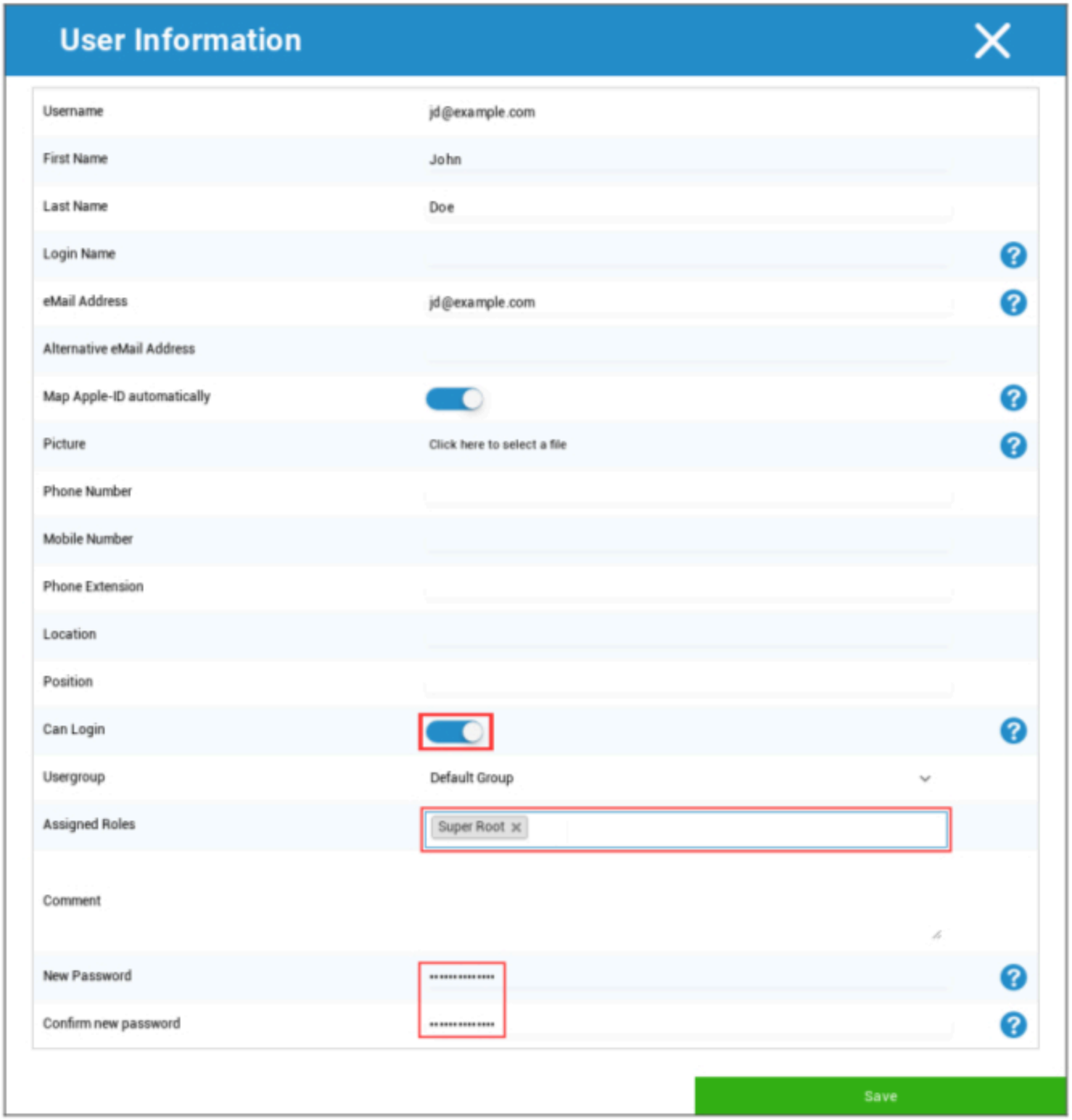
Com "Criar um utilizador", podes adicionar um novo utilizador.

Cria um novo utilizador-administrador

Podes definir um utilizador como Admin-User. Ao fazê-lo, dá-lhe permissões para entrar na consola e também para alterar utilizadores/grupos/dispositivos.

Cria um utilizador normal ou utiliza um utilizador existente. Escolhe o utilizador a quem queres dar permissões de administrador, clica na roda e escolhe "Editar utilizador":

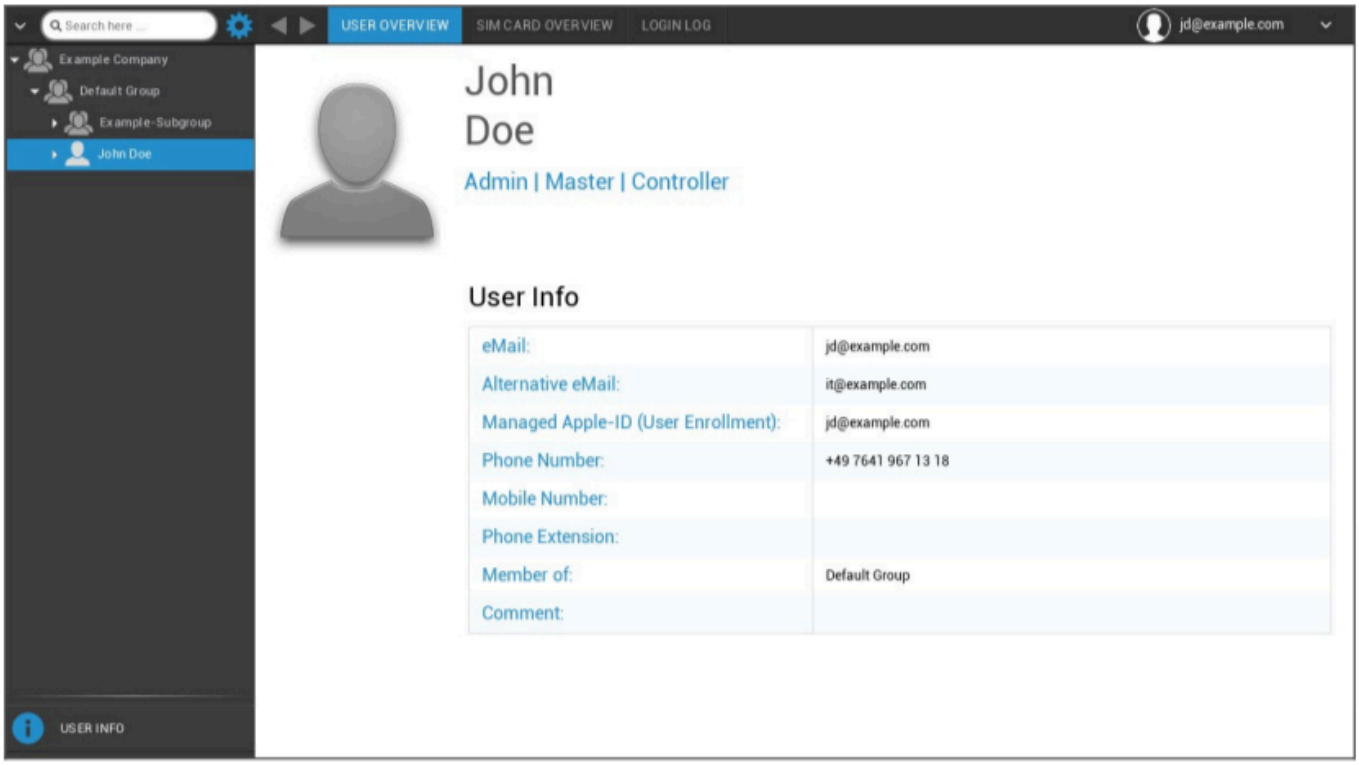
Ativa o interrutor para "Can Login", atribui o papel de "Super-Root" ao utilizador e define uma palavra-passe.



Guarda isto e o utilizador pode agora iniciar sessão com o nome de utilizador e a palavra-passe.

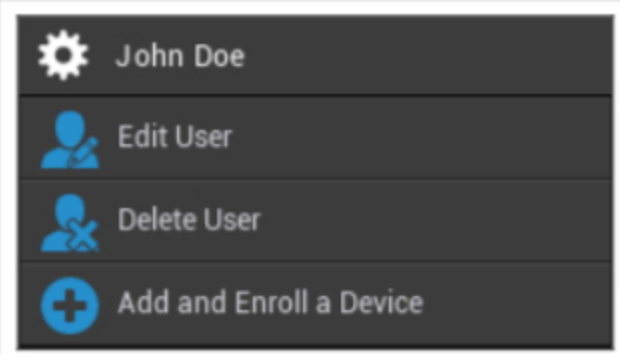
Gestão de utilizadores na gestão móvel

Quando seleccionas um determinado utilizador, vês a seguinte síntese:



Receberás uma visão geral de todas as informações que introduziste anteriormente em "Criar um utilizador".

Com a engrenagem instalada na parte superior, podes efetuar as seguintes configurações:



Nome do utilizador	Nome de utilizador do utilizador selecionado
Editar utilizador	Edita as informações do utilizador
Eliminar utilizador	Eliminar utilizador

	• Eliminar do sistema = O dispositivo será removido do AppTec • Limpar e apagar = O dispositivo será restaurado para as definições de fábrica e removido da AppTec
Adicionar e registar um dispositivo	Inscreve um dispositivo para o utilizador selecionado

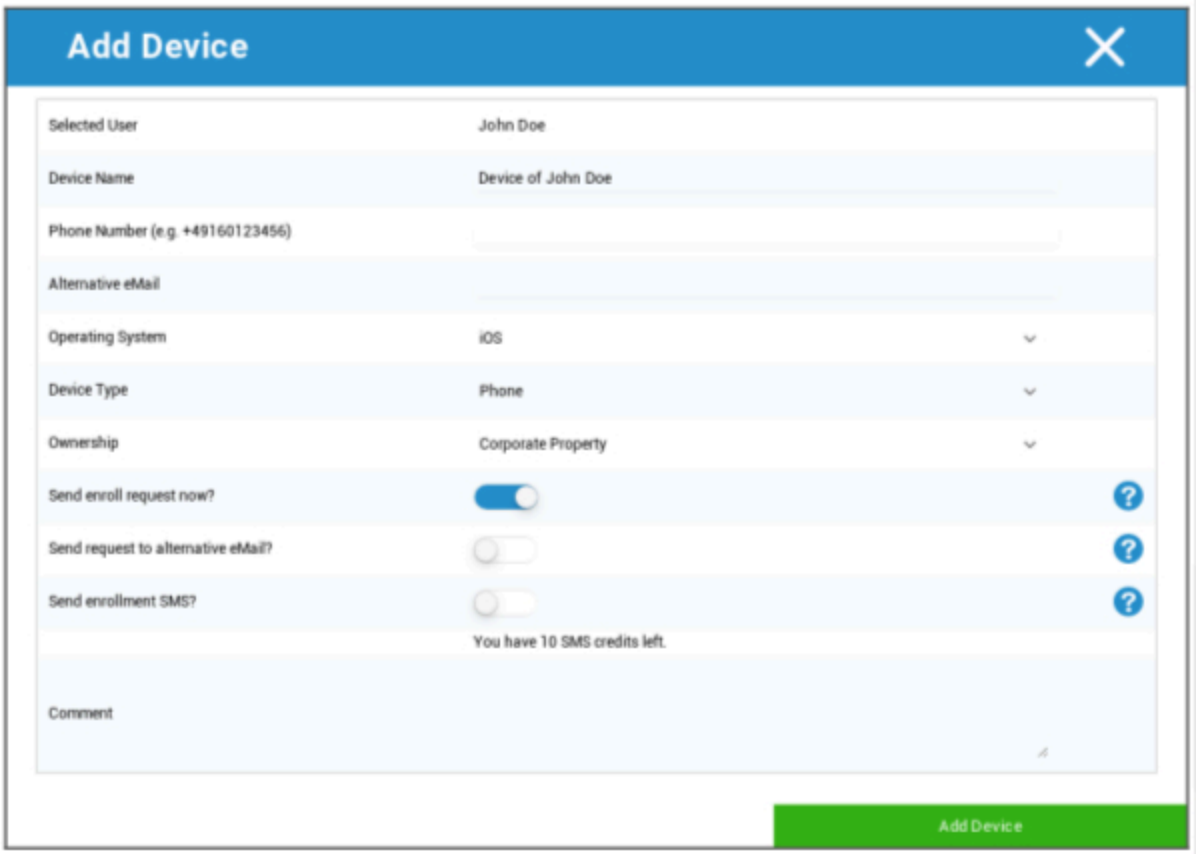
Tem em atenção que o acesso de administração também pode ser arquivado como uma conta de utilizador local na estrutura hierárquica. Sem o estabelecimento de um administrador adicional, este não deve ser suprimido!

Adicionar e registar um dispositivo

Aqui podes selecionar um aparelho para a utilização selecionada.

Em alternativa, podes inscrever dispositivos diretamente num grupo. Para isso, clica no grupo, clica na roda e selecciona "Adicionar e inscrever um dispositivo".

Deves ver a seguinte síntese:



Dependendo do tipo de dispositivo que pretendes registar, tens de efetuar as seguintes configurações:

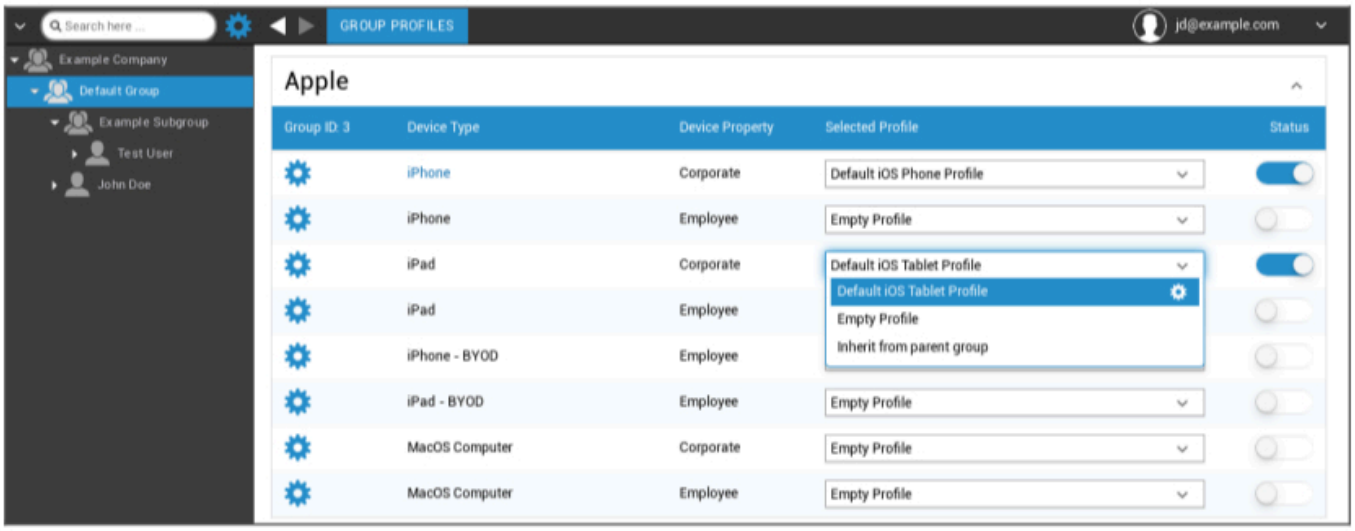
Utilizador selecionado	Utilizador selecionado (será preenchido automaticamente)
Nome do dispositivo	Será preenchido automaticamente (dispositivo para "nome do utilizador") - pode, no entanto, ser alterado
Número de telefone	Número de telefone, será preenchido automaticamente (desde que tenha sido fornecido pelo utilizador) - aqui, no entanto, pode ser adicionado ou alterado
Correio eletrónico alternativo	E-mail alternativo, que será preenchido automaticamente (desde que tenha sido fornecido pelo utilizador) - aqui, no entanto, pode ser adicionado ou alterado
Proprietário do dispositivo	Propriedade da empresa = dispositivo da empresa Propriedade do empregado = dispositivo BYOD
Selecionar a operação Sistema	Aqui, podes escolher entre os seguintes sistemas operativos: • iOS • iOS BYOD (Registo de utilizadores) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Envia um pedido de inscrição?	O e-mail é enviado imediatamente para o endereço de e-mail principal e o utilizador é convidado a ligar o seu dispositivo
Envia um pedido para um eMail alternativo?	Envia o e-mail adicionalmente ou exclusivamente (no caso de "Enviar pedido de inscrição?" ter sido desativado) para o endereço de e-mail alternativo (o e-mail é diferente do e-mail "normal" do Pedido de inscrição)
Envia SMS de inscrição?	Envia um pedido de inscrição por SMS (o "Número de telefone" deve ser introduzido)

Após o envio do pedido de inscrição, o dispositivo é imediatamente apresentado (marcado a vermelho).

Assim que o dispositivo tiver sido ligado com êxito, o dispositivo será marcado a verde pouco tempo depois e estará pronto para receber restrições, aplicações, etc.

Gestão de perfis em Mobile Management

Depois de clicar num grupo, obtém uma visão geral de todas as plataformas de dispositivos que devem ser configuradas e dos perfis respetivamente atribuídos.



	Efectua a configuração do perfil selecionado
Tipo de dispositivo	Tipo e/ou modelo do dispositivo
Propriedade do dispositivo	Proprietário do dispositivo (Corporate = propriedade da empresa, Employee = dispositivo de funcionário privado)
Perfil selecionado	Perfil selecionado (a engrenagem abre o diálogo de configuração do perfil)
Estado	Ligar/Desligar (o perfil é ativado/desativado)

Quando seleccionas a mudança, recebes as seguintes opções:

Cria um perfil

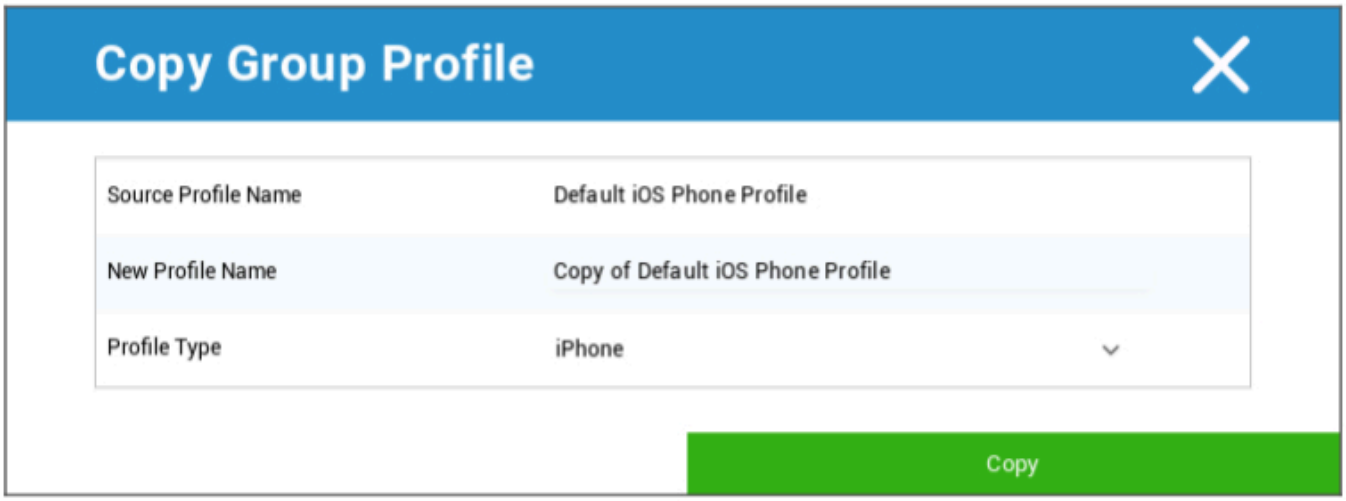
Podes criar e configurar um novo perfil para cada entrada e/ou plataforma. Depois de clicares neste subponto, o perfil será criado imediatamente e podes começar a configurar o iOS, o Android e o Windows Phone imediatamente.

Editar perfil

Depois de clicar em "Editar perfil", acede ao ecrã de configuração do respetivo perfil, onde pode definir as configurações.

Copia o perfil

Com a ajuda da função "Copiar perfil", podes copiar as definições/configurações de um perfil já existente e adicioná-las a um novo perfil.

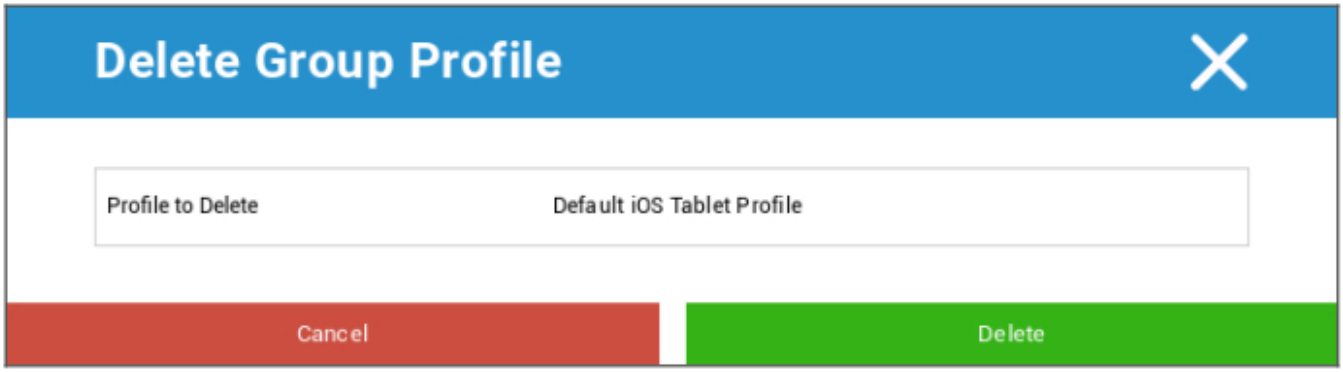


Nome do perfil de origem	Nome do perfil que deve ser copiado
Novo nome de perfil	Nome do novo perfil
Tipo de perfil	Tipo de perfil (telemóvel/tablet)

Depois de clicares em "Copiar", o perfil será criado e pode agora ser atribuído ao grupo

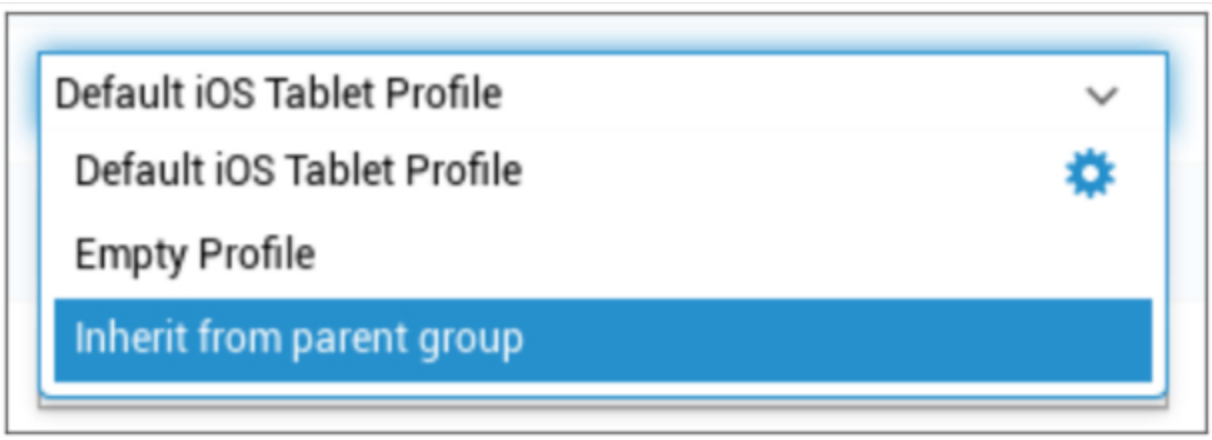
Eliminar perfil

Aqui podes apagar permanentemente um perfil. Tem em atenção que, durante o processo de eliminação e o processo seguinte de "Atribuir agora" para o perfil, a configuração desaparecerá nos respectivos dispositivos de um grupo afetado e não poderá ser recuperada!


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

Herança de perfis

Durante a seleção dos perfis, está disponível a opção "Herdar do grupo pai".



Quando o perfil é ativado, é utilizado o perfil do grupo principal para o dispositivo selecionado (e respetivo tipo de dispositivo). Tem também em atenção que as alterações a este perfil podem afetar vários grupos.

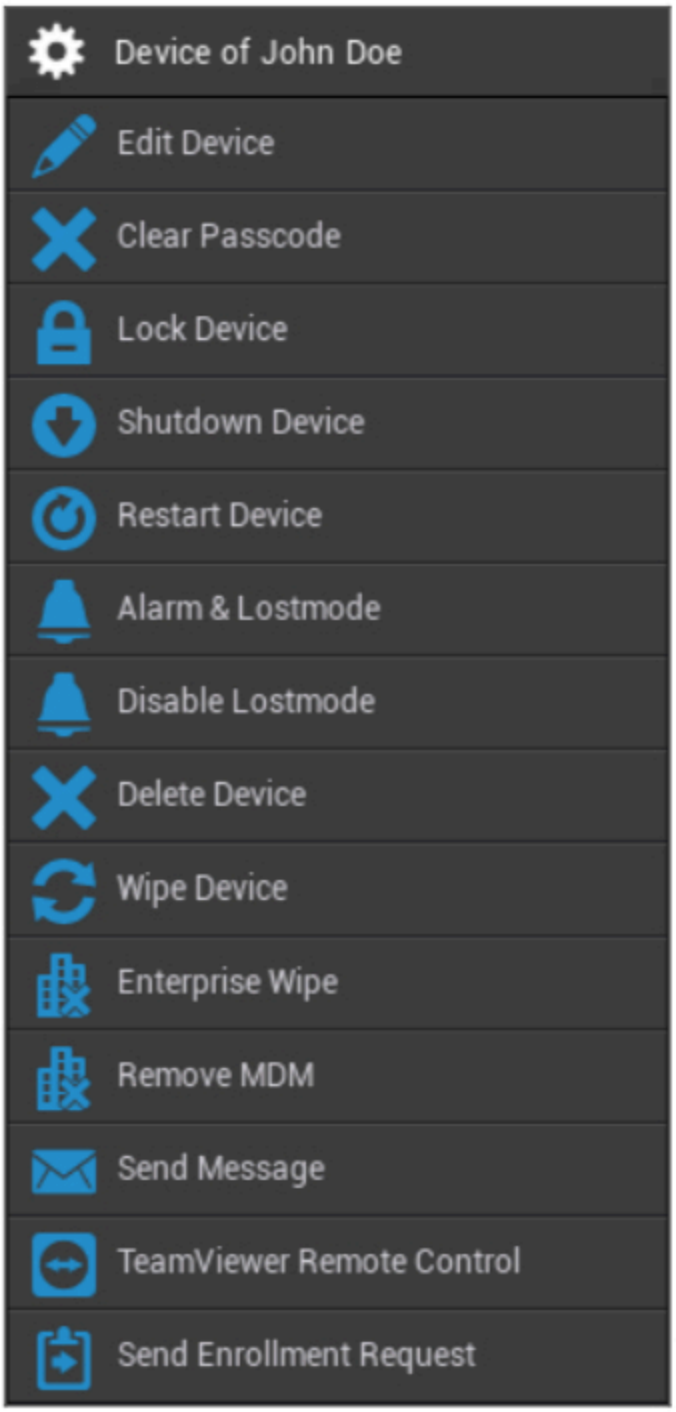
Esta configuração é definida como valor por defeito, quando é criado um novo subgrupo.

Também está disponível a configuração "Empty Profile", que corresponde a um perfil vazio, o que significa que, no final, não serão efectuadas novas configurações no dispositivo do utilizador final.

Gestão de dispositivos na gestão móvel

Quando seleccionas um dispositivo, podes executar uma série de tarefas através da "engrenagem". Estes são diferentes, dependendo das plataformas de SO (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

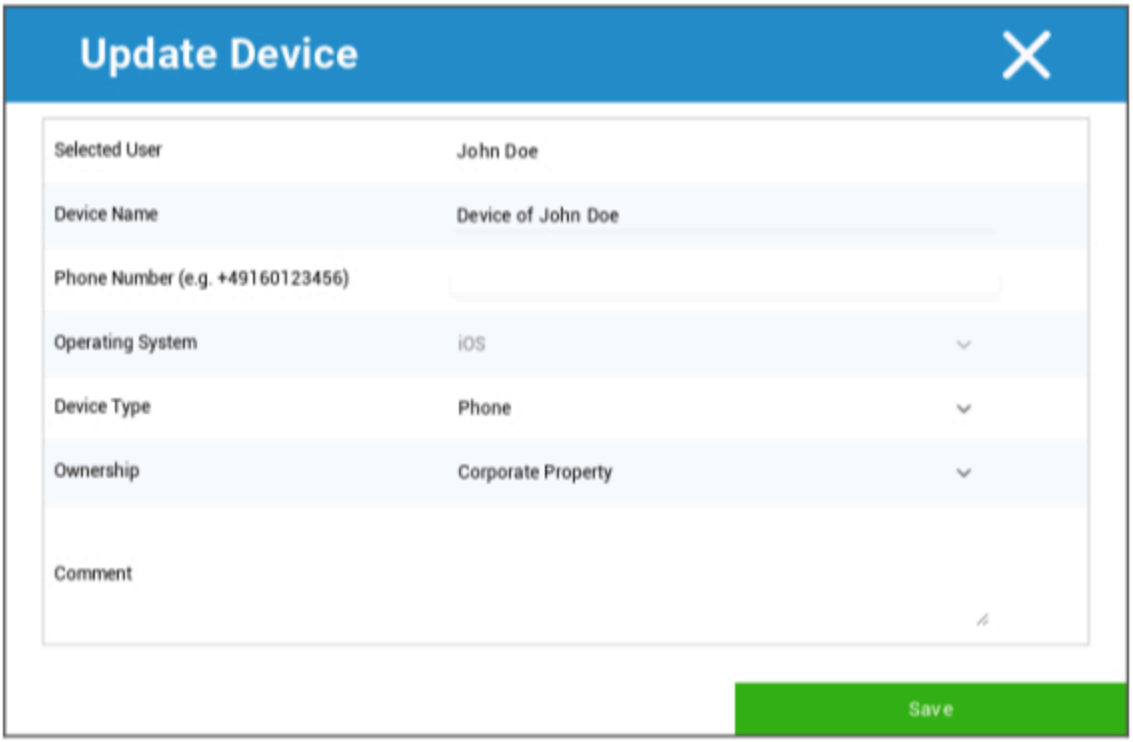
IOS



Editar dispositivo	Editar dispositivo
Limpar código de acesso	Apaga o código de acesso ao aparelho
Dispositivo de bloqueio	Bloqueia o dispositivo (ecrã de bloqueio)

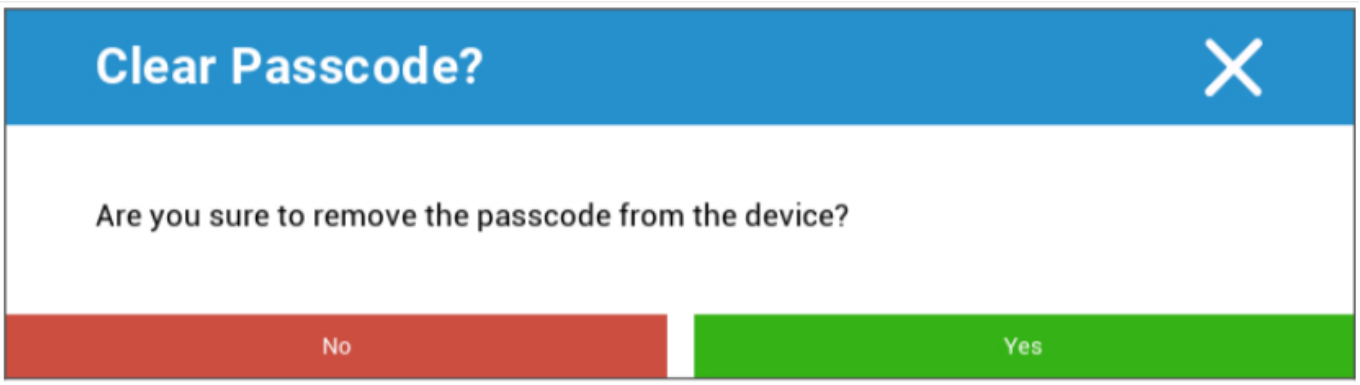
Dispositivo de encerramento	Dispositivo de paragem
Reinicia o dispositivo	Reinicia o dispositivo
Alarme e modo perdido	Alarme de início e modo perdido
Desativar o modo perdido	Desativar o modo perdido
Eliminar dispositivo	Remove o dispositivo da AppTec
Limpa o dispositivo	Repõe o dispositivo para as definições de fábrica
Limpeza da empresa	As informações, aplicações e perfis fornecidos pela AppTec360 são eliminados (o dispositivo é separado da MDM)
Remove a MDM	
Enviar mensagem	Envia notificações push para o dispositivo A mensagem será apresentada na aplicação AppTec360 (separador Mensagem)
Controlo remoto do TeamViewer	Inicia a sessão de controlo remoto com o TeamViewer
Enviar pedido de inscrição	Envia (repetido) o pedido de registo

Editar dispositivo



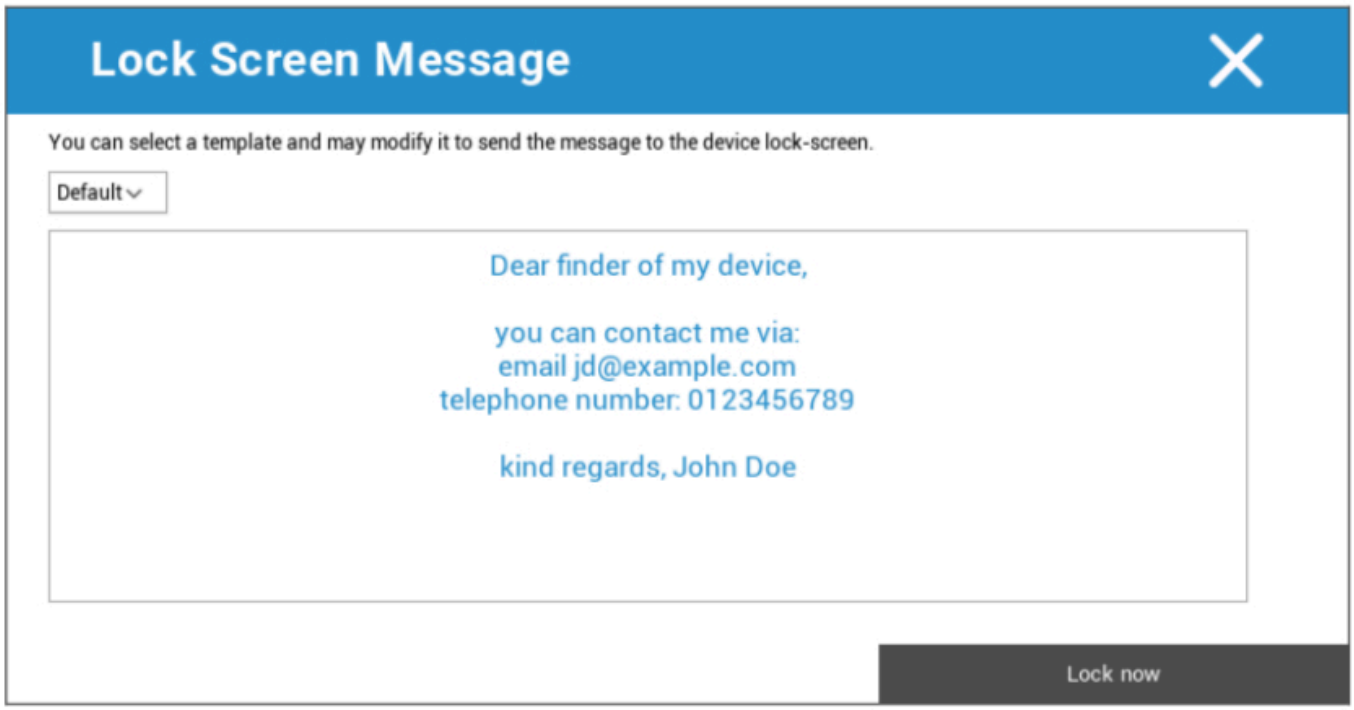
Aqui podes atualizar uma série de informações sobre o aparelho.

Limpar código de acesso



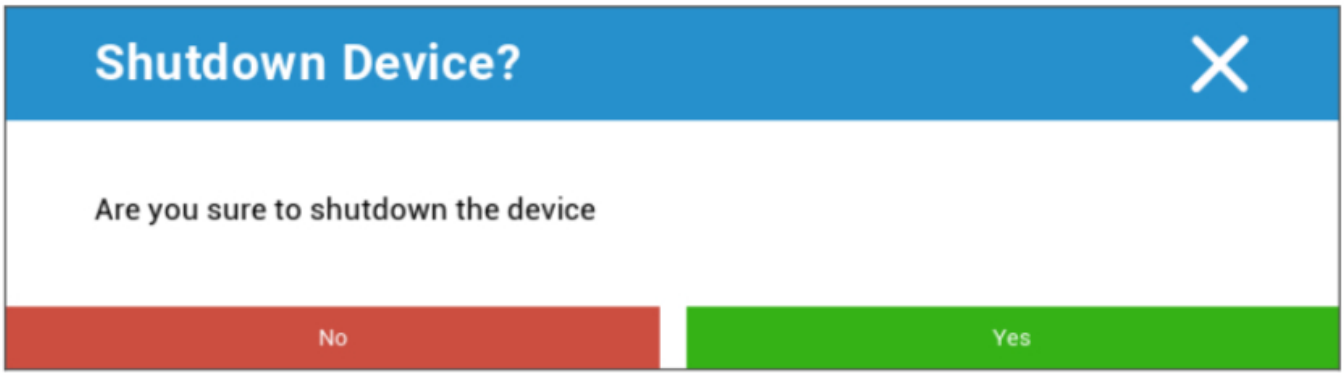
Em "Limpar código de acesso", podes remover remotamente o código de acesso do dispositivo. Posteriormente, será pedido ao utilizador que emita uma nova palavra-passe (dependendo das orientações do código de acesso).

Dispositivo de bloqueio



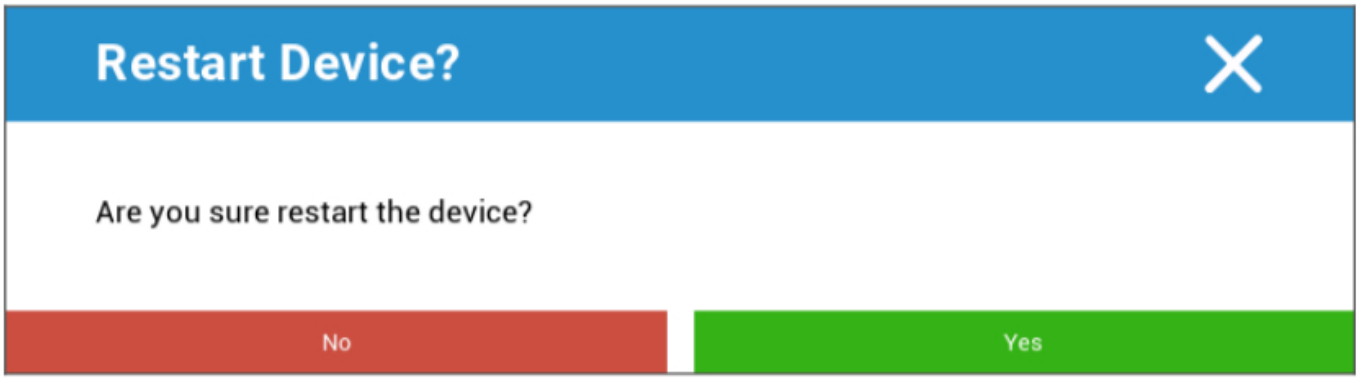
Aqui, é enviado um comando de bloqueio para o dispositivo do utilizador final (ecrã de bloqueio).

Dispositivo de encerramento



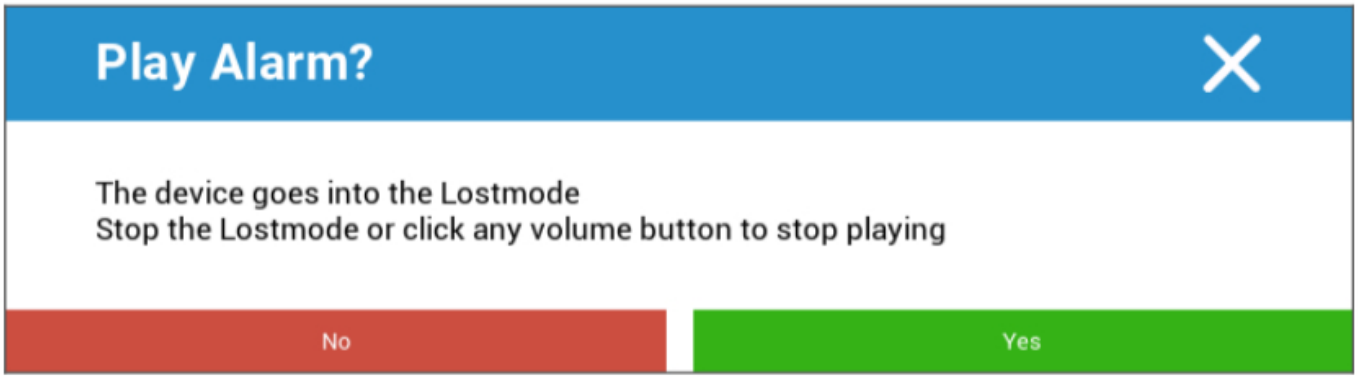
Aqui, é enviado um comando de encerramento para o dispositivo do utilizador final.

Reinicia o dispositivo

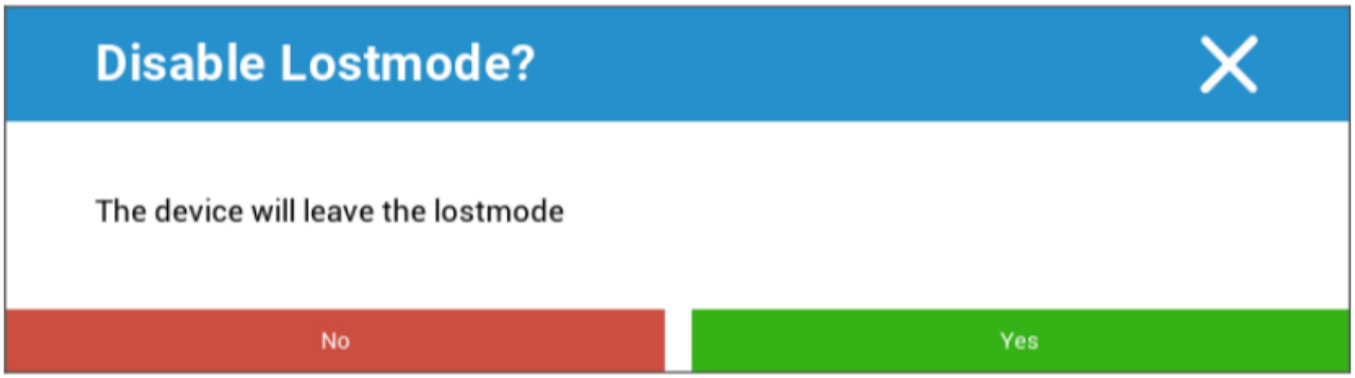


Aqui é enviado um comando de reinício para o dispositivo do utilizador final.

Alarme e modo perdido | Desativar modo perdido



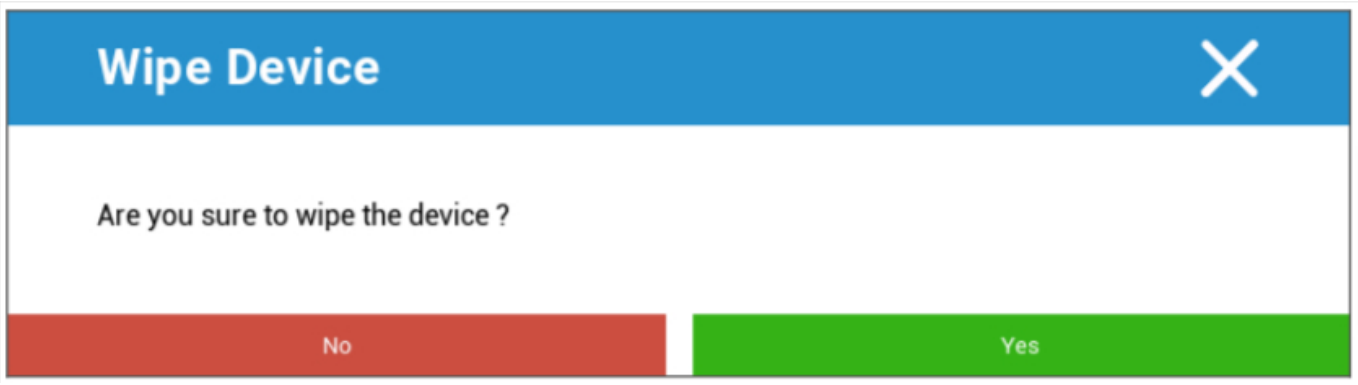
Aqui, o dispositivo pode ser configurado para o Modo perdido, o que faz com que o dispositivo reproduza constantemente um som de alarme. O Lostmode pode ser interrompido premindo qualquer botão de volume do dispositivo ou remotamente clicando em "Disable Lostmode":



Eliminar dispositivo

Aqui podes executar o comando de eliminação. Podes decidir, mais uma vez, se o dispositivo deve ser removido apenas do AppTec360 ("Eliminar do sistema") ou se o dispositivo deve ser removido do AppTec360 e também ser restaurado para a sua configuração de fábrica ("Limpar e eliminar).

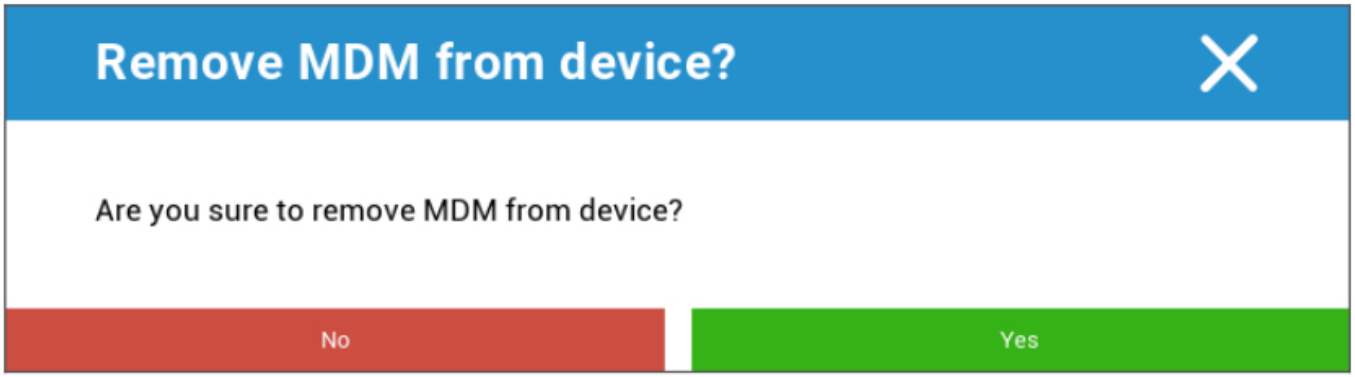
Limpa o dispositivo



Em "Wipe Device" (Limpar dispositivo), podes fazer uma limpeza completa do dispositivo. O dispositivo será restaurado para as definições de fábrica.

Limpeza da empresa | Remover MDM

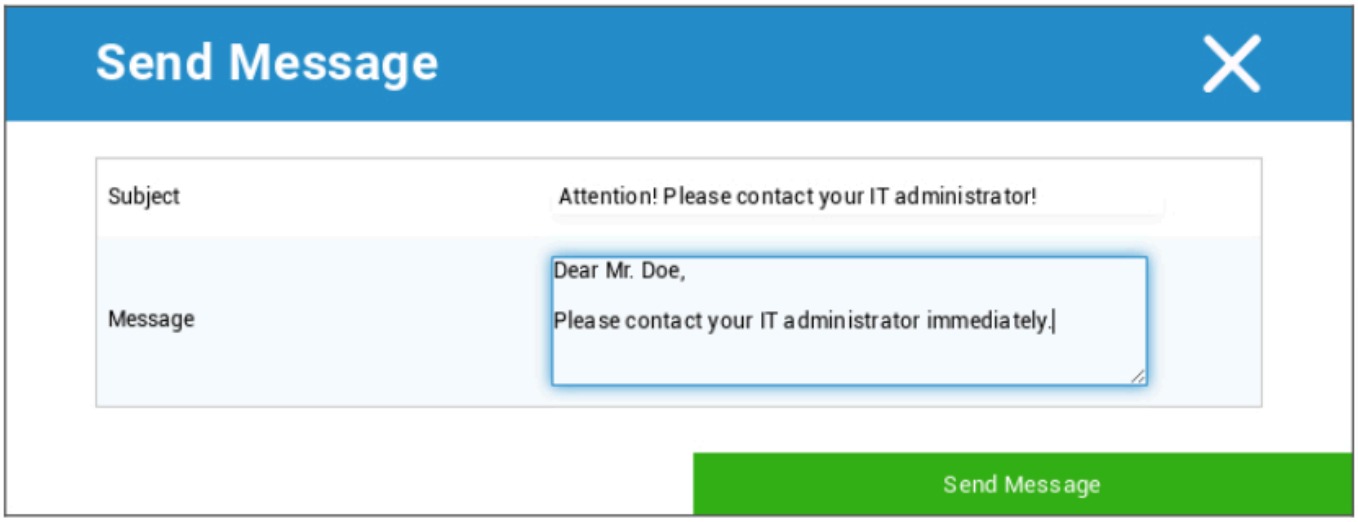
Apenas as informações, aplicações e perfis fornecidos pela AppTec360 são eliminados. Desta forma, os dados da empresa deixam de estar disponíveis no dispositivo do utilizador final. A área privada não é afetada e continua a permanecer no dispositivo do utilizador final.



Com "Remove MDM" podes remover o perfil MDM no dispositivo do utilizador final e todos os outros itens fornecidos pela AppTec.

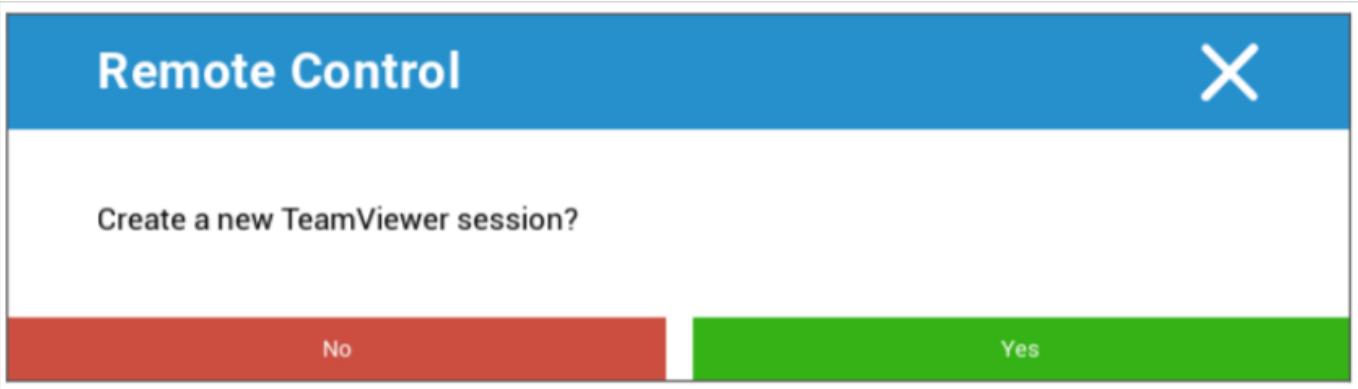
Este comando executa a mesma ação que "Enterprise Wipe".

Enviar mensagem



Aqui podes enviar uma notificação push para o respetivo dispositivo.

Controlo remoto do TeamViewer



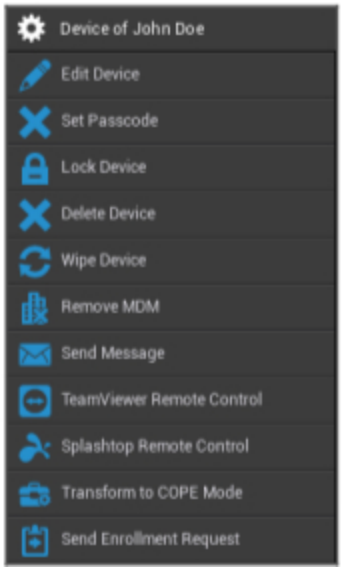
Aqui podes iniciar uma sessão de controlo remoto do Teamviewer.

Enviar pedido de inscrição

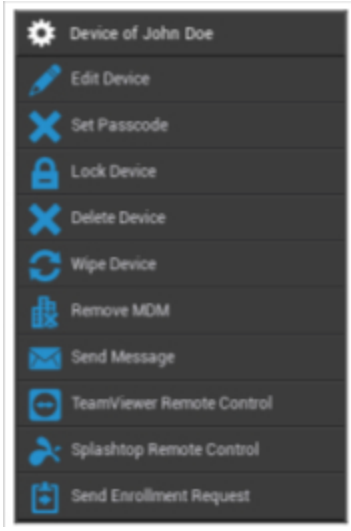
Com "Enviar pedido de inscrição", podes enviar um pedido de inscrição (novamente) para o respetivo utilizador.

Android

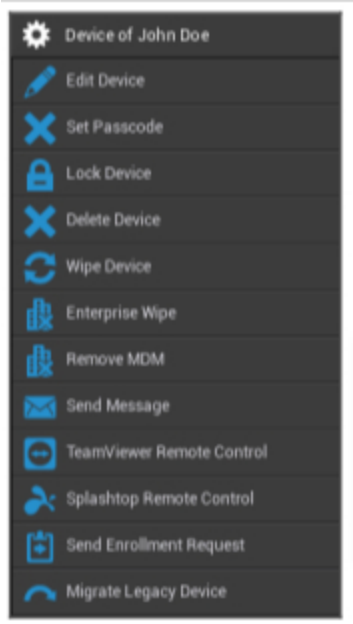
Dispositivo totalmente gerido pela AE (gerido pelo trabalho)



Perfil de trabalho AE (contentor)



Telefone Android | Tablet

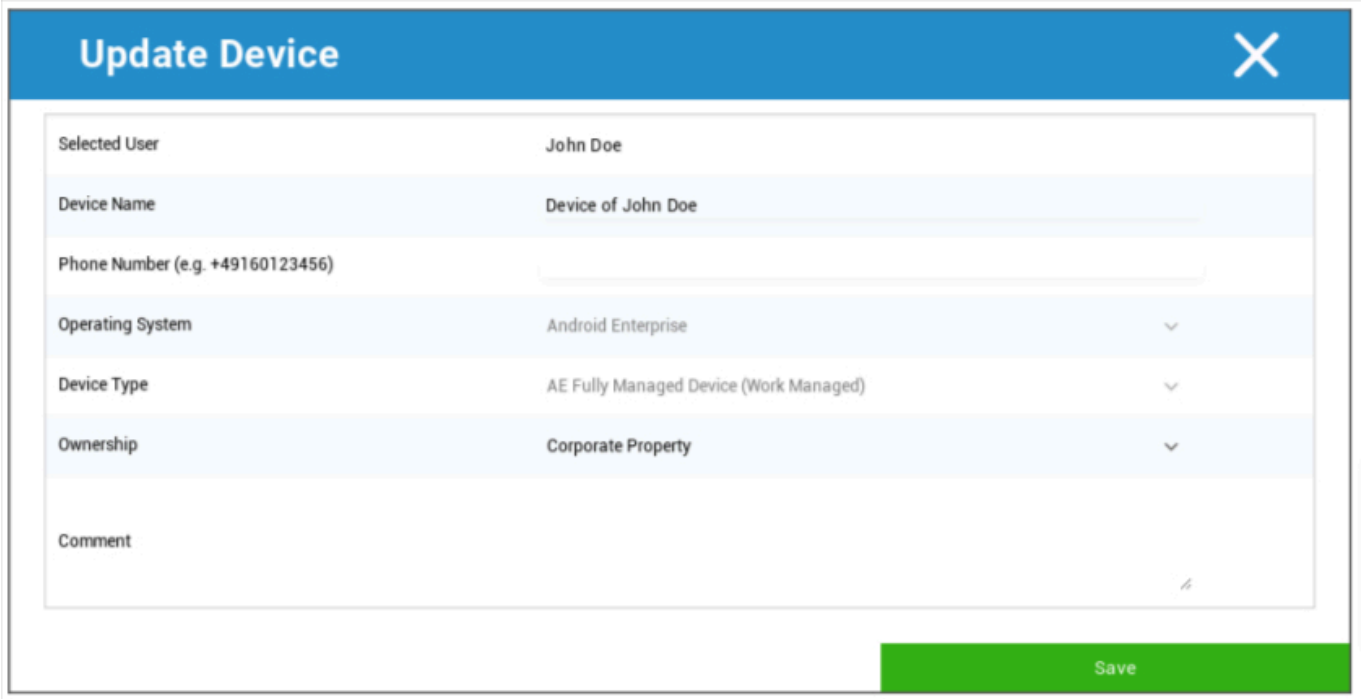


Editar dispositivo	Edita as informações do dispositivo
Definir código de acesso	Define o código de acesso do dispositivo
Dispositivo de bloqueio	Bloqueia o dispositivo (ecrã de bloqueio)
Eliminar dispositivo	Elimina o dispositivo da AppTec
Limpa o dispositivo	Repõe o dispositivo para as definições de fábrica
Limpeza da empresa	As informações, as aplicações e os perfis fornecidos pela AppTec360 são eliminados (o dispositivo será separado da MDM)
Remove a MDM	
Enviar mensagem	Envia notificações push para o dispositivo A mensagem será apresentada na aplicação AppTec360 (separador Mensagem)
Controlo remoto do TeamViewer	Inicia uma sessão de Controlo Remoto para este dispositivo utilizando o TeamViewer
Controlo remoto Splashtop	Inicia uma sessão de Controlo Remoto para este dispositivo utilizando o Splashtop
Transforma para o modo COPE (apenas no dispositivo AE totalmente gerido (gerido pelo trabalho))	Cria um perfil de trabalho neste dispositivo AE totalmente gerido (gerido pelo trabalho)
Enviar pedido de inscrição	Envia um pedido de inscrição (repetido)

Migra o dispositivo antigo (apenas no telefone / tablet Android quando inscrito usando o provisionamento do modo de proprietário do dispositivo)	Migra o perfil de telemóvel/tablet Android para o perfil de dispositivo totalmente gerido pela AE (gerido pelo trabalho)

Editar dispositivo

Aqui podes atualizar uma série de informações sobre o aparelho.



Utilizador selecionado	Utilizador do dispositivo
Nome do dispositivo	Nome do dispositivo
Número de telefone	Número de telefone do dispositivo
Sistema operativo	Android Enterprise Android
Tipo de dispositivo	Android Enterprise: • Dispositivo totalmente gerido pela AE (gerido pelo trabalho) • Modo de perfil de trabalho AE (apenas contentor) • AE Dispositivo totalmente gerido com perfil de trabalho (COPE) Android: • Telefone • Tablet
Propriedade	Corporate = propriedade corporativa

	Empregado = propriedade do empregado
Comenta	Descrições adicionais para o dispositivo

Limpar código de acesso

Aqui podes remover o código de acesso do dispositivo selecionado. Por predefinição, no Android, o código de acesso será definido como "123456" - este pode e deve ser alterado pelo utilizador posteriormente.

Dispositivo de bloqueio

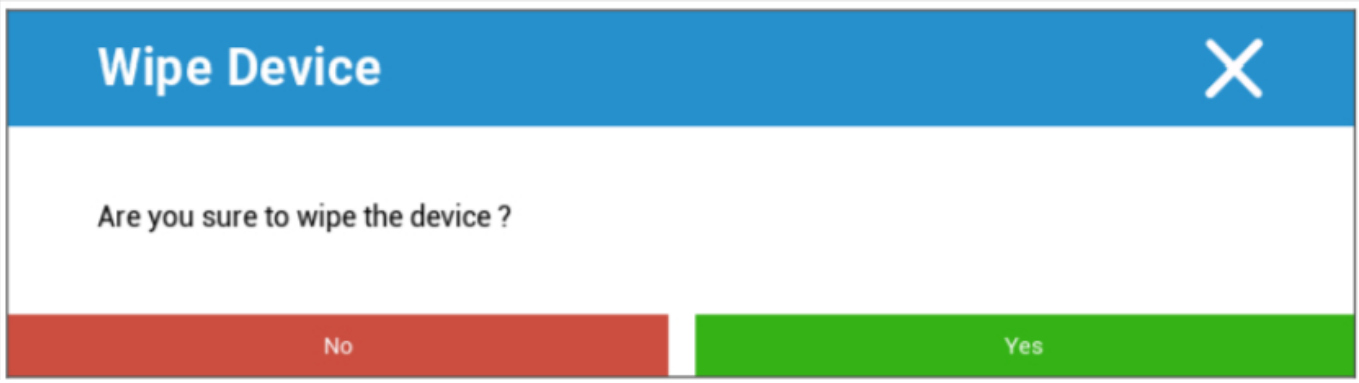
Aqui, é enviado um comando de bloqueio do dispositivo para o dispositivo (ecrã de bloqueio).

Eliminar dispositivo

Aqui podes executar um comando de eliminação. Podes decidir, mais uma vez, se o dispositivo deve ser removido apenas do AppTec360 ("Eliminar do sistema") ou se o dispositivo deve ser removido do AppTec360 e, adicionalmente, ser restaurado para as suas definições de fábrica ("Limpar e eliminar).

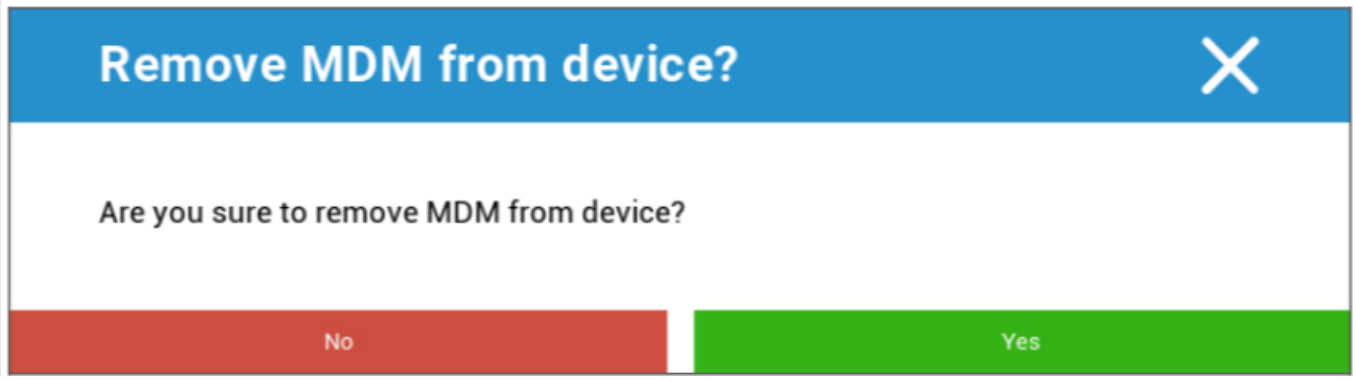
Limpa o dispositivo

Em "Wipe Device" (Limpar dispositivo), podes fazer uma limpeza completa do dispositivo. O dispositivo será então restaurado para as definições de fábrica.



Além disso, se o dispositivo tiver um cartão SD, podes apagar o cartão SD. Podes fazer isso definindo "Wipe SD Card too? " para "Ligado".

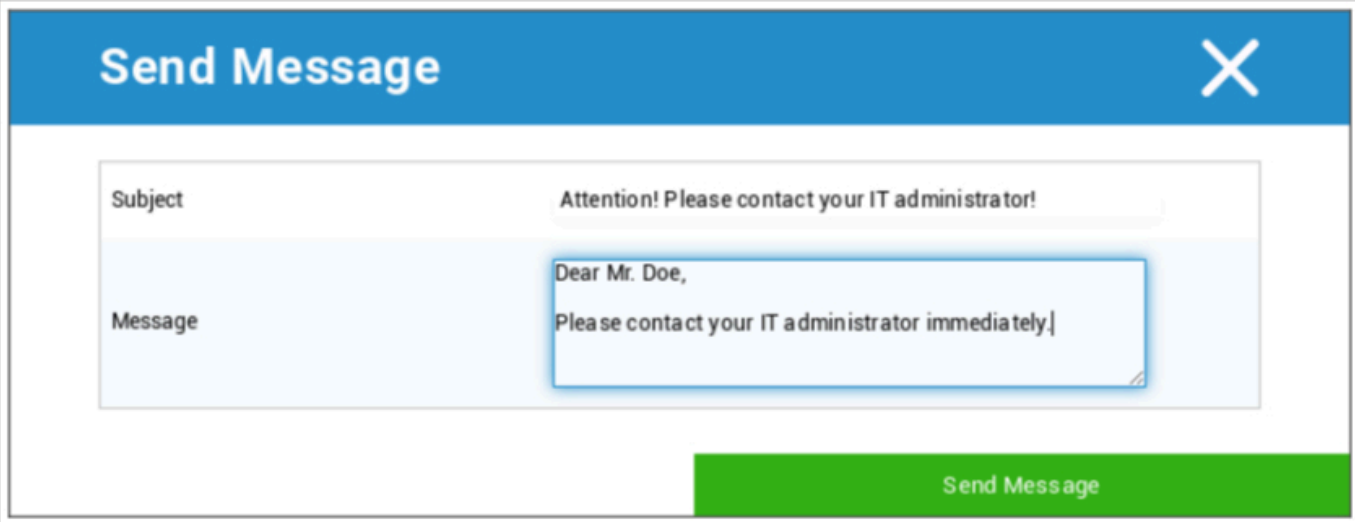
Remove a MDM



Este é o método recomendado para criar uma separação da MDM.

Apenas as informações, aplicações e perfis fornecidos pela AppTec360 são eliminados, o que significa que todos os dados da empresa deixarão de estar disponíveis no dispositivo do utilizador final. A esfera privada, no entanto, não é afetada e continua a permanecer no dispositivo do utilizador final.

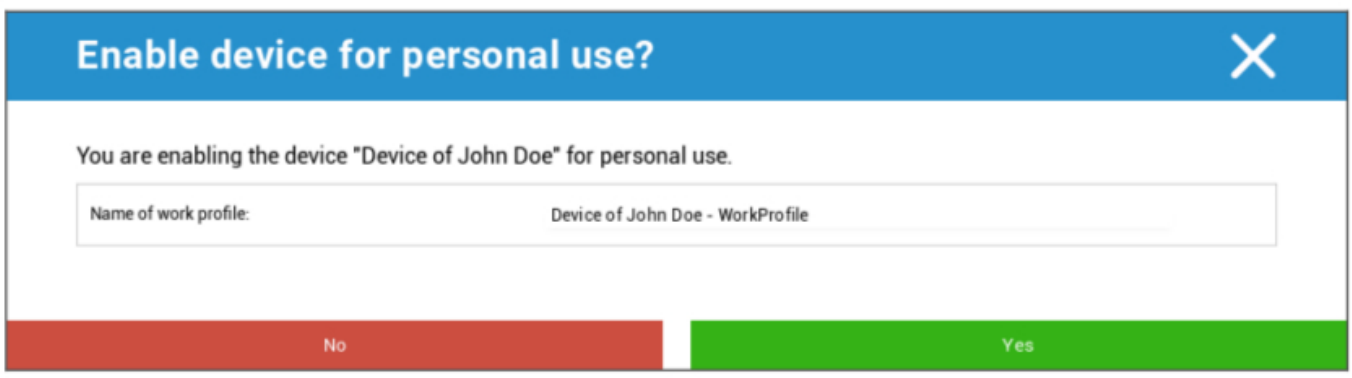
Enviar mensagem



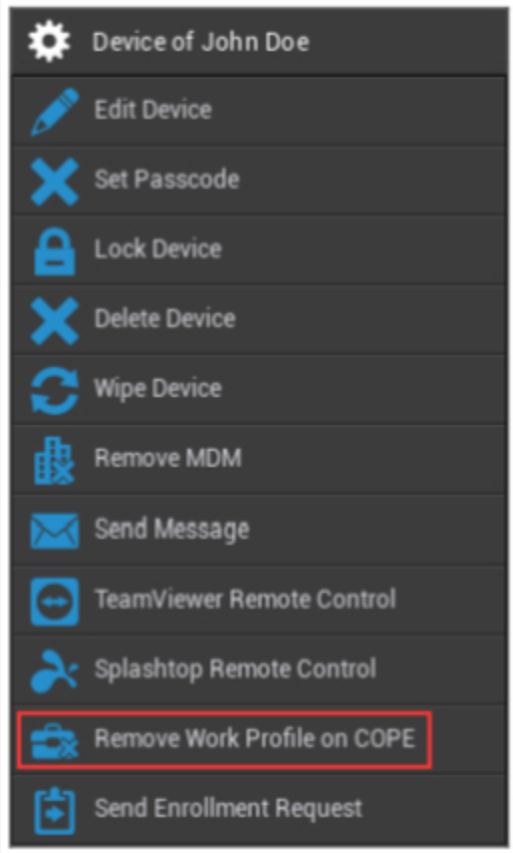
Aqui podes enviar uma notificação push para o respetivo dispositivo do utilizador final.

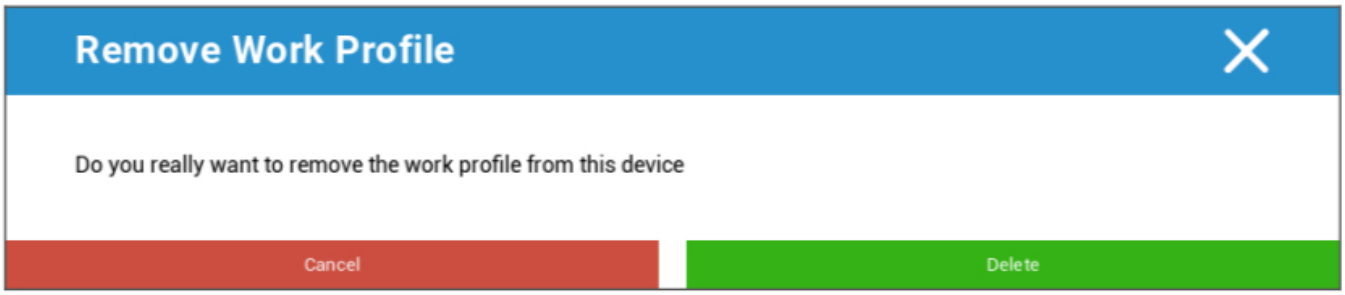
Passa para o modo COPE

Cria um perfil de trabalho neste dispositivo AE totalmente gerido (gerido pelo trabalho)



Depois de transformares o dispositivo no modo COPE, podes remover o perfil de trabalho clicando na opção de engrenagem **Remover perfil de trabalho no COPE:**




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

Enviar pedido de inscrição

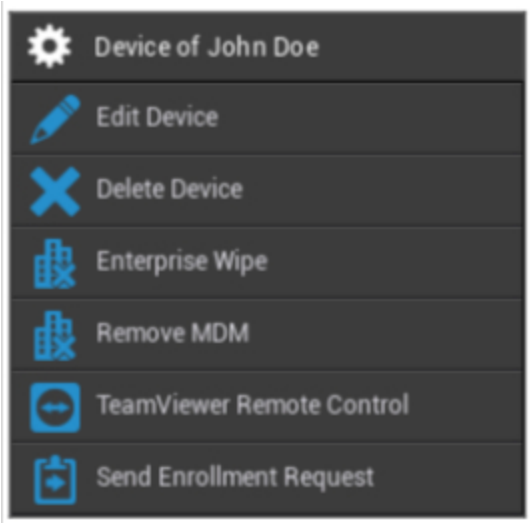
Com "Enviar pedido de inscrição", podes enviar um pedido de inscrição (novamente) ao respetivo utilizador.

Tem em atenção que só é válido o pedido de inscrição mais recente.

Migra o dispositivo antigo

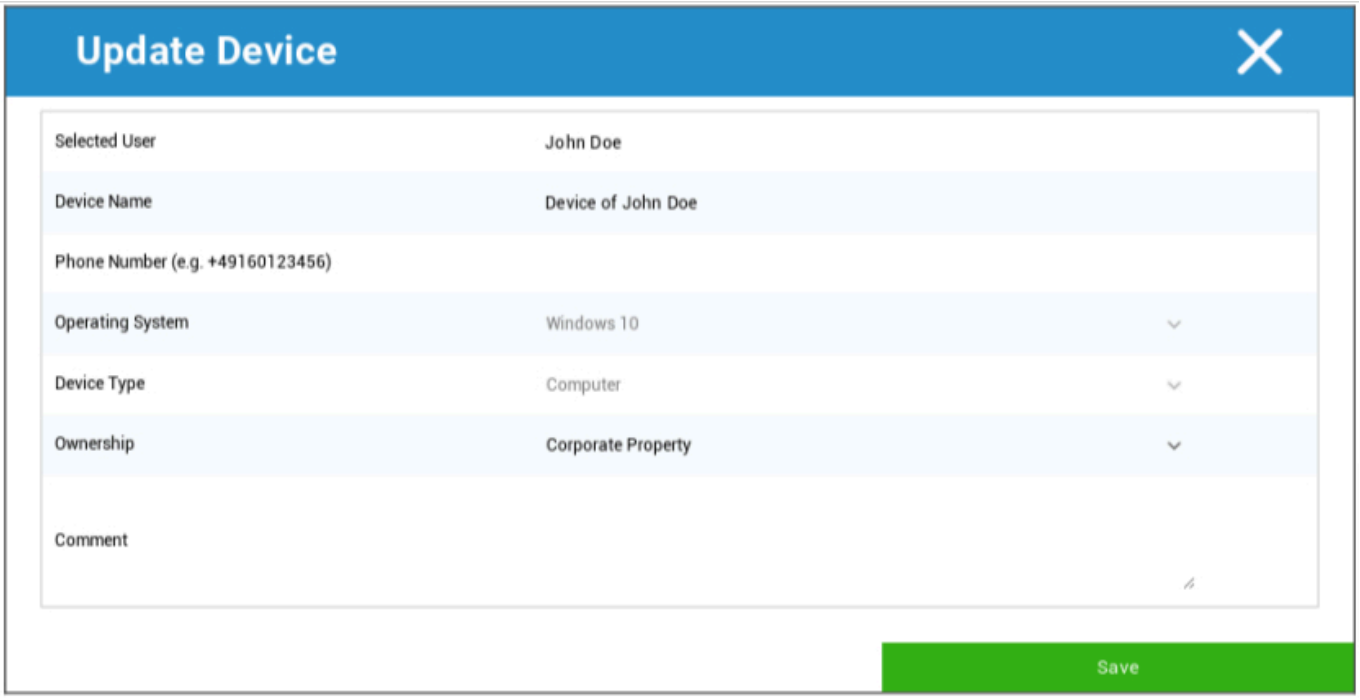
Migra o perfil de telemóvel/tablet Android para o perfil de dispositivo totalmente gerido pela AE (gerido pelo trabalho)

Janelas



Nome do dispositivo	Nome do dispositivo selecionado
Editar dispositivo	Editar dispositivo
Eliminar dispositivo	Remove o dispositivo da AppTec
Limpeza da empresa	As informações, aplicações e perfis fornecidos pela AppTec360 são eliminados
Remove a MDM	
Controlo remoto do TeamViewer	Controla remotamente o dispositivo com o TeamViewer
Enviar pedido de inscrição	Envia o pedido de registo (novamente)

Editar dispositivo

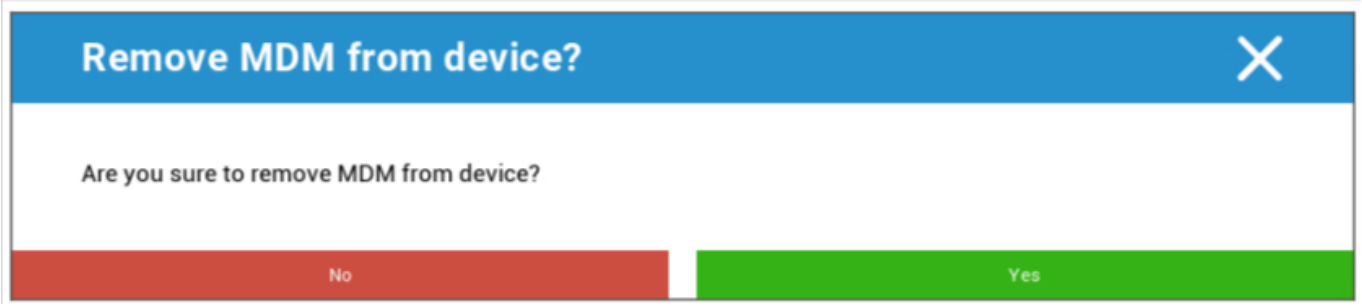


Aqui podes atualizar uma série de informações sobre o aparelho.

Eliminar dispositivo

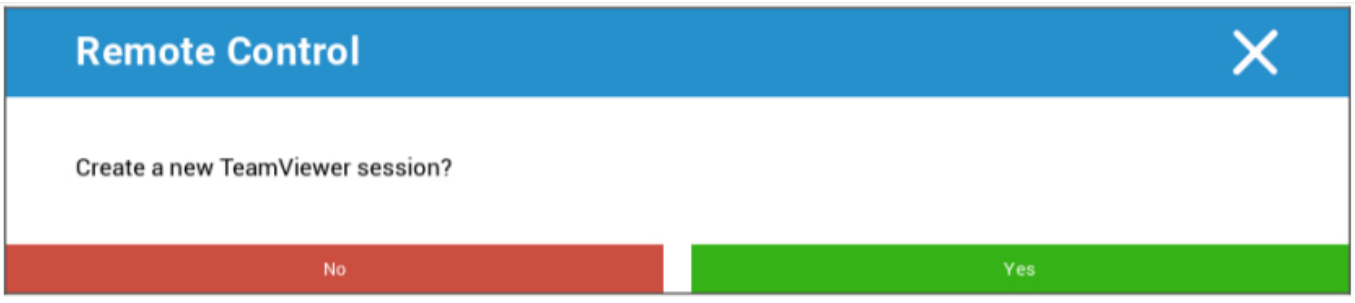
Aqui podes executar o comando de eliminação que apenas remove o dispositivo do AppTec360.

Limpeza da empresa | Remover MDM



Apenas as informações, aplicações e perfis fornecidos pela AppTec360 são eliminados. Desta forma, os dados da empresa deixam de estar disponíveis no dispositivo do utilizador final. A área privada não é afetada e continua a permanecer no dispositivo do utilizador final.

Controlo remoto do TeamViewer



Aqui podes iniciar uma sessão de Controlo Remoto TeamViewer para este dispositivo.

Enviar pedido de inscrição

Com "Enviar pedido de inscrição", podes enviar um pedido de inscrição (novamente) para o respetivo utilizador.

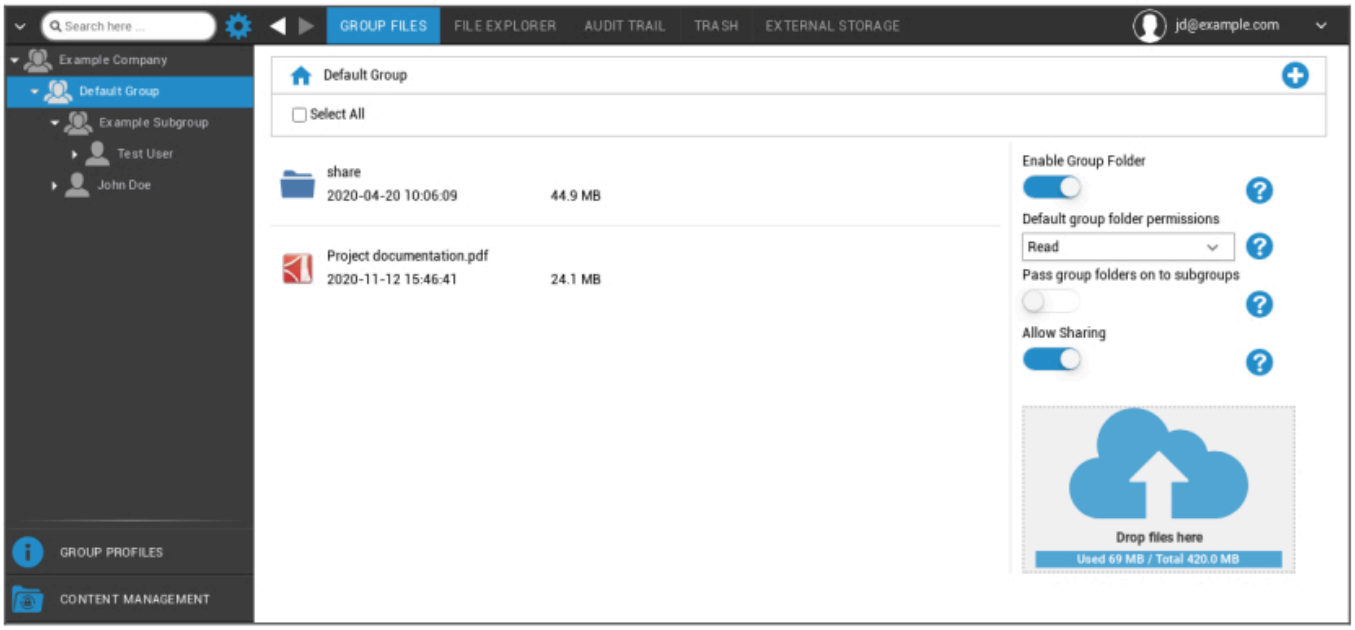
Gestão de conteúdos

Quando estás num grupo, podes gerir a ContentBox da AppTec com "Gestão de conteúdos".

Com a Content Box, podes distribuir com segurança documentos e outros dados da empresa para os dispositivos dos utilizadores finais.

Ficheiros de grupo

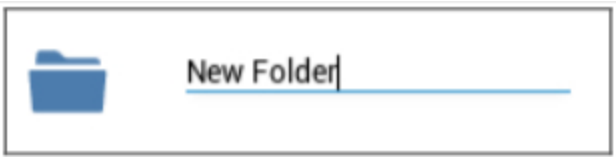
O "Group Files" representa uma parte fundamental da ContentBox. Aqui estabelece definições, carrega documentos, cria novas pastas, etc.



Com o símbolo no canto superior direito, podes criar novas pastas que são designadas para o respetivo grupo com "Adicionar pasta".

Com o símbolo no canto superior direito, podes criar uma nova pasta através de "Adicionar pasta", que deve ser atribuída ao respetivo grupo.

Podes dar o nome que quiseres à pasta.



Através de "Upload Files", podes carregar dados. Aqui abre-se o teu Standard-Explorer. Podes, evidentemente, executar estas duas acções em todas as (sub)pastas.

Com o símbolo no canto superior esquerdo, podes voltar ao menu principal.

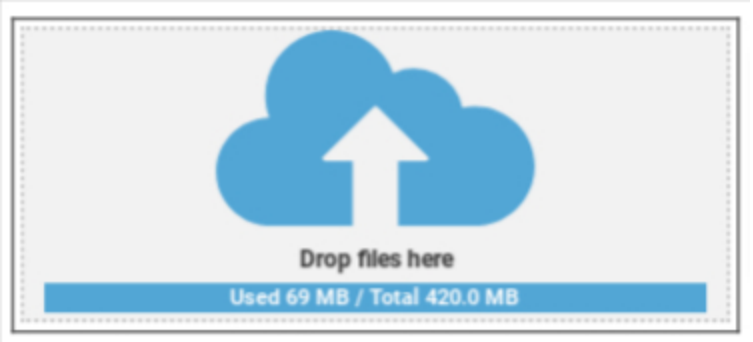
Podes selecionar várias pastas e ficheiros e descarregá-los com "Descarregar" ou podes apagá-los clicando em "Apagar".

Também podes selecionar todos os ficheiros e pastas com e executar os comandos "Transferir" e "Apagar".

Quando passas o rato por cima de uma pasta ou de um ficheiro, vês o seguinte resumo:

- Com "Renomear", podes mudar o nome da pasta/ficheiro
- Com "Descarregar", podes descarregar a pasta/ficheiro
- Com "Apagar", podes apagar a pasta/ficheiro

Ativar a pasta de grupo	Se estiver ativado, todos os membros do grupo têm acesso à respectiva pasta
Permissões de pasta de grupo predefinidas	Permissões dos utilizadores do grupo selecionado: Ler = permissão só de leitura Atualizar = permissão de atualização Criar = permissão de criação Apagar = apaga a permissão
Passa as pastas do grupo para os subgrupos	Se estiver ativado, os respectivos subgrupos podem ter acesso aos ficheiros de dados principais
Permissões para subgrupos	Permissões dos utilizadores no subgrupo selecionado: Ler = permissão só de leitura Atualizar = permissão de atualização Criar = permissão de criação Apagar = apaga a permissão
Permitir a partilha	Se estiver ativado, o utilizador pode partilhar ficheiros através de uma ligação



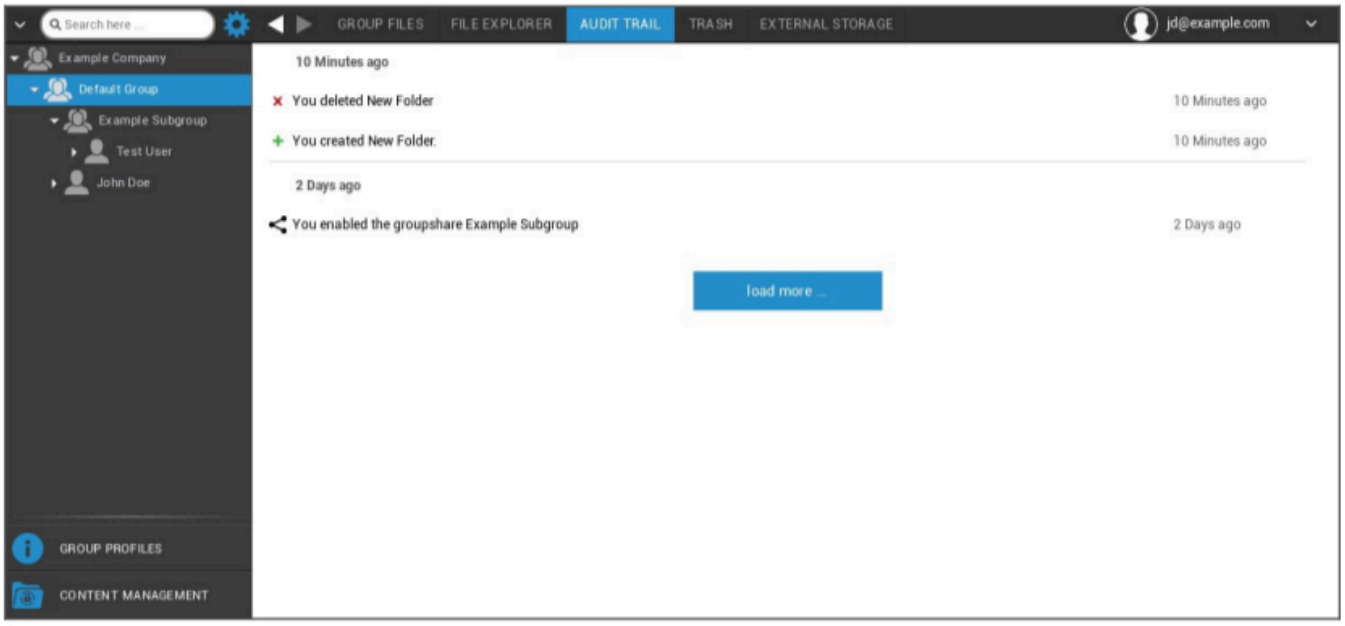
Para carregar ficheiros, podes utilizar este campo, puxando um ficheiro através de Arrastar e Largar para esta janela. Também podes clicar neste campo, para selecionar e carregar um ficheiro com a ajuda do Internet Explorer.

Explorador de ficheiros

Com o "File Explorer", podes gerir todas as pastas e ficheiros - independentemente do grupo onde estão arquivados.

Também encontras as definições e os botões que aprendeste em "Ficheiros de grupo".

Pista de auditoria



Em "Pista de auditoria", podes ver no histórico que utilizador criou, apagou ou partilhou o quê. Desta forma, podes determinar, a qualquer momento, o que foi feito com os dados da empresa.

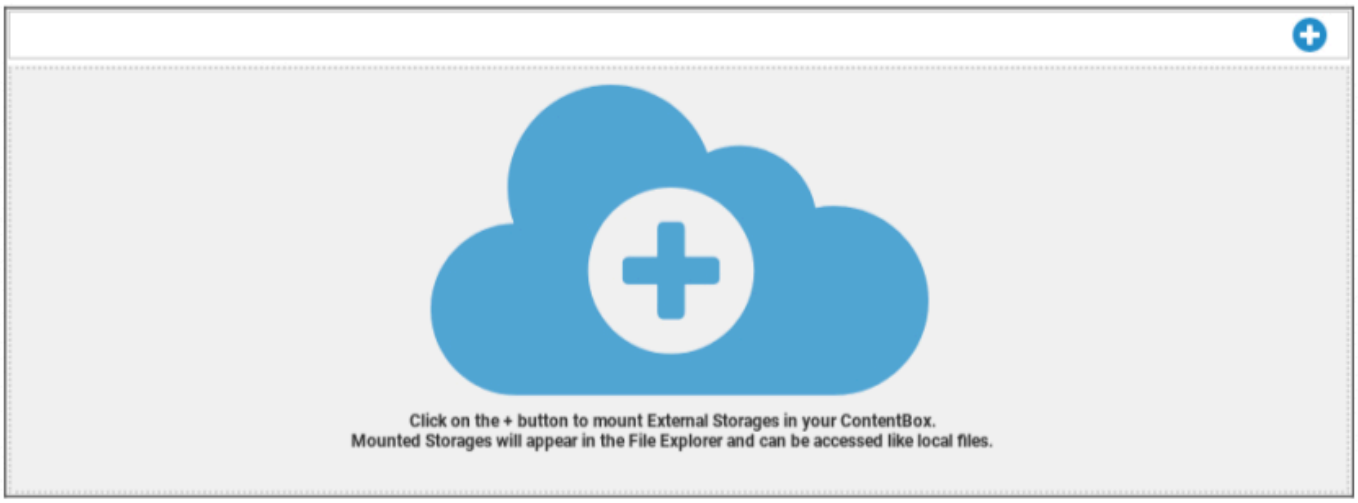
Lixo

Se tiveres apagado algo (por acidente), podes ver as pastas e os ficheiros em "Lixo" e recuperá-los, de acordo com os teus desejos.

- Com "Undelete", podes recuperar os dados/pasta.
- Com "Apagar", podes apagar permanentemente os dados/pasta - tens de confirmar o comando "Apagar" mais uma vez.

Tem em atenção que a capacidade de armazenamento que está a ser utilizada no lixo reduz o "Espaço Total" disponível - este é um requisito do ownCloud.

Armazenamento externo



Sob o título "Armazenamento externo", podes ligar um armazenamento externo.

Com o símbolo, podes acrescentar armazenamento (adicional).

Tipo	Amazon S3, FTP, SFTP, ownCloud, WebDAV, Windows Share, SharePoint

Amazon S3	
Nome de exibição	Mostra o nome
Chave de acesso	Chave de acesso
Chave secreta	Chave de segurança
Balde	Identidade definitiva da subpasta que te foi atribuída
Nome do anfitrião (opcional)	Nome do anfitrião (opcional)
Porta (opcional)	Porta (opcional)
Região	Região (opcional)
Ativar SSL	Ativar SSL
Ativar estilo de trajetória	Endereço do Caminho Limpo que te foi atribuído

FTP	
Nome de exibição	Mostra o nome
Anfitrião	Endereço do anfitrião
Nome de utilizador	Nome de utilizador
Palavra-passe	Palavra-passe
Raiz	Menu principal
Segura ftps://	

SFTP	
Nome de exibição	Mostra o nome
Anfitrião	Endereço do anfitrião
Nome de utilizador	Nome do utilizador
Palavra-passe	Palavra-passe
Raiz	Menu principal

ownCloud	
Nome de exibição	Mostra o nome
URL	URL do ownCloud
Nome de utilizador	Nome de utilizador
Palavra-passe	Palavra-passe
Subpasta remota	Pasta standard
Segura https://	

WebDAV	
Nome de exibição	Mostra o nome
URL	URL WebDAV
Nome de utilizador	Nome do utilizador
Palavra-passe	Palavra-passe
Raiz	Menu principal
Segura https://	
Partilha do Windows	O suporte para o Windows Share estará disponível em breve
SharePoint	O suporte para o Microsoft SharePoint estará disponível em breve

Registo de auditoria

Aqui podes encontrar um registo que regista informações sobre as acções que são executadas na consola MDM.

Com o ícone do filtro, podes aplicar filtros à lista apresentada.

Com o menu pendente **Itens por página**: podes selecionar a quantidade de itens a apresentar numa página da lista.

Ação tomada / Definição alterada	A ação que foi tomada / A definição que foi alterada
Valor	O valor da ação tomada / definição alterada
Utilizador	O nome do utilizador que executou a ação / alterou a definição
Data	O carimbo de data/hora de quando esta ação foi realizada/esta definição foi alterada
Caminho / Tipo	O caminho para onde esta ação foi tomada / esta definição foi alterada

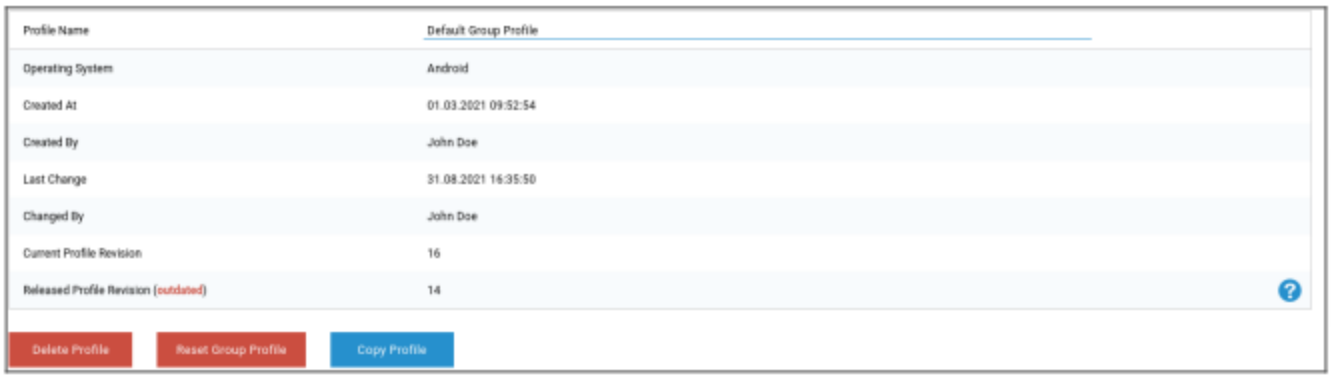
Configuração do iOS

Geral

Dependendo de teres selecionado um grupo ou um dispositivo, o ecrã e os seus subpontos são diferentes - presta atenção a isto!

Síntese do perfil do grupo (apenas a nível do grupo)

Ao abrires um perfil de grupo, terás uma visão geral rápida do perfil



Nome do perfil	Nome do perfil (pode ser alterado aqui)
Sistema operativo	Sistema operativo para o qual o perfil se destina
Criado em	Tempo de criação
Criado por	O criador do perfil
Última alteração	Hora da última modificação do perfil
Alterado por	Conta que efectuou as últimas alterações
Revisão do perfil atual	Revisão do estado do perfil guardado
Revisão do perfil lançado	Revisão do perfil atribuído ("Atribuir agora"). Se a etiqueta apresentar " (desatualizado)" por trás do texto, significa que guardaste o perfil mas ainda não o atribuíste, pelo que os dispositivos continuarão a receber uma versão mais antiga.

Informações gerais

Se estiveres diretamente no aparelho, receberás uma breve descrição do aparelho selecionado.

Nome do dispositivo	Nome do dispositivo
Número de telefone	Número de telefone do dispositivo
Modelo	Número do modelo
Sistema operativo	SO
Número de série	Número de série do dispositivo
Propriedade do dispositivo	Dispositivo empresarial ou privado Corporate = dispositivo corporativo Empregado = dispositivo privado
Tipo de dispositivo	Tipo de dispositivo (Tablet ou Telefone)
Desbloqueado	Se houver um Jailbreak no dispositivo
Supervisionado	Indica se este é um dispositivo supervisionado
Conformidade	Se alguma orientação foi violada
Visto pela última vez	Indica a última vez que o dispositivo comunicou com o servidor AppTec360

Definições

Estas definições contêm o nome do dispositivo e um fundo predefinido.

Nomeia o dispositivo com o nome do sistema	O nome que será emitido na Consola AppTec360 (na estrutura hierárquica esquerda), será o mesmo que no respetivo dispositivo do utilizador final (pode ser consultado nas definições do dispositivo)
Utiliza papel de parede personalizado (apenas dispositivos supervisionados)	Aqui podes pré-definir o fundo que deve ser apresentado no dispositivo do utilizador final (por exemplo, para um tipo de marca corporativa para o dispositivo) Só está disponível no modo supervisionado!
Actualizações automáticas do SO	Força as atualizações do sistema operacional, se disponíveis. Apenas para dispositivos DEP em modo supervisionado.
Fontes personalizadas	Aqui podes adicionar tipos de letra personalizados.
Nome	Optativo. O nome visível para o utilizador do tipo de letra. Este campo é substituído pelo nome real do tipo de letra após a instalação.
Tipo de letra	Carrega o ficheiro do tipo de letra (.otf ou .ttf).

Revisão da configuração

Aqui tens uma visão geral do perfil de grupo que está atribuído ao aparelho.

Se clicares no perfil de grupo, acederás diretamente ao perfil e poderás efetuar definições.

Com o símbolo, podes reverter as aplicações atribuídas para as definições do perfil de grupo.

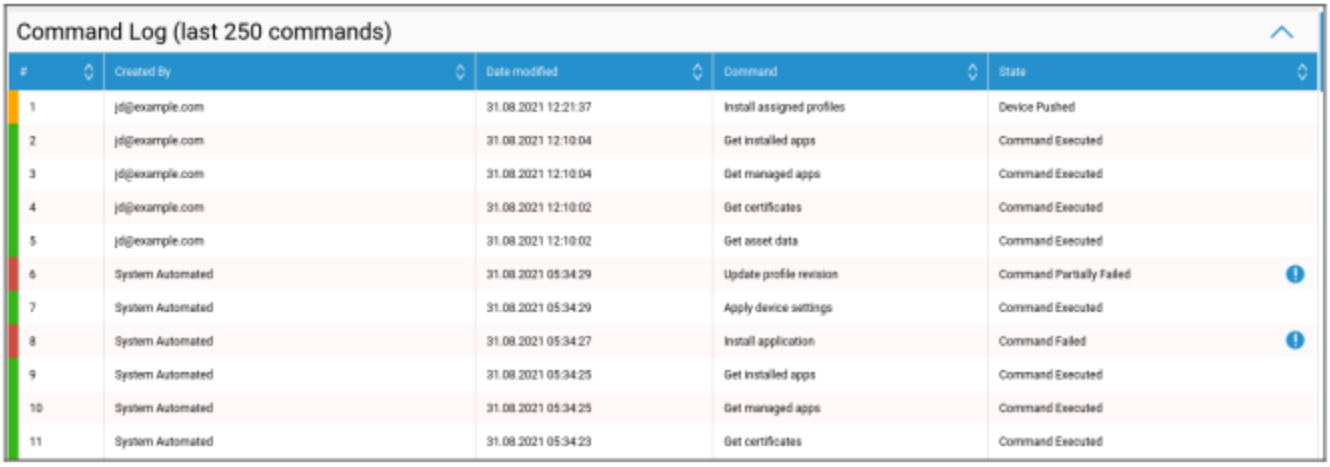
Com o símbolo, podes repor o perfil do dispositivo para que não tenha quaisquer definições.

"Newer Revision available" indica que o perfil de grupo foi alterado e guardado, mas não atribuído. O perfil de grupo tem de ser atribuído com "Atribuir agora" ao nível do grupo para aplicar as alterações aos dispositivos.

Registo do dispositivo (apenas ao nível do dispositivo)

Registo de comandos

Aqui podes ver quais os comandos que foram emitidos para o dispositivo e qual o seu estado.



Os comandos criados por "Sistema automatizado" são automaticamente criados pelo sistema.

Status de comando possíveis

Dispositivo empurrado	Foi enviado um pedido push para o serviço push (por exemplo, APNS) para dizer ao dispositivo para se ligar novamente ao servidor EMM.
Comando criado	O comando foi criado no sistema.
Comando enviado	O comando foi enviado para o dispositivo depois de este se ter ligado ao servidor.
Comando Executado	O comando foi executado com sucesso.
Falha no comando	O comando falhou. *
Comando parcialmente falhado	Dependendo do sistema operativo do dispositivo, alguns comandos podem ser agrupados. Neste caso, algumas partes deste grupo de comandos falharam. *
Comando executado, eventualmente falhou	O comando foi executado, mas talvez não o tenha sido.
Comando repuxado	O comando foi reenviado por um utilizador.
Descartado	O comando foi rejeitado. Por exemplo, porque foi substituído por outro comando ou porque o dispositivo foi registado novamente e os comandos antigos foram removidos

Se houver um ponto de exclamação por trás da mensagem, podes obter mais informações passando o cursor por cima do ícone.

Gestão de activos (apenas a nível do dispositivo)

Gestão de activos (apenas a nível do dispositivo)

Informações sobre o dispositivo

Modelo	Número do modelo do aparelho
Sistema operativo	SO
Versão do SO	Versão do SO
Número de série	Número de série
UDID	UDID do dispositivo
Nome do dispositivo	Nome do dispositivo
Supervisionado	Mostra se o dispositivo é supervisionado
Estado da bateria	Estado da bateria

Wi-Fi

Endereço IP	Endereço IP do dispositivo
WiFi MAC	Endereço MAC WiFi

Celular

Estado	Estado (cartão SIM presente)
Número de telefone	Número de telefone
Estado do roaming	Estado atual do roaming
Roaming (voz/dados)	Estado do roaming para voz/dados
Endereço IP	Endereço IP
IMEI	Número IMEI
Operador/Carrier	Fornecedor de serviços celulares
Rede da operadora SIM	Rede da operadora SIM
Versão para transportadora	Versão de transporte
Firmware do modem	Firmware do modem
Atual MCC/MNC	Ver "SIM MCC/MNC"
SIM MCC/MNC	O código de país móvel é uma identificação de país estabelecida pela UIT de acordo com a norma E.212 Norma que, em conjunto com o código de rede móvel (MNC), é utilizada para identificar uma rede celular (=código do país) Se entrares numa outra rede celular, o "MCC/MNC atual" e o "MCC/MNC SIM" são diferentes.

Bluetooth

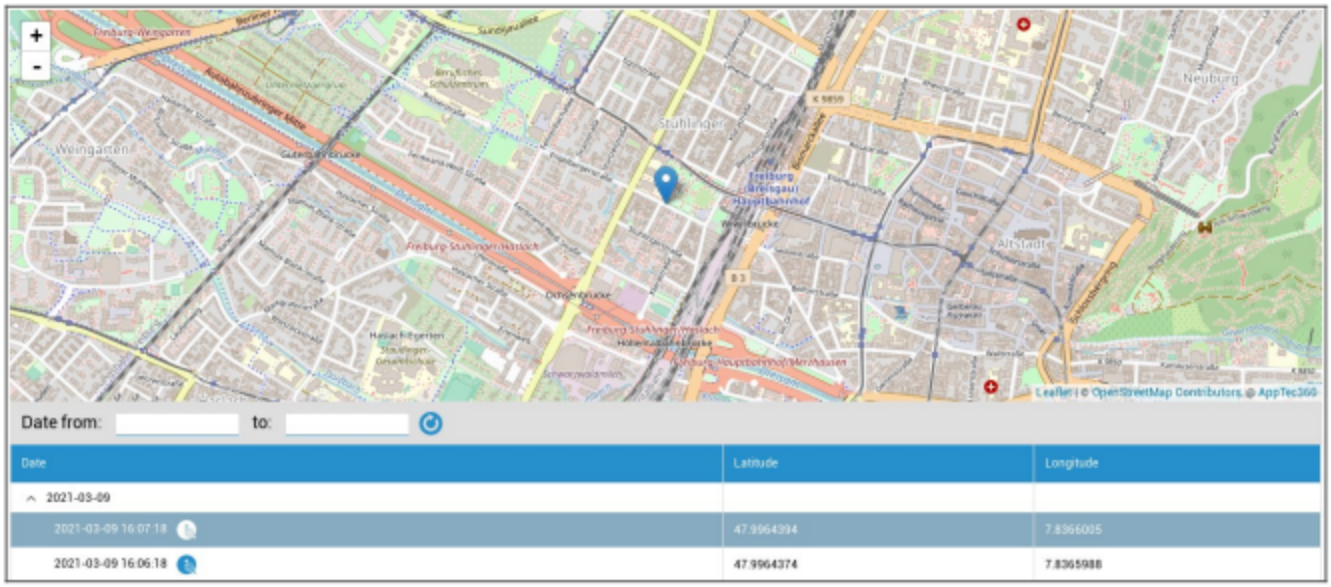
Bluetooth MAC	Endereço MAC Bluetooth

Gestão da segurança

Antirroubo (apenas ao nível do dispositivo)

Informação GPS (apenas ao nível do dispositivo)

Aqui podes avaliar a localização atual/última do aparelho. A localização pode ser protegida com uma ou até duas palavras-passe - Vê: Definições gerais - Privacidade - Acesso ao GPS



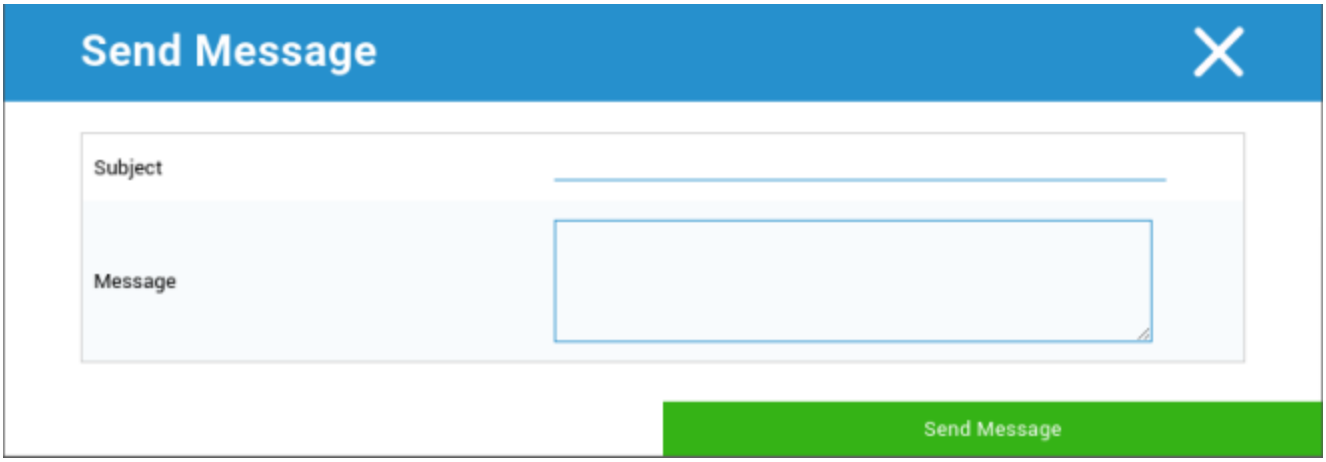
Limpa e bloqueia (apenas ao nível do dispositivo)

Em "Limpar e bloquear", podes realizar as três acções seguintes:

Limpeza total	O dispositivo é restaurado para as definições de fábrica (os dados empresariais e pessoais são eliminados)
Limpeza da empresa	Apenas os dados empresariais são removidos do dispositivo do utilizador final (todas as aplicações, dados, etc. que foram fornecidos pela AppTec)
Bloqueio do ecrã	Se o bloqueio do ecrã estiver ativado, basta desbloquear o dispositivo com a palavra-passe/PIN do dispositivo
Bloqueio forense (apenas dispositivos supervisionados)	Se esta função for activada com o símbolo  , o aparelho será bloqueado, apresentando uma mensagem que não pode ser fechada. O empregado também não pode desbloquear o dispositivo. Só o administrador pode desbloquear o aparelho na consola com o símbolo de desbloqueio  .
Permitir bloqueio de ativação (apenas dispositivos supervisionados)	Se esta função for activada, o dispositivo será bloqueado, assim que a função "Encontrar o meu iPhone" estiver activada nas definições do iCloud

Mensagem (apenas a nível do aparelho)

Com a janela seguinte, podes preencher o assunto e uma mensagem e enviá-la para um dispositivo de utilizador final:



Configuração de segurança

Código de acesso

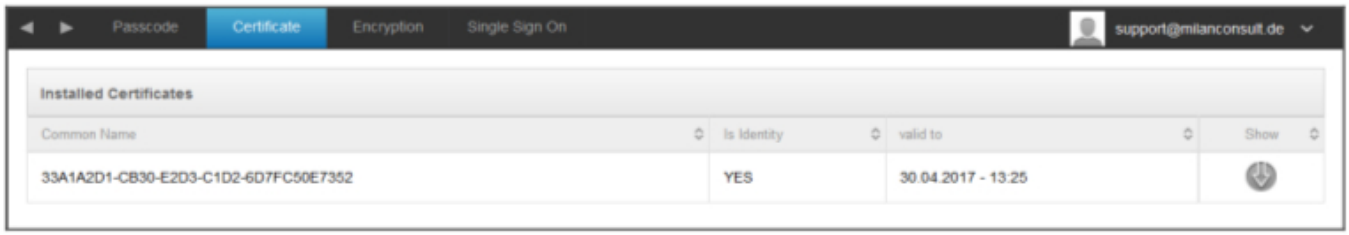
Aqui estabeleces as definições da palavra-passe do aparelho

Desativação do código permitida	Quando esta definição está activada, não é solicitada a introdução de uma palavra-passe A partir do momento em que uma palavra-passe é estabelecida, não pode ser desactivada
Permite um valor simples	Permitir que o utilizador utilize as mesmas sequências de números, escalonadas e reduzidas (ex. 1234, 1111)
Exige um valor alfanumérico	As palavras-passe devem conter pelo menos uma letra
Comprimento mínimo do código de acesso	Comprimento mínimo da palavra-passe
Número mínimo de caracteres complexos	Número mínimo de símbolos alfanuméricos na palavra-passe
Idade máxima do código de acesso	Número de dias, após os quais a palavra-passe deve ser alterada
Bloqueio automático máximo	Tempo máximo após o qual o dispositivo é bloqueado
Período máximo de tolerância para o bloqueio do dispositivo	Tempo, após o qual o dispositivo entra no modo de espera bloqueado
Número máximo de tentativas falhadas	Estabelece a frequência com que uma palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo
Idade máxima da palavra-passe (1-730 dias)	Idade máxima da palavra-passe
Histórico de códigos de acesso (1-50 códigos de acesso)	A utilização de uma palavra-passe antiga é permitida após este número

Um clique no lixo abre a caixa de diálogo de reposição da palavra-passe, com a qual podes apagar uma palavra-passe esquecida do dispositivo.

Certificado (apenas a nível do dispositivo)

Apresenta os certificados que estão disponíveis no dispositivo


Passcode
Certificate
Encryption
Single Sign On
support@mlianconsult.de
Installed Certificates
Common Name
Is Identity
valid to
Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352
YES
30.04.2017 - 13:25

Encriptação

Exige encriptação do armazenamento	Ativar a função de encriptação do dispositivo instalado

Início de sessão único

No ponto "Single Sign-On", podes configurar a autenticação Kerberos.

Aqui, estabelece as credenciais de acesso e os respectivos URLs / Apps que estão autorizados a utilizar os Tokens Kerberos.

Disponível no modo supervisionado	
Nome da conta	Nome da conta
Nome principal	Identidade única para a qual os bilhetes Kerberos podem ser distribuídos
Reino	O teu Kerberos Realm, que deve ser utilizado (ex.: o teu domínio)

Com o Símbolo, podes estabelecer URLs adicionais.

Padrão de URL utilizado para limitar esta conta	URLs a determinar, para os quais os bilhetes Kerberos podem ser distribuídos

Com o Símbolo, podes estabelecer aplicações adicionais.

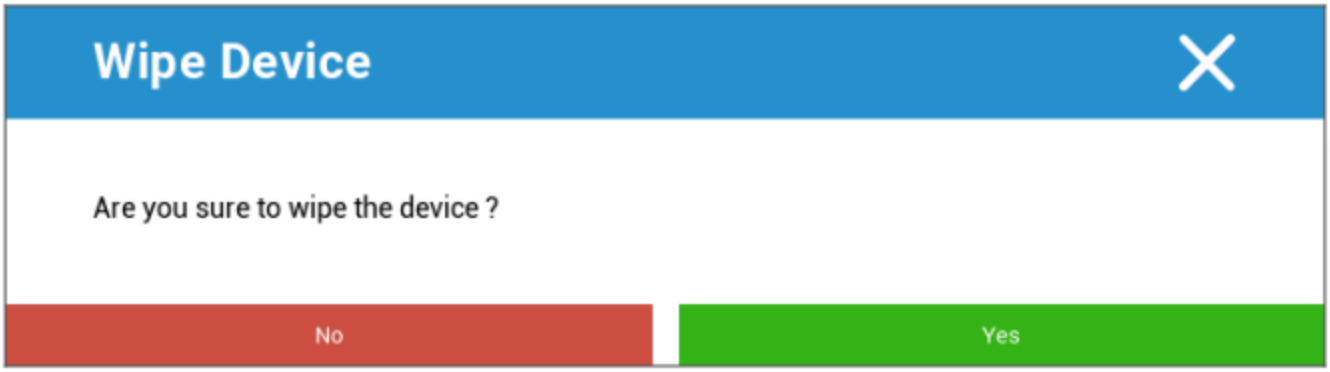
Aplicações para limitar esta conta	A determinar Aplicações, para as quais os bilhetes Kerberos podem ser distribuídos

Fim de vida (apenas a nível do dispositivo)

Limpa (apenas ao nível do dispositivo)

Em "Limpar", podes restaurar o dispositivo para as definições de fábrica. Aqui, os dados empresariais, bem como os dados privados, serão eliminados no dispositivo do utilizador final.

Ao clicares no "Símbolo de menos", deves receber a seguinte mensagem



Com "Sim" podes fazer a limpeza.

Em "Relatório de limpeza", podem ser apresentados os seguintes itens

Limpado por	Histórico de quem realizou a limpeza
Data	Data
Estado	Estado (por exemplo, se a limpeza foi efectuada com êxito)

Definições de restrições

Funcionalidade do dispositivo

Aqui podes bloquear funcionalidades individuais do dispositivo do utilizador final

Permitir a instalação de aplicações	Permite a instalação de aplicações
Permite a câmara	Permite a utilização da câmara
Permitir FaceTime	Permitir FaceTime
Permite a captura de ecrã	Permite a captura de ecrã
Permite a sincronização automática em roaming	Permite a sincronização automática em roaming
Permitir a Siri	Permitir a Siri
Permite a marcação por voz	Permite a marcação por voz
Permite a compra na aplicação	Permite a compra na aplicação
Exige a palavra-passe da iTunes Store para todas as compras	Exige a palavra-passe da iTunes Store para todas as compras
Permite jogos multijogador	Permite jogos multijogador
Permite adicionar amigos do Game Center	Permite adicionar amigos do Game Center
Permite abrir de gerido para não gerido	Permitir a abertura de conteúdos de aplicações geridas em aplicações não geridas
Permite abrir de não gerido para gerido	Permitir a abertura de conteúdos de aplicações não geridas em aplicações geridas
Permite a visualização do dia de hoje no ecrã de bloqueio	Quando esta definição está ativa, a vista "Hoje" é apresentada no Centro de Notificações do ecrã de bloqueio
Permitir o centro de controlo no ecrã de bloqueio	Permitir o Centro de Controlo no ecrã de bloqueio
Permitir TouchID	Permitir TouchID
Permite actualizações da PKI pelo ar	Permite actualizações da PKI pelo ar

Permite a utilização da caderneta quando bloqueada	Permite a utilização da caderneta enquanto o dispositivo está bloqueado
Limita o seguimento de anúncios	Esta função desactiva o Seguimento de Anúncios (por exemplo, os anunciantes não podem utilizar o Seguimento de Anúncios para distribuir anúncios personalizados)
Permitir Handoff	Permitir Handoff
Permitir resultados da Internet em destaque	Permite resultados da Internet em destaque (ex. Bing ou Wikipedia)
Exige um código de acesso no primeiro emparelhamento AirPlay	Exige um código de acesso no primeiro emparelhamento AirPlay
Proteção do pulso do relógio Force	Se estiver ativado, o Apple Watch é forçado a utilizar a "Proteção de pulso" (reconhecimento de pulso)
Permitir a Fototeca iCloud	Permite a Biblioteca de fotografias iCloud. Se não for permitido, todas as imagens que não foram completamente transferidas do iCloud serão apagadas do armazenamento local
Disponível no modo supervisionado	
Permitir a modificação da conta	Permite a modificação de "correio, contactos, calendário".
Permitir AirDrop	Permitir AirDrop
Permitir a modificação celular da aplicação	Esta definição bloqueia a definição das aplicações que podem utilizar dados móveis Esta definição pode, por exemplo, ser definida manualmente no dispositivo do utilizador final e, em seguida, esta restrição pode ser activada
Permite que a Siri consulte conteúdos gerados pelo utilizador a partir da Web	A pesquisa na Web em determinados sítios Web está bloqueada, por exemplo. Wikipédia, porque todos podem fazer alterações à vontade
Ativar o filtro de palavrões da Siri	Os palavrões, dirigidos à Siri, são censurados
Permitir a iBook Store	Permitir a iBook Store
Permitir o Erotismo na iBook Store	Permitir o Erotismo na iBook Store
Permite modificar as definições de Encontrar os meus amigos	Permite modificar as definições de Encontrar os meus amigos

Permite o Game Center	Permite o Game Center
Permite o emparelhamento de anfitriões	Emparelhamento do computador de controlo
Permite a instalação de perfis de configuração	Permite a instalação de perfis de configuração
Permitir Remover aplicação	Remoção de aplicações de controlo
Permitir o iMessage	Permitir o iMessage
Permite apagar todos os conteúdos e definições	Permite apagar todos os conteúdos e definições
Permite a configuração de restrições	Permite a configuração de restrições
Permitir Podcast	Permitir Podcast
Permite a pesquisa de definições	Permite a pesquisa de definições
Permitir teclado preditivo	Permite o teclado preditivo
Permite a correção automática	Permite a correção automática
Permitir a instalação da aplicação UI	Se estiveres desativado, não é possível instalar aplicações da AppStore pública (o ícone deixa de ser apresentado). No entanto, as aplicações ainda podem ser instaladas através do iTunes e do Configurador
Permitir atalhos de teclado	Permite atalhos de teclado, se o dispositivo estiver ligado a um teclado físico
Permitir o emparelhamento do Apple Watch	Proíbe o emparelhamento entre o dispositivo e o Apple Watch, as ligações existentes serão terminadas
Permite a modificação do código de acesso	Se não for permitido, não podes adicionar, alterar ou remover nenhuma palavra-passe de dispositivo
Permite a modificação do nome do dispositivo	Orientação para determinar se o nome do dispositivo pode ser alterado
Permite a modificação do papel de parede	Orientação para determinar se o papel de parede pode ser alterado
Permite transferências automáticas de aplicações	Se estiveres desactivada, uma aplicação comprada não será instalada automaticamente noutros dispositivos. Não se aplica a actualizações de aplicações existentes
Permitir notícias	Permitir notícias no dispositivo iOS

Permite a confiança nas aplicações empresariais	Se definido como falso, impede a confiança nas aplicações empresariais

iCloud

Bloqueia determinadas funcionalidades durante o emparelhamento do iCloud

Permitir cópia de segurança	Permitir cópia de segurança
Permite a sincronização de documentos	Permite a sincronização de documentos
Permitir fluxo de fotos	Permitir fluxo de fotos
Permitir partilha de fotografias	Permitir partilha de fotografias
Permitir a sincronização do chaveiro na nuvem	Permitir a sincronização do chaveiro na nuvem
Permite que as aplicações geridas armazenem dados	Permite que as aplicações geridas armazenem dados
Permite a sincronização de notas e destaques para livros empresariais	Permite a sincronização de notas e destaques para livros empresariais
Permite a cópia de segurança dos livros da empresa	Permite a cópia de segurança dos livros da empresa

Segurança e privacidade

Bloqueia estas funcionalidades associadas aos dados de diagnóstico

Permite o envio de dados de diagnóstico para a Apple	Permite o envio de dados de diagnóstico para a Apple
Permite ao utilizador aceitar certificados TLS não fidedignos	Permite ao utilizador aceitar certificados TLS não fidedignos
Força backups encriptados	Força backups encriptados

BYOD

Segurança incorporada no iOS (contentor)

O iOS sempre foi capaz de distinguir entre gerido (empresarial) e não gerido (privado). Tudo o que vem do sistema MDM é tratado como gerido. Por exemplo, se instalares uma aplicação através da MDM ou configurares uma conta Exchange, esta será tratada como gerida pelo iOS.

Tudo o resto que for configurado/instalado manualmente no dispositivo será tratado como não gerido. Por exemplo, se o utilizador instalar o WhatsApp por si próprio ou se estiver a adicionar uma conta Exchange. No entanto, esta separação nunca afectou os contactos. Mas a partir do iOS 11.3 (e superior), esta funcionalidade também foi adicionada aos contactos.

Uma vez que esta é uma funcionalidade básica do sistema operativo, não precisas de instalar nada nem de configurar um contentor especial.

Ativa a função incorporada para separar aplicações/informações/ficheiros privados e profissionais. Esta definição também desactivará algumas outras funções que, por engano, poderiam desativar partes desta separação.

Ativação

Ativa as Container-Solutions que são suportadas pela AppTec360

Ativar o Google Divide Container	Ativar o Google Divide Container
Ativar o contentor SecurePIM	Ativar o contentor SecurePIM

Se tiveres ativado o SecurePIM Container, encontrarás também o seguinte ponto em "Ativação". Além disso, serão abertos imediatamente mais quatro separadores, que são descritos abaixo.

Endereço de e-mail do suporte	Endereço de correio eletrónico de apoio onde o utilizador se pode dirigir em caso de problemas

Senha do SecurePIM

Em "Palavra-passe SecurePIM", podes definir as orientações para a força de segurança da palavra-passe.

Tempo limite da sessão	Aqui podes estabelecer após quantos minutos uma nova senha deve ser inserida novamente, uma vez que o SecurePIM é executado em segundo plano
Comprimento da palavra-passe	Comprimento da palavra-passe para aceder ao contentor SecurePIM
Caracteres em maiúsculas	Mínimo de caracteres maiúsculos
Caracteres em minúsculas	Mínimo de caracteres minúsculos
Caracteres especiais	Caracteres especiais mínimos
Dígitos	Dígitos mínimos
Aplicação de toalhetes	Número de vezes que uma palavra-passe pode ser introduzida incorretamente, antes de o conteúdo do SecurePIM ser eliminado (A aplicação, no entanto, continua a estar no dispositivo do utilizador final)

Segurança do SecurePIM

Em "Segurança SecurePIM", podes estabelecer uma série de definições de segurança.

Detetar dispositivos com Jailbroken	Se esta definição estiver activada, o acesso ao contentor do SecurePIM será bloqueado, assim que o dispositivo for detectado como jailbroken
Campos de texto seguros	O conteúdo dos campos de envio será encriptado, nenhuma informação chega ao SO (iOS) Nota: Enquanto esta definição estiver ativa, a correção automática deixa de estar disponível
Exportar dados de contacto para o dispositivo	Se esta definição estiver activada, o utilizador tem permissão para exportar os contactos do Exchange para o seu dispositivo local Nota: Apenas o nome e o número de telefone são exportados
Mostra o local do evento	Se esta definição estiver activada, a localização dos próximos eventos será apresentada na barra de notificação
Mostra o título do evento	Se esta definição estiver activada, a localização do título do próximo evento será apresentada na barra de notificação

Navegador SecurePIM

Aqui podes configurar o navegador do SecurePIM.

Com o símbolo, podes definir um novo URL.

Com o símbolo, podes voltar a remover um URL definido.

Os "URLs da lista branca" são URLs que podem ser carregados.

Os "URLs na lista negra" são URLs que não podem ser carregados e, por isso, são bloqueados.

Tem em atenção que as entradas da lista branca têm uma prioridade mais elevada do que as entradas da lista negra. Em "Título do marcador" podes emitir um título. Com "URL do marcador", podes associar o endereço URL ao título do marcador - desta forma, podes distribuir marcadores individualizados aos respectivos utilizadores.

Troca

Em "Exchange" podes configurar uma conta Exchange.

Endereço de e-mail do ActiveSync	Endereço de correio eletrónico do Exchange (toma nota dos "Placeholders")
Início de sessão do ActiveSync Exchange	Troca os nomes de utilizador (toma nota dos "Placeholders")
ActiveSync Exchange Server	Endereço do Exchange Server (FQDN)
Domínio do Exchange ActiveSync	Endereço de domínio do Exchange
Certificado de utilizador	Certificado de utilizador
Autenticação baseada em certificados	O utilizador autentica-se com um certificado
Permite a encriptação S/MIME	Permite ao utilizador encriptar o seu correio
Permite a assinatura S/MIME	Permite ao utilizador assinar o seu correio
Verificação da LCR	Se estiver ativo, o certificado privado será comparado com a LCR (Lista de revogação de certificados)

Gestão de ligações

Wi-Fi

Identificador do conjunto de serviços (SSID)	SSID da rede que deve ser ligada
Auto Join	Ativar a adesão automática ao aderir a uma rede
Rede oculta	Ativar, no caso de o AP não transmitir o SSID

Configuração de proxy

Configuração de um Proxy para cada ponto de acesso

Não tens	Não estabelecer um proxy
Manual	Estabelece um proxy manual
URL do servidor proxy	Endereço para aceder às definições de proxy
Porto	Estabelece a porta para o Proxy
Autenticação	Nome de utilizador para a autenticação no Proxy
Palavra-passe	Palavra-passe para a autenticação no Proxy
Automático	Estabelece um Proxy automaticamente
URL do servidor proxy	URL para aceder às definições de Proxy

Tipo de segurança

Estabelece o tipo de segurança para o PA

WEP	
Palavra-passe	Palavra-passe para o PA

WPA/WPA2	
Palavra-passe	Palavra-passe para o PA

WEP Enterprise - WPA / WPA2 Enterprise - Qualquer empresa			
	Protocolos		
	TLS	Ativar/Desativar	
	TTLS	Ativar/Desativar	
	LEAP	Ativar/Desativar	
	PEAP	Ativar/Desativar	
	EAP-FAST	Ativar/Desativar	
	EAP-SIM	Ativar/Desativar	
	Utiliza o PAC		Utilização do PAC (Protected Access Controll)
	Provisão PAC	Configuração do PAC de provisão	
	Provisiona a PAC de forma anónima	Fornecimento anónimo de CAP	
	Autenticações internas	Protocolo de autenticação que deve ser utilizado: PAP, CHAP, MSCHAP, MSCHAPv2	
	Nome de utilizador	Nome de utilizador de autenticação	
	Não utilizes a palavra-passe por ligação	Não utilizes a palavra-passe por ligação	
	Certificado de identidade	Carrega/selecciona o certificado de autenticação	
	Identidade exterior	Identidade que pode ser vista externamente	
	Confia		
	Certificado de confiança 1	Carrega o primeiro certificado de confiança	
	Certificado de confiança 2	Carrega o segundo certificado de confiança	
	Certificado de confiança 3	Carrega o terceiro certificado de confiança	
	Nomes de certificados de servidores confiáveis	Os nomes dos certificados de servidor esperados (numa lista separada por vírgulas)	

Não tens	Não estabelece nenhuma segurança

VPN

Nome da ligação	Nome do perfil VPN

Tipo de VPN

VPN

Todo o tráfego de rede do dispositivo será encaminhado através de uma ligação VPN.

Tipo de ligação	Estabelece o tipo de ligação VPN
IPsec (cisco)	Protocolo IPsec da cisco
PPTP	Protocolo PPTP
L2TP	Protocolo L2TP
Cisco AnyConnect	Protocolo AnyConnect
Juniper SSL	Protocolo SSL da Juniper
F5 SSL	Protocolo SSL F5
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protocolo VIA da Aruba
SSL personalizado	Ligação através de SSL personalizado
OpenVPN	Protocolo OpenVPN

VPN por aplicação

Quando abres uma determinada aplicação, é estabelecida uma ligação VPN

Inicia automaticamente a ligação VPN por aplicação		Inicia automaticamente a ligação VPN por aplicação
Tipo de ligação		Estabelece o tipo de ligação VPN
	Cisco AnyConnect	Protocolo AnyConnect
	Juniper SSL	Protocolo SSL da Juniper
	F5 SSL	Protocolo SSL F5
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protocolo VIA da Aruba
	SSL personalizado	Ligação através de SSL personalizado
	OpenVPN	Protocolo OpenVPN

Configuração de proxy

Configuração de um Proxy para a ligação VPN

Não tens	Não estabelecer um proxy
Manual	Estabelece manualmente um Proxy
URL do servidor proxy	Endereço para aceder às definições de proxy
Porto	Estabelece a porta para o Proxy
Autenticação	Nome de utilizador para a autenticação no Proxy
Palavra-passe	Palavra-passe para a autenticação no Proxy
Automático	Estabelece um Proxy automaticamente
URL do servidor proxy	URL para aceder às definições de Proxy

Mostrar marcadores de posição	Apresenta todas as variáveis de utilizador disponíveis, que a AppTec360 pode utilizar

APN

Nome do ponto de acesso	Nome do ponto de acesso
Nome do utilizador do ponto de acesso	Nome do utilizador do ponto de acesso
Palavra-passe do ponto de acesso	Palavra-passe do ponto de acesso
Servidor proxy	Endereço do servidor proxy
Porto	A respectiva porta Proxy

Celular

Ativar o roaming de dados	Ativar o roaming de dados
Ativar o Roaming de Voz	Ativar o Roaming de Voz
Ativar Hotspot	Ativar Hotspot

Proxy HTTP

Tipo de proxy	
Manual	Estabelece um Proxy manualmente
URL do servidor proxy	Endereço de acesso às definições de proxy
Porto	Estabelece a porta proxy
Autenticação	Nome de utilizador para a autenticação no Proxy
Palavra-passe	Palavra-passe para a autenticação no Proxy
Automático	Estabelece um Proxy automaticamente
URL do PAC de proxy	URL do PAC de proxy
Permite a ligação direta se o PAC não estiver acessível	Permite a ligação direta (sem VPN), se o PAC não estiver acessível
Permite contornar o proxy para aceder a redes cativas	Permite contornar o proxy para aceder a redes internas cativas

AirPrint

Endereço IP	Endereço IP da impressora
Caminho de recursos	Caminho definido para o dispositivo AirPrint

AirPlay

Nome do dispositivo	Nome do dispositivo
Palavra-passe	Palavra-passe de emparelhamento
Lista branca	Define uma lista de dispositivos, com os quais o dispositivo pode emparelhar-se exclusivamente

Gestão PIM

Exchange Active Sync

Nome da conta	Nome da conta de correio eletrónico
Anfitrião do Exchange ActiveSync	Endereço/FQDN do servidor
Permite mover	Permite a transferência de e-mails
Utiliza apenas no correio	As interacções só podem ocorrer na aplicação de correio nativa
Utiliza SSL	Utiliza a encriptação SSL
Domínio	Domínio do servidor
Utilizador	Nome de utilizador
Endereço de correio eletrónico	endereço de correio eletrónico (apenas a nível do dispositivo)
Palavra-passe (apenas ao nível do aparelho)	Palavra-passe do utilizador
Certificado de identidade	Selecciona o respetivo certificado para autenticação no servidor
Dias anteriores do Mail to Sync	Número de dias, até que os e-mails sejam sincronizados novamente. Sem limite = ilimitado
Ativar S/MIME	Ativar a encriptação S/MIME
Assina o certificado	Carrega o respetivo certificado de assinatura
Certificado de encriptação	Carrega o respetivo certificado de encriptação

eMail

Configuração de contas POP3 / IMAP no dispositivo do utilizador final

Descrição da conta	Nome das contas de e-mail		
Tipo de conta	IMAP	Prefixo do caminho	O prefixo do caminho para pastas especiais
	POP		
Nome de exibição do utilizador	Nome de apresentação do utilizador		
Endereço de e-mail	Endereço de correio eletrónico do utilizador		
Permite mover	Permite a transferência de e-mails		
Ativar S/MIME	Ativar a encriptação S/MIME		
Assina o certificado	Carrega o respetivo certificado de assinatura		
Certificado de encriptação	Carrega o respetivo certificado de encriptação		

Correio de entrada

Definições do servidor de entrada

Endereço do servidor de correio eletrónico	Endereço do servidor de correio eletrónico
Porta do servidor de correio	Porta do servidor de correio
Nome do utilizador	Nome do utilizador correspondente
Tipo de autenticação	Tipo de autenticação
Não tens	Não Tipo de autenticação
Palavra-passe (apenas ao nível do aparelho)	Solicitação da palavra-passe
Desafio-Resposta MDM	
NTLM	NTLM-Autenticação
HTTP MD5 Digest	
Utiliza SSL	Utiliza SSL, se necessário

Correio de saída

Definições do servidor de saída

Endereço do servidor de correio eletrónico	Endereço do servidor de correio eletrónico
Porta do servidor de correio	Porta do servidor de correio
Nome do utilizador	Nome do utilizador correspondente
Tipo de autenticação	
Não tens	Nenhum método de autenticação
Palavra-passe (apenas ao nível do aparelho)	Solicitação da palavra-passe
Desafio-Resposta MDM	
NTLM	NTLM-Autenticação
HTTP MD5 Digest	
Utiliza SSL	Utiliza SSL, se necessário
Senha de saída igual à de entrada	Senha de saída igual à de entrada

Utiliza apenas no correio	Ativar, se todas as mensagens de correio eletrónico de saída tiverem de ser enviadas através da aplicação de correio eletrónico

CalDav

Configura a instalação e a distribuição de uma conta CalDav

Descrição da conta	Nome de exibição da conta
Nome do anfitrião	Nome do anfitrião e/ou endereço IP
Porto	Porta da conta CalDav
URL principal	URL principal da conta
Nome de utilizador	Nome de utilizador CalDav correspondente
Palavra-passe (apenas ao nível do aparelho)	Respectiva palavra-passe CalDav
Utiliza SSL	Utiliza SSL, se necessário

Calendários subscritos

Configuração e distribuição de Calendários Subscritos

Descrição	Nome de exibição da conta
URL	URL da base de dados do calendário
Nome de utilizador	Nome de utilizador da subscrição do calendário
Palavra-passe (apenas ao nível do aparelho)	Palavra-passe da subscrição do calendário
Utiliza SSL	Utiliza SSL, se necessário

LDAP

Nesta área, configura uma ligação LDAP, de modo a permitir uma troca dinâmica de certificados entre o dispositivo do utilizador final e o Active Directory.

Tem em atenção que o utilizador selecionado necessita da respectiva permissão de leitura.

Descrição da conta	Descrição da conta
Nome de utilizador da conta	Utilizador para acesso LDAP
Palavra-passe da conta	Palavra-passe para o acesso LDAP
Nome de anfitrião da conta	Nome de anfitrião/endereço IP do servidor LDAP

Utiliza SSL	Utiliza SSL, se necessário

Na segunda parte, podes definir filtros individuais para pesquisar no registo LDAP.

Descrição	Âmbito de aplicação	Pesquisa na base
Descrição do filtro	Nível de pesquisa no registo LDAP	Define o filtro individual

Gestão Web

Webclips

Neste local, define os marcadores, com ligações a páginas Web, portais de intranet, etc., que serão visíveis como uma aplicação no dispositivo do utilizador final.

Etiqueta	Nome da ligação no dispositivo do utilizador final
URL	Ligação ao respetivo sítio Web
Removível	Se estiver ativado, o utilizador pode remover o webclip
Ícone	Através desta caixa de diálogo, carrega um logótipo para a ligação: Dimensões 180x180, formato png
Ícone pré-composto	Se estiveres ativado, não serão apresentados efeitos adicionais (sombra, reflexo) no ícone
Ecrã inteiro	Ao abrir webclips, o browser abre no modo de ecrã inteiro

Filtro de conteúdo da Web

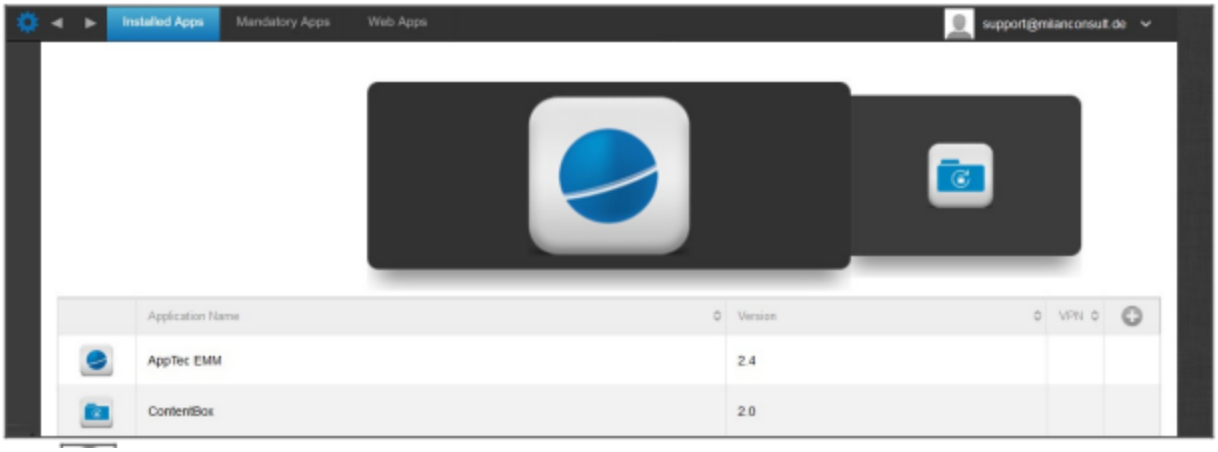
O filtro de conteúdo da Web permite limitar o acesso a páginas específicas da Internet.

Sítios Web permitidos	
Limita o conteúdo para adultos	O Webfilter é aplicado automaticamente para conteúdos para adultos
URLs permitidos	Com o símbolo + adiciona páginas permitidas
URLs na lista negra	Com o símbolo + adiciona páginas bloqueadas
Apenas sítios Web específicos	Só podem ser apresentados conteúdos específicos, que podes adicionar com o símbolo +.

Gestão de aplicações

Gestor de aplicações empresariais

Aplicações instaladas (apenas ao nível do dispositivo)



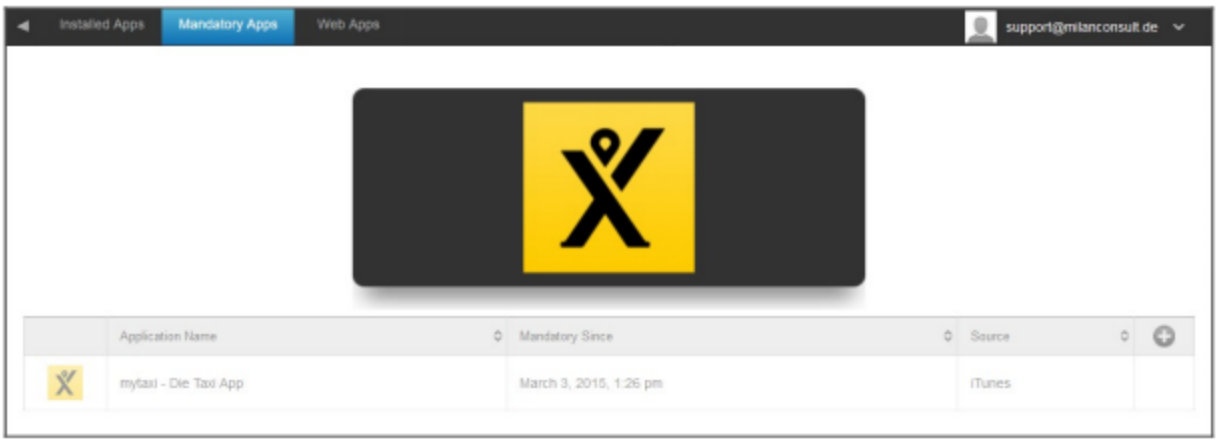
Aqui podes ver as aplicações que estão atualmente instaladas no dispositivo.

Aplicações obrigatórias

Em Aplicações obrigatórias, podes impor as aplicações necessárias.

O utilizador será continuamente lembrado de instalar esta aplicação.

Através do , podes definir a aplicação obrigatória.



Pode ser uma aplicação da Apple App Store, mas também uma aplicação interna.

Se se tratar de um dispositivo supervisionado, a aplicação será instalada automaticamente.

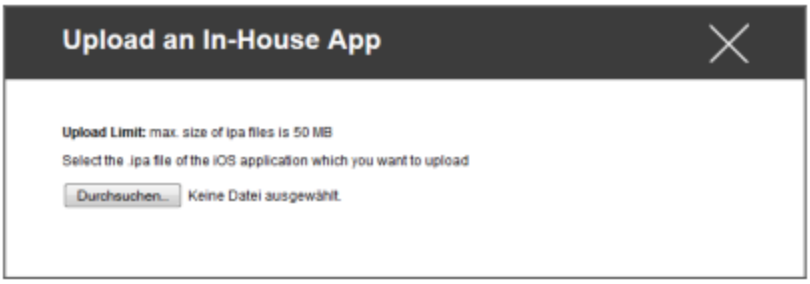
Podes enviar uma aplicação "Apple AppStore" da AppStore pública para o dispositivo, bem como uma aplicação interna desenvolvida internamente.

Ou podes selecionar a categoria "Aplicações internas do iOS" e escolher uma aplicação interna que tenhas carregado nas Definições gerais.

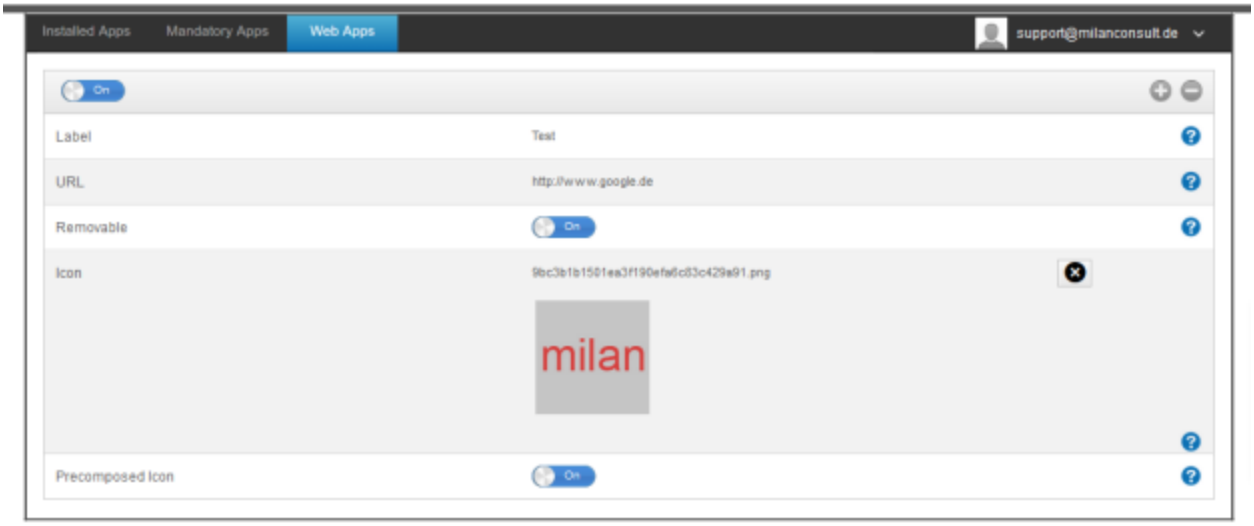
Opções de instalação

Mantém-te atualizado (apenas suportado para VPP por dispositivo)	Uma vez por semana, será determinado se existe uma atualização para a aplicação. Se sim, esta atualização será instalada Para as aplicações internas, o destino de atualização que configuraste nas definições gerais será utilizado para o processo de atualização.
Ultrapassa quando não é gerido	Se a aplicação já estiver instalada, a MDM assume o controlo da aplicação e gere-a
Remove a aplicação quando o perfil MDM é removido	No caso de uma remoção da gestão de dispositivos, a aplicação será desinstalada
Evita a cópia de segurança dos dados da aplicação	Não será criada uma cópia de segurança dos dados específicos da aplicação
Definição da aplicação	Em "Definições da aplicação", podes atribuir à aplicação determinados valores para o primeiro plano (desde que a aplicação o suporte, se necessário pergunta ao programador da aplicação).

Também podes selecionar e carregar diretamente um ficheiro ipa, através de "Upload In-House App".



Aplicações Web



No ponto "Web Apps", podes, à semelhança do que acontece com os "Web Clips", enviar páginas da Internet ou portais de intranet como uma aplicação para o dispositivo do utilizador final, na área da Gestão Web. Por predefinição, as aplicações Web são apresentadas no modo de ecrã inteiro, que pode ser configurado em Webclips.

Etiqueta	Nome da ligação no dispositivo do utilizador final
URL	Ligação ao respetivo sítio Web
Removível	Se estiver ativado, o utilizador pode remover o Webclip
Ícone	Através desta caixa de diálogo, carrega um logótipo para a ligação: Dimensões 180x180, formato png
Ícone pré-composto	Se estiveres ativado, não serão apresentados efeitos adicionais (sombra, reflexo) no ícone

Restrições e definições

Aplicações colocadas na lista negra / na lista branca

Aqui podes definir as aplicações que são bloqueadas (ou permitidas), dependendo das tuas definições em "Definições gerais". Se clicares, aparecerá a pesquisa de aplicações conhecidas. Aí podes procurar as aplicações que pretendes adicionar.

Nota que é necessário um dispositivo supervisionado para esta função

Restrições da SysApp

Bloqueia aplicações ou funções específicas do teu dispositivo

Permite a utilização do YouTube	Permite a utilização do YouTube
Permite a utilização da iTunes Store	Permite a utilização da iTunes Store
Permite a utilização do Safari	Permite a utilização do Safari
Ativar o preenchimento automático	Permite o preenchimento automático
Alerta de fraude da força	Força o aviso de fraude
Ativar JavScript	Permite a utilização de JavaScript
Bloqueia pop-ups	Bloqueia todos os tipos de pup-ups
Permitir cookies	Escolhe quando o Safari aceita cookies

App-VPN

Através do símbolo, podes definir as aplicações que lançarão automaticamente a ligação VPN selecionada no arranque.

Definições da aplicação

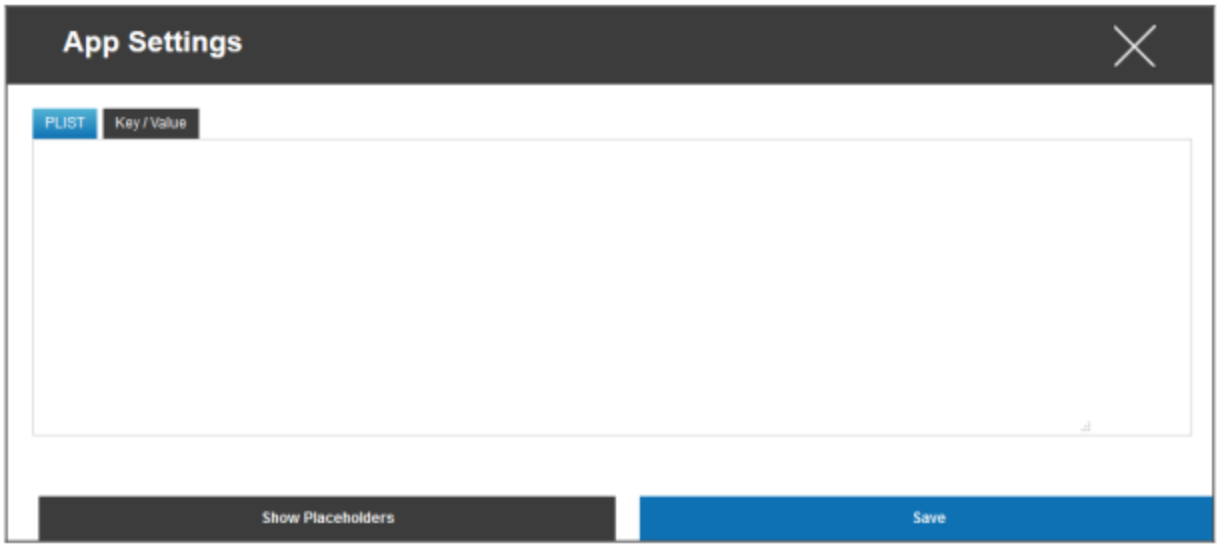
Em "Definições da aplicação", podes atribuir à aplicação determinados valores para o primeiro plano (desde que a aplicação o suporte, se necessário pergunta ao programador da aplicação).

Através do símbolo, adicionas uma aplicação (adicional). Vais encontrar, mais uma vez, a representação familiar da AppTec360 de uma App-Import.

Procura aqui a aplicação que queres configurar e selecciona-a. As definições só se aplicam às aplicações geridas.

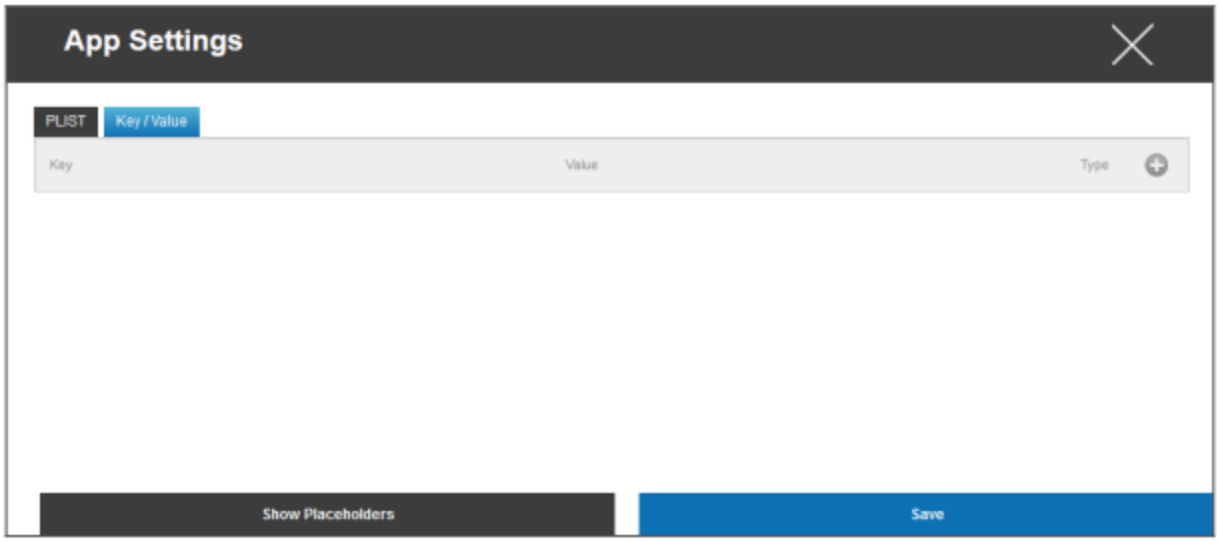
Se a importação tiver sido bem sucedida, verás o seguinte ecrã:

Agora, com um clique em , podes efetuar uma variedade de configurações. Receberás então o seguinte resumo:

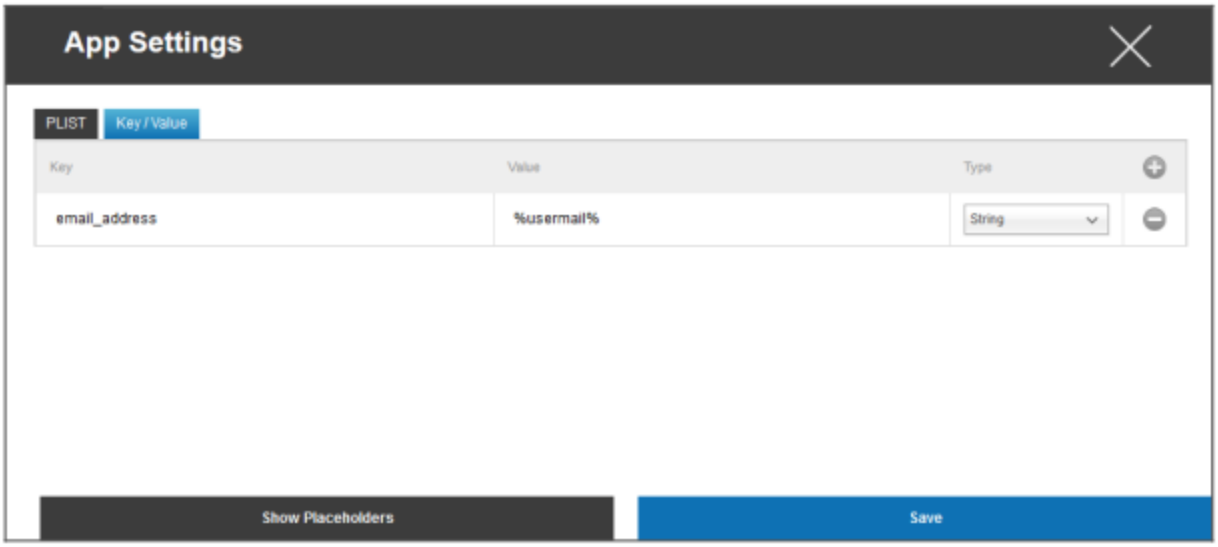


Se já tiveres uma PLIST (texto de origem da configuração), podes adicioná-la aqui e guardar tudo com "Guardar".

Em "Chave / Valor", podes anexar configurações específicas à aplicação



Aqui, podes estabelecer uma nova chave e o seu valor com o símbolo.



Naturalmente, todos os marcadores de posição da AppTec estão à tua disposição

Explicação de "Tipo":

Cordas	Texto
Booleano	Verdadeiro/Falso
Número	Número

Com o símbolo, podes voltar a remover uma aplicação.

Loja de aplicações para empresas

Aplicações iTunes

Neste ponto, podes distribuir aplicações opcionais para o teu utilizador.

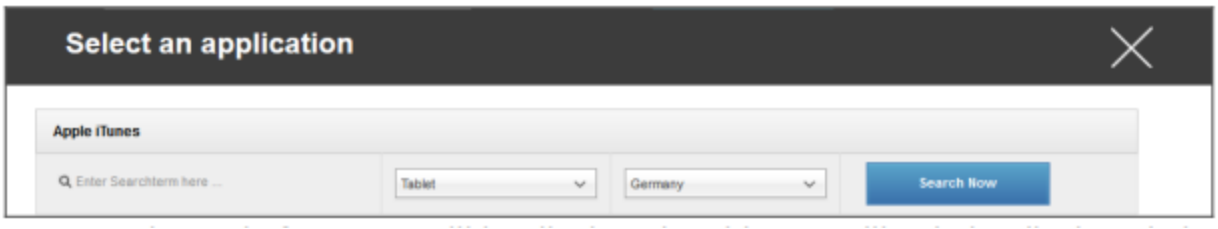
Se houver uma aplicação aqui, esta será instalada automaticamente no dispositivo do utilizador final da AppTec360 Store.

Estas são simplesmente ligações para a Apple App Store oficial. Por este motivo, cada dispositivo do utilizador final tem de ser equipado com uma ID da Apple.

Nesta altura, recomendamos que cada utilizador tenha o seu próprio ID Apple.

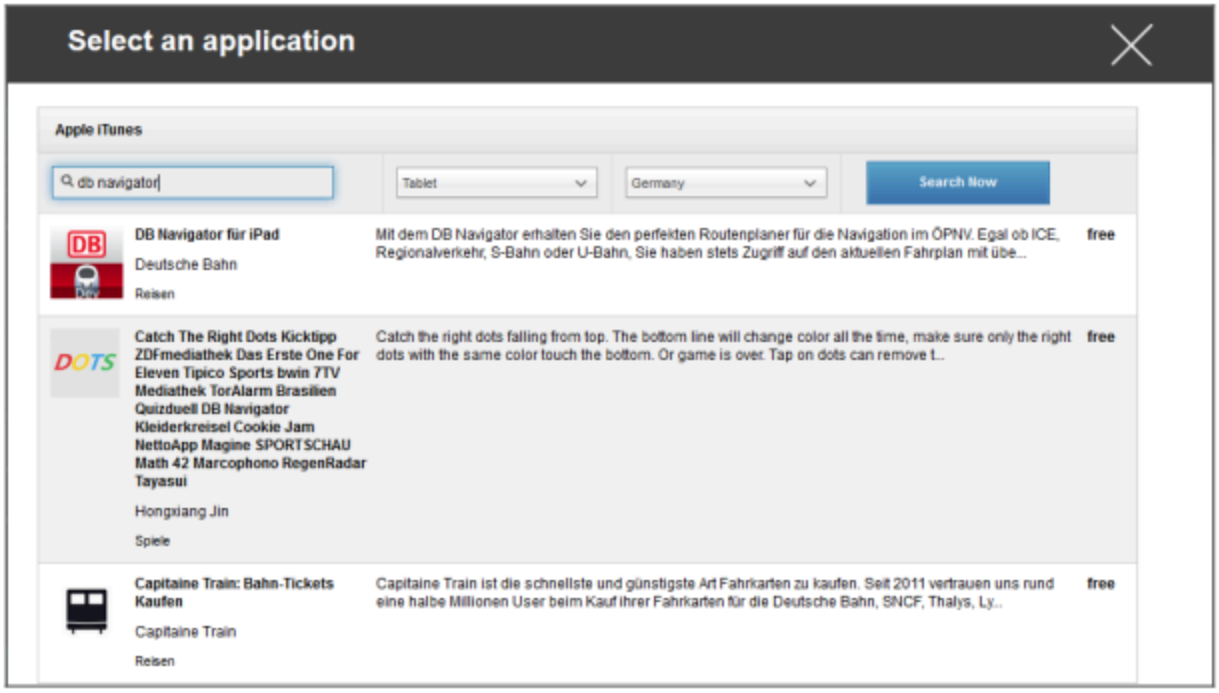
Com o símbolo, podes adicionar outras aplicações.

Depois disso, abre uma janela com a seguinte visão geral.



Tem em atenção que só serão apresentadas as aplicações gratuitas, as aplicações pagas só serão apresentadas através de VPN.

Em "Introduzir termo de pesquisa aqui...", podes procurar uma aplicação que esteja na Apple App Store.



Depois de clicares no ícone ou no nome da aplicação, ser-te-á pedido novamente que efectues configurações adicionais.

Mantém-te atualizado	Uma vez por semana, será determinado se existe uma atualização para a aplicação. Se sim, esta atualização será instalada
Remove a aplicação quando o perfil MDM é removido	No caso de uma remoção da gestão de dispositivos, a aplicação será desinstalada
Evita a cópia de segurança dos dados da aplicação	Não será criada uma cópia de segurança dos dados específicos da aplicação
App-VPN	Selecciona uma ligação VPN, que será iniciada ao abrir a aplicação

Depois de clicares em "Instalar", a aplicação será adicionada à Enterprise App Store e pode ser instalada no dispositivo do utilizador final, através da AppTec360 AppStore.

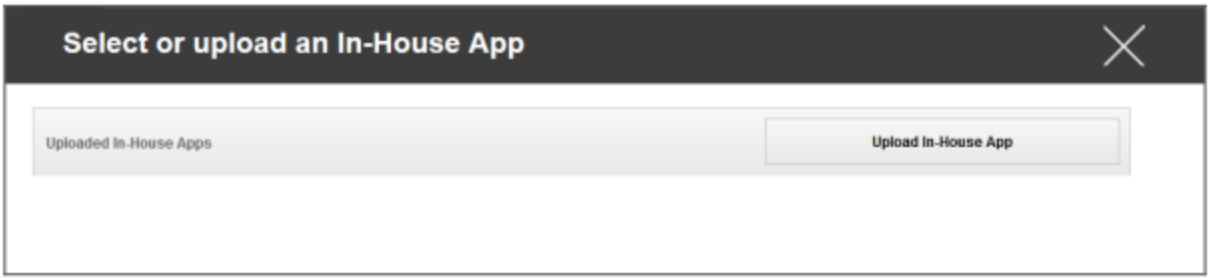
Se a importação da App-Store tiver sido bem sucedida, receberás a seguinte visão geral:

Internamente

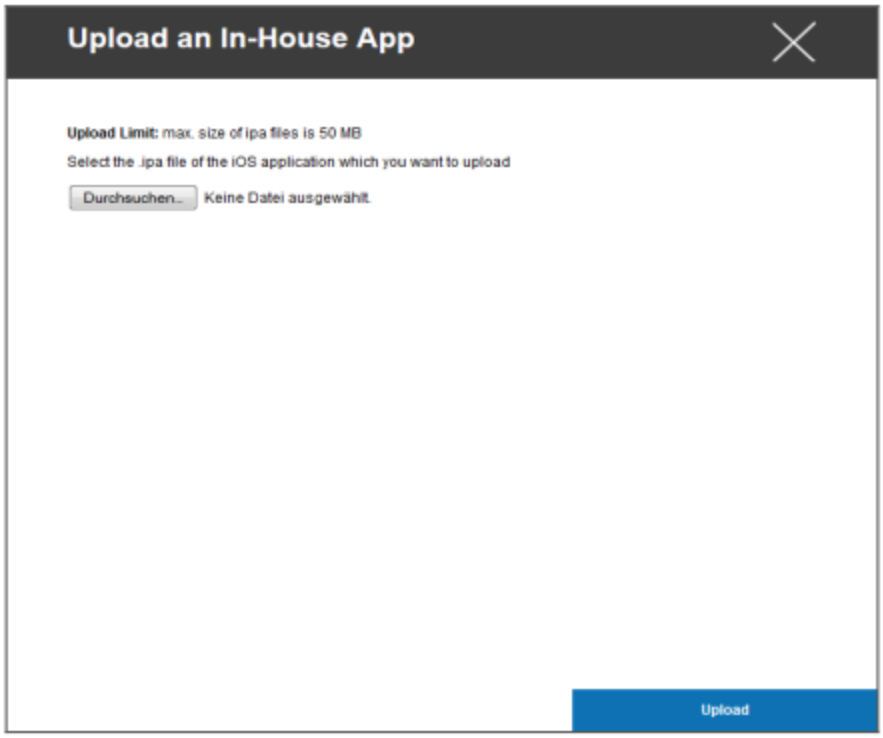
No ponto "In-House", podes carregar aplicações desenvolvidas internamente e distribuí-las.

Com o símbolo, podes distribuir mais aplicações internas.

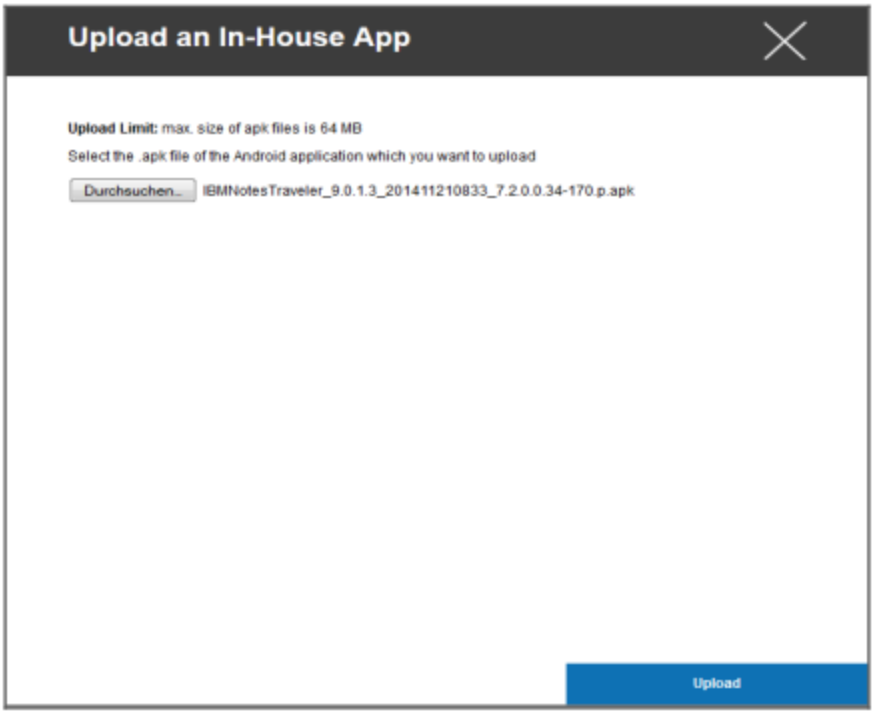
Se nunca distribuíste a aplicação In-House, receberás a seguinte visão geral:



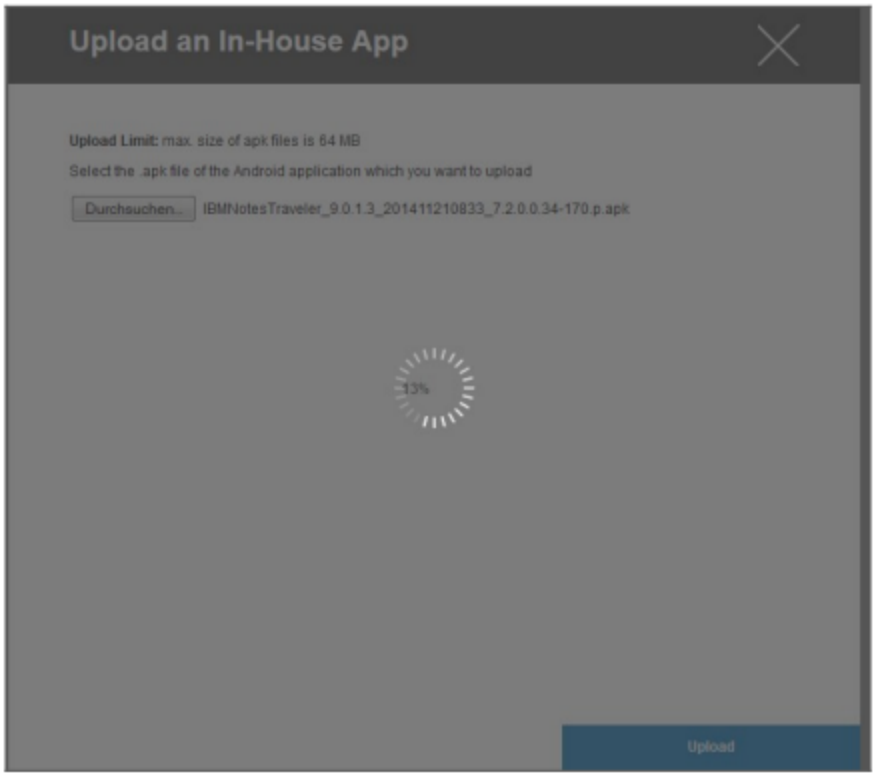
Para isso, clica em "Upload In-House App", e receberás a seguinte visão geral:



Agora, selecciona com "Procurar..." um ficheiro .ipa e depois clica em "Carregar"



A tua aplicação será agora carregada. No meio do círculo, podes ver a percentagem da quantidade da tua aplicação que já foi carregada.



Se o carregamento da aplicação interna tiver sido efectuado com êxito, verás a aplicação recentemente carregada no teu Catálogo de Aplicações.

O utilizador tem agora a opção de ver e instalar esta aplicação na AppTec360 Store no dispositivo do utilizador final, na categoria "In-House".

Devido ao facto de não envolver uma aplicação pública da Apple AppStore, o utilizador não necessita de um ID Apple armazenado no dispositivo do utilizador final.

Modo quiosque

O Modo Quiosque iOS só está disponível no Modo Supervisionado

O Modo Quiosque permite-te pré-definir uma aplicação ou URL, para que seja possível executar/visitar exclusivamente essa aplicação/URL.

Além disso, podes desativar vários botões de hardware no Modo Quiosque.

Tipo de aplicação

Embalagem

Se quiseres lançar a aplicação no modo Quiosque, selecciona "Pacote" em "Tipo de aplicação"

Aplicação de quiosque	Clica aqui para selecionar uma aplicação que deve ser iniciada no modo de quiosque Encontra a visão geral atual da Gestão de aplicações Podes selecionar entre "Apple iTunes Apps" e "iOS In-House Apps"

URL

Se quiseres lançar um URL no modo de quiosque, selecciona "URL" em "Tipo de aplicação"

URL	Agora, define o endereço URL pretendido
Política de mesma origem	Se esta função estiver ativa, o utilizador só pode navegar nas subpáginas do URL predefinido Por exemplo, se tiveres definido o seguinte URL: www.mypage.com, então o utilizador pode navegar em www.mypage.com/subpage
URLs na lista branca	Aqui podes manter uma Whitelist, todos estes URLs são permitidos Máximo de 1 URL por linha Um URL deve começar por http:/ ou https://
URLs na lista negra	Aqui podes manter uma Lista Negra, todos estes URLs não são permitidos Máximo de 1 URL por linha Um URL deve começar por http:/ ou https://
Limpa o navegador após inatividade	Após inatividade, a cache do navegador será esvaziada
Senha de saída activada	Se activares esta função, o utilizador tem a opção de terminar o Modo Quiosque com uma palavra-passe predefinida por ti
Sair da palavra-passe	Esta é a palavra-passe que foi predefinida por ti

Definições do modo de quiosque

Modo de quiosque programado	Com base na hora do dia, podes definir o Modo Quiosque, para que o modo seja iniciado e terminado automaticamente a uma hora pré-determinada
Hora de início	Hora de início
Tempo em minutos	Tempo, em minutos, após o qual o modo de quiosque deve ser novamente encerrado
Desativar o toque	Se estiver ativado, o ecrã tátil é desativado
Desativar a rotação do dispositivo	Se estiver ativado, a adaptação automática do ecrã é desactivada
Desativar o interrutor de toque	Se estiveres ativado, o interrutor de toque será desativado. A partir daí, o comportamento depende da função previamente definida
Desativar os botões de volume	Se estiveres ativado, os botões de volume serão desactivados
Desativar o botão Sleep Wake	Se estiveres ativado, o interrutor de ligar/desligar será desativado
Desativar o bloqueio automático	Se estiver ativado, o aparelho não passa para o modo de espera
Ativar o Voice Over	Se estiveres ativado, o Assistente de voz será ativado
Ativar o zoom	Se estiver ativado, o zoom será ativado
Ativar a inversão de cores	Se ativado, o modo de visualização invertido será ativado
Ativar o Assistive Touch	Se estiver ativado, o AssistiveTouch será ativado
Ativar a seleção de voz	Se estiver ativado, a seleção de voz será activada
Ativar o áudio mono	Se estiver ativado, o áudio mono será ativado
Comando de voz	Se estiver ativado, o utilizador pode ativar o VoiceOver
Zoom	Se estiver ativado, o utilizador pode ativar o Zoom
Inverte as cores	Se estiver ativado, o utilizador pode ativar as cores invertidas
Toque de assistência	Se estiver ativado, o utilizador pode ativar o toque de assistência

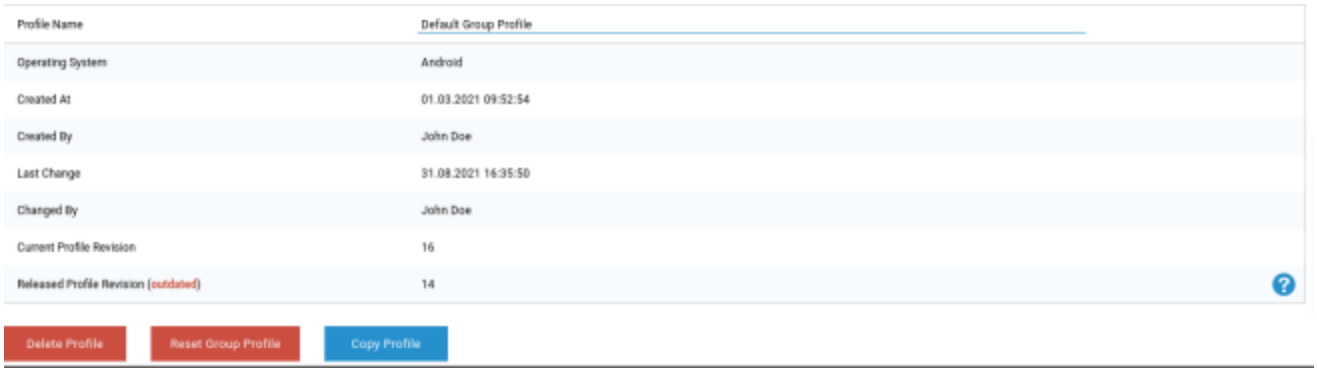
Android Enterprise – Configuração de dispositivos totalmente gerida

Dependendo de teres selecionado um perfil de grupo ou um dispositivo, a síntese e os seus subpontos são diferentes - tem isto em atenção!

Geral

Síntese do perfil do grupo (apenas a nível do grupo)

Ao abrires um perfil de grupo, terás uma visão geral rápida do perfil.



Nome do perfil	Nome do perfil (pode ser alterado aqui)
Sistema operativo	Sistema operativo para o qual o perfil se destina
Criado em	Tempo de criação
Criado por	O criador do perfil
Última alteração	Hora da última modificação do perfil
Alterado por	Conta que efectuou as últimas alterações
Revisão do perfil atual	Revisão do estado do perfil guardado
Revisão do perfil lançado	Revisão do perfil atribuído ("Atribuir agora"). Se a etiqueta apresentar " (desatualizado)" por trás do texto, significa que guardaste o perfil mas ainda não o atribuíste, pelo que os dispositivos continuarão a receber uma versão mais antiga.

Síntese do dispositivo (apenas ao nível do dispositivo)

Se estiveres num dispositivo, receberás uma recapitulação geral do dispositivo selecionado, que contém o seguinte:

Nome do dispositivo	Nome do dispositivo
Localização	Coordenadas de localização
Número de telefone	Número de telefone
Atribuição de aplicações obrigatórias	Número de aplicações obrigatórias atribuídas
Versão do SO	Versão do sistema operativo do dispositivo
Sistema operativo	Sistema operativo (Android Enterprise)
Número de série	Número de série do dispositivo
Propriedade do dispositivo	Dispositivo empresarial ou privado
Tipo de dispositivo	Dispositivo gerido pelo AE Work
Enraizado	Estado, indicando se o dispositivo foi enraizado
Conformidade	Em conformidade com as directrizes
Endereço IP	Endereço IP do dispositivo
Visto pela última vez	Ponto no tempo, quando o dispositivo se ligou pela última vez à AppTec
Último empurrão	Ponto no tempo, quando o último push foi enviado para o dispositivo
Modo de proprietário do dispositivo AE	Sim
Atribuição de utilizadores	O utilizador ou grupo a que este dispositivo está atribuído

Config Revision (apenas a nível do dispositivo)

Aqui tens uma visão geral do perfil de grupo que está atribuído ao aparelho.

Se clicares no perfil de grupo, terás acesso direto a esse perfil e poderás efetuar definições.

Com este símbolo, podes reverter as aplicações distribuídas para as definições do perfil de grupo.

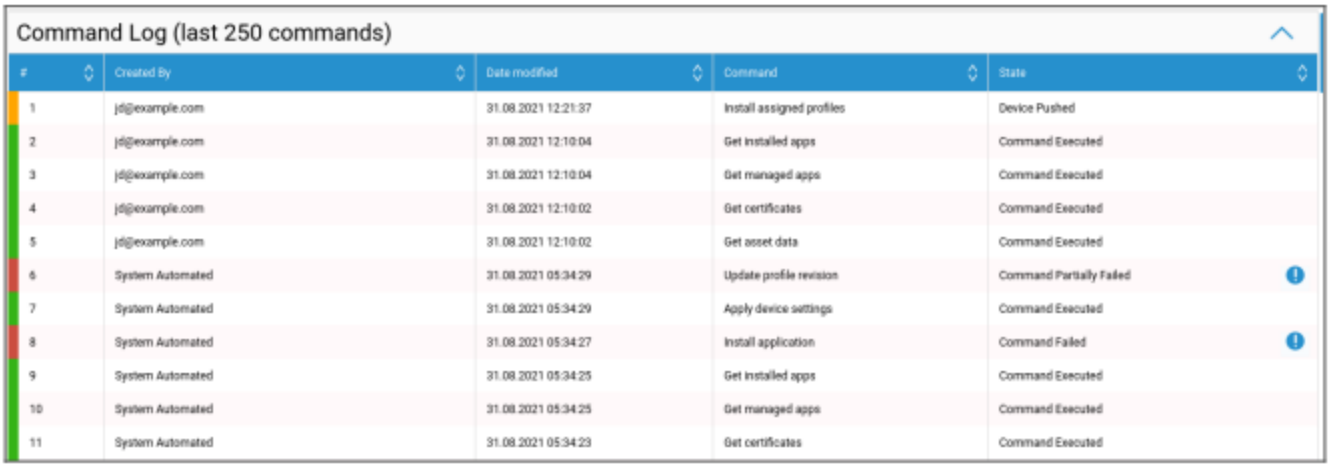
Com este símbolo, podes reverter todas as aplicações utilizadas para as definições do perfil de grupo.

"Newer Revision available" indica que o perfil de grupo foi alterado e guardado, mas não atribuído. O perfil de grupo tem de ser atribuído com "Atribuir agora" ao nível do grupo para aplicar as alterações aos dispositivos.

Registo do dispositivo (apenas ao nível do dispositivo)

Registo de comandos

Aqui podes ver quais os comandos que foram emitidos para o dispositivo e qual o seu estado.



Os comandos criados por "Sistema automatizado" são automaticamente criados pelo sistema.

Status de comando possíveis

Dispositivo empurrado	Foi enviado um pedido push para o serviço push (por exemplo, APNS) para dizer ao dispositivo para se ligar novamente ao servidor EMM.
Comando criado	O comando foi criado no sistema.
Comando enviado	O comando foi enviado para o dispositivo depois de este se ter ligado ao servidor.
Comando Executado	O comando foi executado com sucesso.
Falha no comando	O comando falhou. *
Comando parcialmente falhado	Dependendo do sistema operativo do dispositivo, alguns comandos podem ser agrupados. Neste caso, algumas partes deste grupo de comandos falharam. *
Comando executado, eventualmente falhou	O comando foi executado, mas talvez não o tenha sido.
Comando repuxado	O comando foi reenviado por um utilizador.
Descartado	O comando foi rejeitado. Por exemplo, porque foi substituído por outro comando ou porque o dispositivo foi registado novamente e os comandos antigos foram removidos

Se houver um ponto de exclamação por trás da mensagem, podes obter mais informações passando o cursor por cima do ícone.

Definições do dispositivo

Configuração do cliente

Aqui podes efetuar as seguintes configurações no teu dispositivo Android:

Tempo fora de conformidade	O limite de tempo limite de resposta do utilizador após o qual a ação de execução é aplicada.
Ação de execução após o tempo limite de cumprimento	Ação de execução quando um utilizador não executa acções que conduzam a um estado de dispositivo conforme
Frequência da recolha de dados	Frequência com que as informações do dispositivo/GPS devem ser recolhidas
Frequência de batimento cardíaco do dispositivo	Intervalo em que o dispositivo deve contactar o servidor AppTec360 Min. 1 minuto Máximo. 24 horas
Ativar actualizações de localização	Se estiver ativado, o dispositivo envia actualizações de localização para o servidor AppTec360
Localização Hora de atualização	Determina em que intervalos de tempo o dispositivo envia actualizações de localização para a AppTec360
Utilizar a precisão da localização do Google para a atualização da localização	Se estiver activada, a localização da rede será utilizada para actualizações de localização (se estiver desactivada em "Restrições", esta definição não afectará nada)
Utilizar a localização GPS para atualizar a localização	Se estiver ativado, o GPS será utilizado para atualizar a localização
Permitir locais simulados (falsos)	Permite a falsificação de informações de localização através de aplicações de terceiros
Ação de ligação perdida	Se estiver ativado, podes especificar uma ação para o caso de um dispositivo não obter uma ligação ao servidor MDM no intervalo de pulsação. Por exemplo, se o dispositivo tiver um tempo de pulsação de 5 minutos, liga ao servidor às 10:35 AM. Depois disso, o dispositivo sai do alcance do Wi-Fi. O próximo heartbeat às 10:40 AM falhará e a ação especificada será executada.
Ação	A ação que deve ser tomada assim que um dispositivo se torna não-conforme.

	• Bloquear dispositivo = bloqueia o dispositivo • Limpar dispositivo = o dispositivo será restaurado para as definições de fábrica • Limpar dispositivo e cartão SD = o dispositivo será restaurado para as definições de fábrica e o armazenamento do cartão SD será eliminado
Limiar	Podes especificar um limiar de batimentos cardíacos falhados que são necessários para desencadear a ação especificada.

Modo de aplicação da política	Não cumpre a norma:	Os utilizadores serão solicitados periodicamente a executar acções pendentes
	Aplicação de política preguiçosa:	Nunca será pedido aos utilizadores que executem acções pendentes. Todas as acções abertas serão mostradas no cliente AppTec360
	Aplicação agressiva de políticas:	Os utilizadores serão solicitados ininterruptamente a executar acções pendentes
AppTec360 Version Lock	Se ativado, pode ser especificado um código de versão para o AppTec360 MDM Client. O cliente AppTec360 só será atualizado para a versão especificada. As versões mais recentes serão ignoradas. NÃO é possível fazer um downgrade.	
Código da versão	Código da versão para o Cliente MDM AppTec360 a ser bloqueado.	
Desativar a notificação AppTec360	Se estiveres desativado, o Cliente AppTec360 não mostrará uma Notificação na Barra de Notificações. Assim, os utilizadores podem fechar o cliente AppTec360 através do gestor de tarefas. Se o cliente AppTec360 estiver fechado, várias funcionalidades, incluindo o Kiosk Mode e a App Black/Whitelisting, não funcionarão corretamente. Os dispositivos Samsung oferecem um mecanismo de proteção para o Cliente AppTec360. A notificação está desactivada por predefinição nos dispositivos Samsung que suportam as APIs KNOX. A notificação não deve ser desactivada em dispositivos com Android 8.0 ou superior.	

Papel de parede

Define um papel de parede personalizado	Ativar/desativar o papel de parede personalizado
Papel de parede	Define o modo de papel de parede para utilizar um código de cores ou uma imagem
Especifica uma cor	Especifica uma cor de fundo como valor hexadecimal, por exemplo, #000000 para preto ou #ffffff para branco
Definir imagem como papel de parede	Carrega o ficheiro de imagem que pretendes utilizar como papel de parede

Gestão de activos (apenas a nível do dispositivo)

Informações sobre o dispositivo

Modelo	Designação do modelo do aparelho
Sistema operativo	SO
Versão do SO	Versão do SO
Número de série	Número de série
Nome do dispositivo	Nome do dispositivo
Estado da bateria	Estado da bateria
Memória livre / total	Memória livre / total
Samsung Safe	Interface Samsung SAFE, necessária para uma variedade de opções de definição
Cartão SD disponível	Cartão SD disponível
Emulação de cartão SD	Cartão SD emulado
Cartão SD amovível	Cartão SD amovível
SD Livre / Memória Total	SD Free / Memória total do cartão SD

Wi-Fi

Endereço IP	Endereço IP do dispositivo
WiFi MAC	Endereço MAC WiFi

Celular

Estado	Estado (cartão SIM instalado)
Número de telefone	Número de telefone
Roaming (Voz / Dados)	Roaming para voz / dados
Estado do roaming	Estado atual do roaming
Endereço IP	Endereço IP
Operador/Carrier	Operador/Carrier
Tecnologia celular	Tecnologia celular
IMEI	Número IMEI
ICCID	Esta é a identificação do cartão SIM, muitas vezes também um Smartcard ou um cartão de circuito integrado (ICC)
IMSI	O International Mobile Subscriber Identity (IMSI) fornece, nas redes móveis GSM e UMTS, uma identificação definitiva dos utilizadores da rede O IMSI é composto por um máximo de 15 dígitos e é configurado da seguinte forma: • Código de país móvel (MCC), 3 dígitos • Código de rede móvel (MNC), 2 ou 3 dígitos • Número de identificação do assinante móvel (MSIN), 1-10 dígitos
Atual MCC/MNC	Ver "SIM MCC/MNC"
SIM MCC/MNC	O código de país móvel é um identificador de país estabelecido, definido pela UIT de acordo com a norma E.212 Padrão. Trabalha em conjunto com o código de rede móvel (MNC) para a identificação da rede móvel. Significa o país/código de rede móvel do cartão SIM. Se fizeres roaming para outra rede móvel, logicamente, o "Current MCC/MNC" e o "SIM MCC/MNC" serão diferentes.

Bluetooth

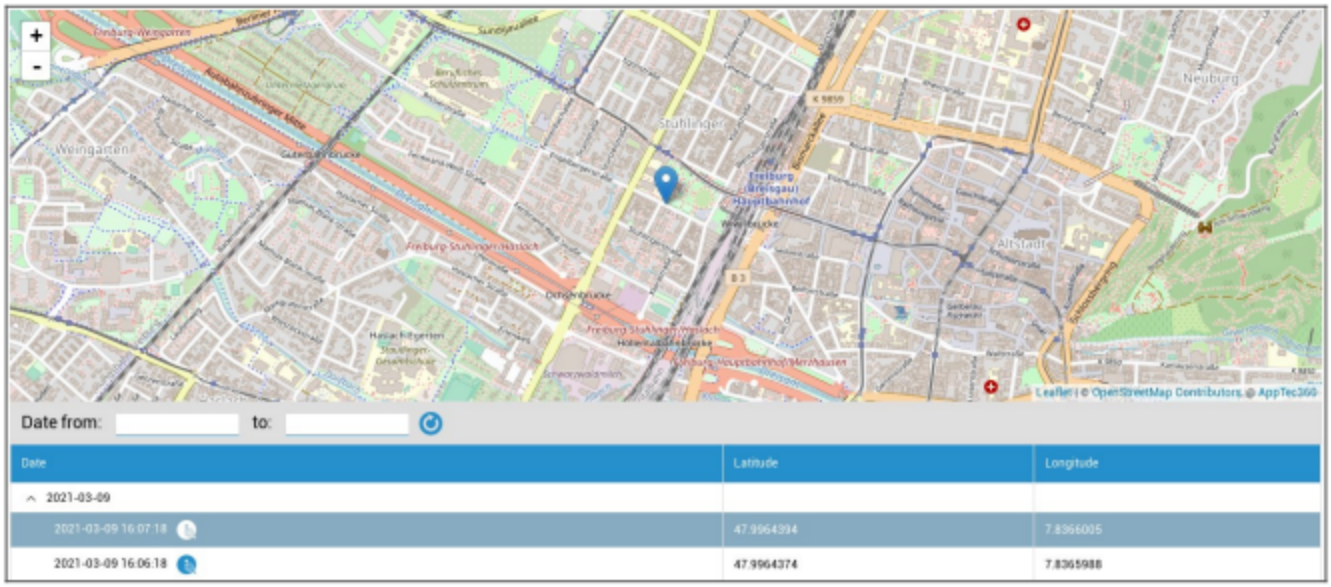
Bluetooth MAC	Endereço MAC Bluetooth

Gestão da segurança

Antirroubo (apenas ao nível do dispositivo)

Informação GPS (apenas ao nível do dispositivo)

Aqui podes determinar a localização atual/última do aparelho. A localização pode ser protegida com uma ou até duas palavras-passe - Vê: Definições gerais - Privacidade - Acesso ao GPS



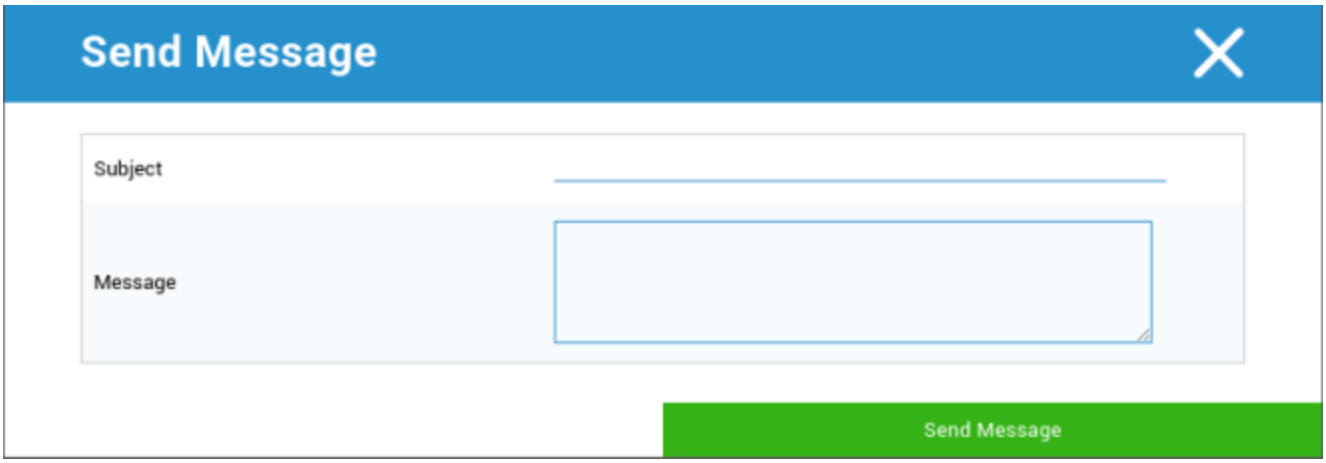
Limpa e bloqueia (apenas ao nível do dispositivo)

Em "Limpar e bloquear", podes realizar as três acções seguintes:

Limpeza total	O dispositivo é restaurado para as definições de fábrica (os dados empresariais e pessoais são eliminados)
Limpeza da empresa	Apenas os dados empresariais são removidos do dispositivo do utilizador final (todas as aplicações, dados, etc. que foram fornecidos pela AppTec360)
Bloqueio do ecrã	Se o bloqueio do ecrã estiver ativado, basta desbloquear o dispositivo com a palavra-passe/PIN do dispositivo

Mensagem (apenas a nível do aparelho)

Aqui podes preencher o assunto e uma mensagem e enviá-la para um dispositivo de utilizador final.



Configuração de segurança

Código de acesso do dispositivo

Em "Código de acesso" podes definir uma palavra-passe para o dispositivo, estando disponíveis as seguintes opções de definição

Comprimento mínimo da palavra-passe	Estabelece o número mínimo de símbolos que uma palavra-passe deve ter	
Qualidade da palavra-passe	Não especificado	Esta política não prevê requisitos para a palavra-passe.
	Biometria Fraca	Esta política permite a utilização de tecnologia de reconhecimento biométrico de baixa segurança. Isto implica tecnologias que possam reconhecer a identidade de um indivíduo até cerca de um PIN de 3 dígitos (a deteção falsa é inferior a 1 em 1.000).
	Alguma coisa	Esta política requer a definição de algum tipo de palavra-passe ou padrão, mas não impõe quaisquer regras específicas.
	Alfabético	O utilizador deve ter introduzido uma palavra-passe que contenha pelo menos caracteres alfabéticos (ou outro símbolo).
	Alfanumérico	O utilizador deve ter introduzido uma palavra-passe que contenha, pelo menos, caracteres numéricos e alfabéticos (ou outro símbolo).
	Complexo	O utilizador deve ter introduzido uma palavra-passe que contenha pelo menos uma letra, um dígito numérico e um símbolo especial, por defeito. Com esta qualidade de palavra-passe, as palavras-passe podem ser restringidas a conter vários conjuntos de caracteres, como pelo menos uma letra maiúscula, etc.
Comprimento mínimo da palavra-passe	Define o número necessário de caracteres para a palavra-passe. Por exemplo, podes exigir que o PIN ou as palavras-passe tenham pelo menos seis caracteres.	
Mínimo de dígitos numéricos exigidos na palavra-passe	Mínimo de dígitos numéricos exigidos na palavra-passe	

Mínimo de letras minúsculas exigidas na palavra-passe	Mínimo de letras minúsculas exigidas na palavra-passe
Mínimo de letras maiúsculas exigidas na palavra-passe	Mínimo de letras maiúsculas exigidas na palavra-passe
Mínimo de caracteres não alfabéticos exigidos na palavra-passe	Mínimo de caracteres não alfabéticos exigidos na palavra-passe
Símbolos mínimos exigidos na palavra-passe	Símbolos mínimos exigidos na palavra-passe

Bloqueio do tempo máximo de inatividade	Inatividade máxima do utilizador até ao bloqueio de tempo
Tempo limite de expiração da palavra-passe	Estabelece, após o que a palavra-passe expira e tem de ser emitida uma nova palavra-passe
Restrição do histórico de palavras-passe	Número de palavras-passe utilizadas anteriormente que não são permitidas
Máximo de tentativas falhadas da palavra-passe	Estabelece a frequência com que uma palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo
Permite a autenticação biométrica	Permite a autenticação através da leitura de impressões digitais ou da íris. Apenas para Samsung KNOX 2.1 e superior

AntiVírus

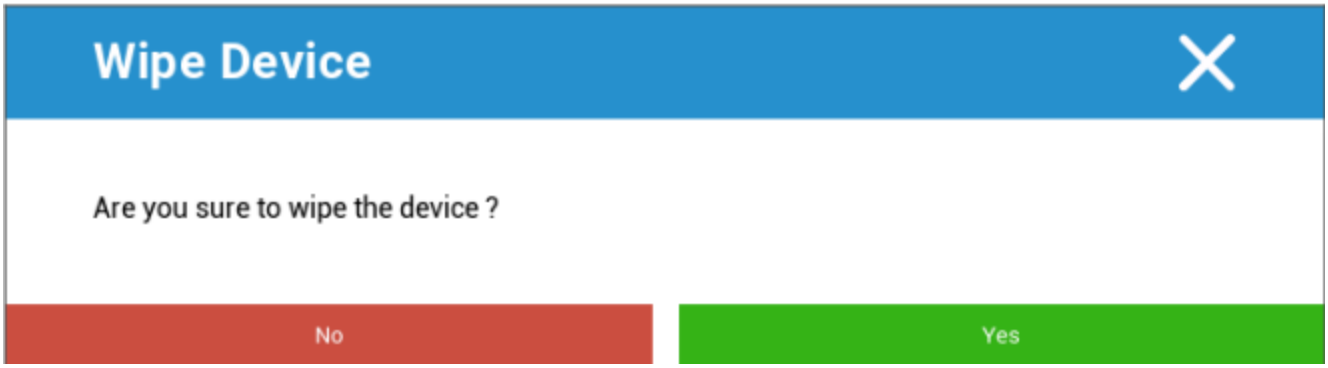
Verificação automática	Ativar as verificações automáticas periódicas
Intervalo de digitalização	Intervalo para exame (rápido / completo)
Verificação automática completa	Ativar as verificações automáticas completas
Actualizações automáticas	Ativar actualizações automáticas
Intervalo de verificação de atualização	Com que frequência a aplicação e a sua base de dados devem ser actualizadas (vírus / código danificado)
Proteção de aplicações	Ativar a verificação automática de aplicações
Proteção do cartão SD	Ativar a verificação automática do cartão SD
Atualização apenas de Wi-Fi	Quando ativado, as actualizações só serão aplicadas quando o dispositivo estiver ligado com êxito a uma rede Wi-Fi

Fim de vida (apenas a nível do dispositivo)

Limpa (apenas ao nível do dispositivo)

Em "Limpar", podes restaurar o dispositivo para as definições de fábrica. Aqui, os dados empresariais, bem como os dados privados, serão eliminados no dispositivo do utilizador final.

Ao clicar no "Símbolo de Menos" recebes a seguinte mensagem:



Com "Sim" podes fazer a limpeza.

Em "Relatório de limpeza", podem ser apresentados os seguintes itens

Limpado por	Histórico de quem realizou a limpeza
Data	Data
Estado	Estado (por exemplo, se a limpeza foi efectuada com êxito)

Definições de restrições

Restrições

Aqui, é possível restringir e bloquear uma série de coisas.

Ativar a câmara	Permite a utilização da câmara	
Forçar sincronização automática	Ligado	A sincronização está permanentemente activada
	Desliga	A sincronização está permanentemente desactivada
	Escolha do utilizador	Selecionado pelo utilizador
Forçar Bluetooth	Ligado	O Bluetooth está permanentemente ativado
	Desliga	O Bluetooth está permanentemente desativado
	Escolha do utilizador	Selecionado pelo utilizador
Forçar GPS	Ligado	O GPS está permanentemente ativado
	Desliga	O GPS está permanentemente desativado
	Escolha do utilizador	Selecionado pelo utilizador
Localização da rede de forças	Ligado	Localização permanente na Internet
	Desliga	Desativação permanente da localização na Internet
	Escolha do utilizador	Selecionado pelo utilizador

Segurança		
Não permitir a localização da partilha	Especifica se um utilizador não está autorizado a ativar a partilha de local.	
Não permitir o arranque seguro	Especifica se o utilizador não tem permissão para reiniciar o dispositivo no modo de arranque seguro.	
Não permitir a reinicialização da rede	Especifica se um utilizador não está autorizado a repor as definições de rede a partir das Definições.	
Não permitir a reposição de fábrica	Especifica se um utilizador não está autorizado a repor o dispositivo.	
Ativar ADB	Permite a ligação a um PC através de ADB	
Desativar o Keyguard	Desactiva o Keyguard	
Proprietário do dispositivo Informações do ecrã de bloqueio	Define a informação do proprietário do dispositivo a ser mostrada no ecrã de bloqueio.	
Aplicação da conformidade	Modo Prompt Utilizador	O utilizador será convidado a realizar as acções necessárias.
	Contentor de bloqueio de modo	Oculta todas as aplicações até que todos os requisitos sejam cumpridos

Gestão de aplicações	
Permitir ligações entre aplicações de perfil	Permite que as aplicações no perfil principal tratem de ligações Web a partir do perfil gerido.
Não permitir o controlo de aplicações	Especifica se um utilizador não está autorizado a modificar aplicações nas Definições ou nos lançadores.
Não permitir a instalação de aplicações	Especifica se um utilizador não está autorizado a instalar aplicações.
Não permitir a desinstalação de aplicações	Especifica se um utilizador não está autorizado a desinstalar aplicações.
Política de permissão de tempo de execução	Especifica como serão tratados os novos pedidos de permissão das aplicações.
Permitir fontes desconhecidas	Se estiver ativado, os utilizadores podem fazer o sideload de aplicações instalando um ficheiro .apk.

Conectividade	
Não permitir a configuração da rede móvel	Especifica se um utilizador não está autorizado a configurar redes móveis.
Desautoriza a configuração de Tethering	Especifica se um utilizador não está autorizado a configurar o Tethering e os hotspots portáteis.
Não permitir a configuração VPN	Especifica se um utilizador não está autorizado a configurar uma VPN.
Não permitir a configuração Wifi	Especifica se um utilizador não está autorizado a alterar os pontos de acesso WiFi.
Não permitir o feixe NFC de saída	Especifica se o utilizador não está autorizado a utilizar NFC para transmitir dados de aplicações.
Bloqueia a configuração WiFi	Esta definição controla se as configurações de WiFi criadas por uma aplicação Proprietário do dispositivo devem ser bloqueadas (ou seja, ser editáveis ou removíveis apenas pela aplicação Proprietário do dispositivo, nem mesmo pela aplicação Definições).
Ativar o roaming de dados	Ativa o Roaming de dados

Bluetooth	
Não permitir Bluetooth	Especifica se o bluetooth não é permitido no dispositivo. Necessita do Android 8.0
Não permitir a partilha Bluetooth	Especifica se a partilha Bluetooth de saída não é permitida no dispositivo. Necessita do Android 8.0
Não permitir a configuração Bluetooth	Especifica se um utilizador não está autorizado a configurar o Bluetooth.

Gestão de contas	
Não permitir a adição de perfil gerido	Especifica se um utilizador não está autorizado a adicionar perfis geridos. Necessita do Android 8.0
Não permitir a adição de utilizadores	Especifica se um utilizador não está autorizado a adicionar novos utilizadores.
Não permitir Remover perfil gerido	Especifica se os perfis geridos deste utilizador podem ser removidos, exceto pelo respetivo proprietário do perfil. Necessita do Android 8.0
Não permitir a modificação da conta	Especifica se um usuário não pode adicionar e remover contas, a menos que elas sejam adicionadas programaticamente pelo Authenticator.

Telefonia	
Não permitir chamadas de saída	Especifica que o utilizador não está autorizado a fazer chamadas telefónicas de saída.
Não permitir SMS	Especifica que o utilizador não está autorizado a enviar ou receber mensagens SMS.

Sistema	
Não permitir a criação de janelas	Especifica que as janelas para além das janelas da aplicação não devem ser criadas.
Não permitir definir o ícone do utilizador	Especifica se um utilizador não está autorizado a alterar o seu ícone.
Não permitir definir papel de parede	Restrição de utilizador para não permitir a definição de um papel de parede.
Desativar a barra de estado	A desativação da barra de estado bloqueia as notificações, as definições rápidas e outras sobreposições de ecrã que permitem escapar a um dispositivo de utilização única.
Ativar a hora automática	Define a hora automaticamente.
Ativar o fuso horário automático	Define o fuso horário automaticamente.
Mantém-se ligado enquanto estiver ligado à corrente	O dispositivo mantém-se ativo enquanto estiver ligado a uma fonte de alimentação.

Armazenamento	
Não permitir a desativação da verificação da aplicação	Especifica se um utilizador não está autorizado a desativar a verificação da aplicação.
Não permite a montagem de suportes físicos	Especifica se um utilizador não está autorizado a montar suportes físicos externos.
Ativar o serviço de cópia de segurança	O serviço de cópia de segurança gere todos os mecanismos de cópia de segurança e de restauro no dispositivo. Se definir este valor como falso, impede a criação de cópias de segurança ou o restauro de dados. O serviço de cópia de segurança está desativado por predefinição. Necessita do Android 8.0
Ativar o armazenamento em massa USB	Ativa a utilização do armazenamento em massa USB.

Teclado	
Não permitir o preenchimento automático	Especifica se um utilizador não está autorizado a utilizar os serviços de preenchimento automático. Necessita do Android 8.0
Não permitir copiar e colar entre perfis	Especifica se o que é copiado na área de transferência deste perfil pode ser colado em perfis relacionados.

Som	
Não permitir o ajustamento do volume	Especifica se um utilizador não está autorizado a ajustar o volume principal.
Desativar o microfone	Especifica se um utilizador não está autorizado a ajustar o volume do microfone.
Silenciar dispositivo	Silencia o dispositivo.

Gestão de certificados

Aqui podes distribuir Certificados de Confiança e Certificados de Identidade aos teus dispositivos.

O Android 8 ou superior é necessário para distribuir Certificados Fidedignos e o Android 9 ou superior é necessário para distribuir Certificados de Identidade.

Com o "+" podes adicionar vários certificados.

Os certificados de confiança têm de estar no formato PEM.

Os certificados de identidade têm de estar no formato PKCS12

Gestão de ligações

Wifi

Para esta definição, efectua a pré-configuração dos dispositivos do utilizador final, para aceder ao acesso interno
Pontos

Identificador do conjunto de serviços (SSID)	SSID da rede a ser conectada
Rede oculta	Ativar, no caso de o AP não transmitir o SSID

Tipo de segurança

Estabelece o tipo de segurança do PA

WEP

Palavra-passe	Palavra-passe para o PA

WPA/WPA2

Palavra-passe	Palavra-passe para o PA

802.1x EAP

Método EAP

PWD	Identidade	Identidade
	Palavra-passe	Palavra-passe

PEAP	Protocolo de autenticação de fase 2	nenhum	Nenhum protocolo adicional
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidade	Identidade	
	Identidade anónima	Identidade anónima	
	Palavra-passe	Palavra-passe	

TTLS	Protocolo de autenticação de fase 2	nenhum	Nenhum protocolo adicional
		PAP	Protocolo PAP
		MSCHAP	Protocolo MSCHAP
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidade	Identidade	
	Identidade anónima	Identidade anónima	
	Palavra-passe	Palavra-passe	

TLS	Certificado CA	Certificado CA
	Identidade	Identidade
	Palavra-passe	Palavra-passe

VPN

Nome da ligação	Nome da ligação VPN

Tipo de VPN

VPN

Cliente VPN

Cliente VPN AppTec360	
Configuração da porta de entrada	Selecciona a Configuração VPN da Gateway (Ver **Definições Gerais > Gateway Universal > Definições VPN**)
VPN sempre ativa	Ativar o bloqueio nativo
Ativar o bloqueio do AppTec360	Ativar o bloqueio do AppTec360

Integrado (apenas disponível em dispositivos Samsung)			
Tipo de ligação	PPTP	Servidor	Servidor
		Ativar a encriptação PPTP	Ativar a encriptação PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Ativar o segredo L2TP	Ativar o segredo L2TP
		Segredo L2TP	Segredo L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
Domínios de pesquisa DNS	Domínios de pesquisa DNS		
Definições de especialistas	Servidores DNS	Servidores DNS	
	Encaminhamento de rotas	Encaminhamento de rotas	

Abre a VPN		
Servidor	Servidor	
Perfil OpenVPN	Perfil OpenVPN	
Aplicação OpenVPN	OpenVPN para Android (recomendado)	
	Ligação OpenVPN	
Definições de especialistas	Servidores DNS	Servidores DNS
	Encaminhamento de rotas	Encaminhamento de rotas

Samsung / Strong Swan			
Tipo de ligação	PPTP	Servidor	Servidor
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar a encriptação PPTP	Ativar a encriptação PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar o segredo L2TP	Segredo L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
Definições de especialistas	Servidores DNS	Servidores DNS	
	Encaminhamento de rotas	Encaminhamento de rotas	

Cisco Any Connect		
Servidor	Servidor	
Modo de certificado	Desativado	Desativado
	Automático	Automático
Definições de especialistas	Servidores DNS	Servidores DNS
	Encaminhamento de rotas	Encaminhamento de rotas

VPN por aplicação

Cliente VPN

Cliente VPN AppTec360		
Configuração da porta de entrada	Selecciona a Configuração VPN da Gateway (Ver **Definições Gerais > Gateway Universal > Definições VPN**)	
Aplicações VPN	Aplicações VPN	
VPN sempre ativa	Ativar o bloqueio nativo	VPN sempre ativa
Ativar o bloqueio do AppTec360	Ativar o bloqueio do AppTec360	

Samsung / Strong Swan			
Tipo de ligação	PPTP	Servidor	Servidor
		Aplicações VPN	Aplicações VPN
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar a encriptação PPTP	Ativar a encriptação PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Aplicações VPN	Aplicações VPN
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar o segredo L2TP	Segredo L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Aplicações VPN	Aplicações VPN
		Identificador IPSec	Identificador IPSec
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
Definições de especialistas	Servidores DNS	Servidores DNS	
	Encaminhamento de rotas	Encaminhamento de rotas	

Restrições

Aqui podes definir as restrições, em relação à gestão da ligação.

Permitir roaming de dados	Permitir dados móveis em roaming
Forçar Roaming de Dados	Se estiver ativado, o roaming para dados móveis é permanentemente ativado (não recomendado!) Esta definição substitui a definição "Permitir Roaming de Dados"!
As seguintes definições só estão disponíveis no SAFE 2.x ou superior	
Permitir apenas chamadas de emergência	Permitir apenas chamadas de emergência
Permitir WiFi	Permitir WiFi
Nível mínimo de segurança da rede WiFi	Nível mínimo de segurança da rede WiFi Aberto = todos os tipos de WiFi são permitidos
Proibir o utilizador de adicionar redes WiFi	O utilizador não pode adicionar ele próprio uma rede WiFi Esta definição só é possível se tiveres definido um perfil WiFi em "Gestão de ligações"
Permite SMS e MMS	Todos = Todo o tráfego SMS e MMS é permitido Apenas SMS de entrada = Apenas são permitidas mensagens SMS de entrada Apenas SMS de saída = Apenas são permitidas mensagens SMS de saída Nenhum = Não é permitido qualquer tráfego SMS / MMS
Permitir sincronização durante o roaming	Permitir sincronização durante o roaming Ligado = ativado Desligado = desativado Escolha do utilizador = escolha do utilizador
Permitir roaming de voz	Permitir roaming de voz Ligado = ativado Desligado = desativado Escolha do utilizador = escolha do utilizador
Utiliza o servidor proxy http do sistema	A utilização de um servidor proxy HTTP, que é fornecido pelas definições do sistema nas definições, depende da rede ligada (WiFi ou APN)

Gestão PIM

Gmail Exchange

Informação: Esta Configuração será aplicada à aplicação Gmail. Por isso, tens de aprovar e instalar o Gmail.

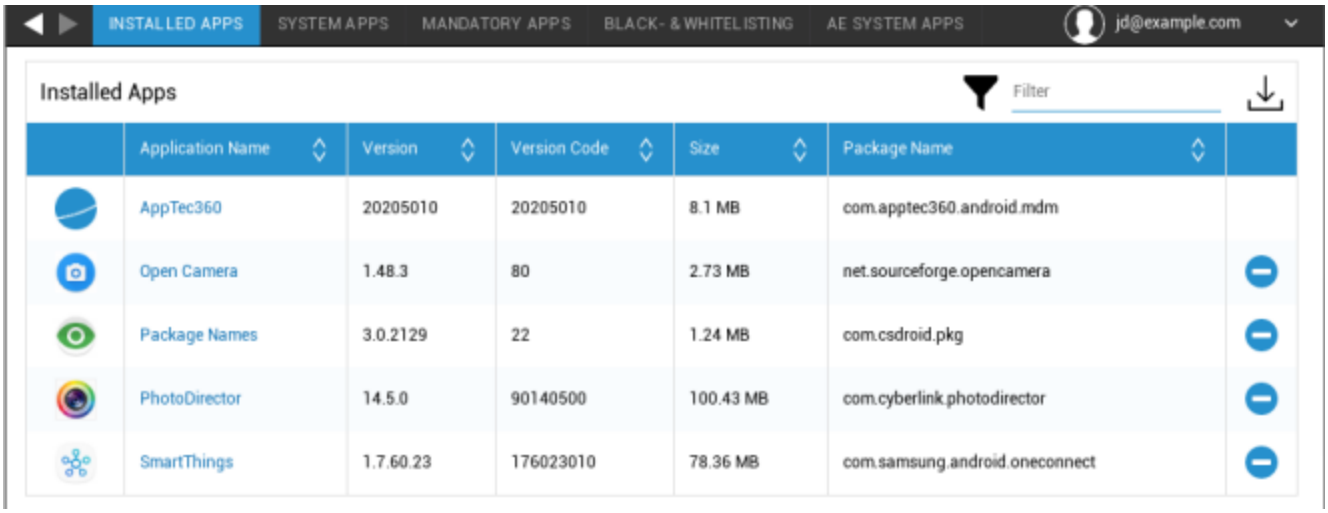
Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique, podes ver por ti próprio
Nome de anfitrião do servidor	Endereço do servidor dos teus Servidores Exchange
Nome de utilizador	O nome de utilizador (Login-Name) do respetivo dispositivo do utilizador final, tem também em atenção os "Placeholders here
Assinatura	Podes anexar uma assinatura (Dica: alguns dispositivos exigem formatação HTML para a assinatura)
Número de dias anteriores a sincronizar	Número de dias, determinando quando os e-mails são sincronizados de volta
Identificador do dispositivo	Uma cadeia de caracteres que contém o ID do dispositivo EAS. Faz parte do protocolo EAS e está disponível em algumas regiões
Utiliza Secure Sockets Layer (SSL)	Utiliza uma ligação SSL
Aceita todos os certificados	Todos os certificados são aceites. Selecciona esta opção, se o teu Exchange Server utilizar um certificado auto-assinado

Gestão de aplicações

Gestor de aplicações empresariais

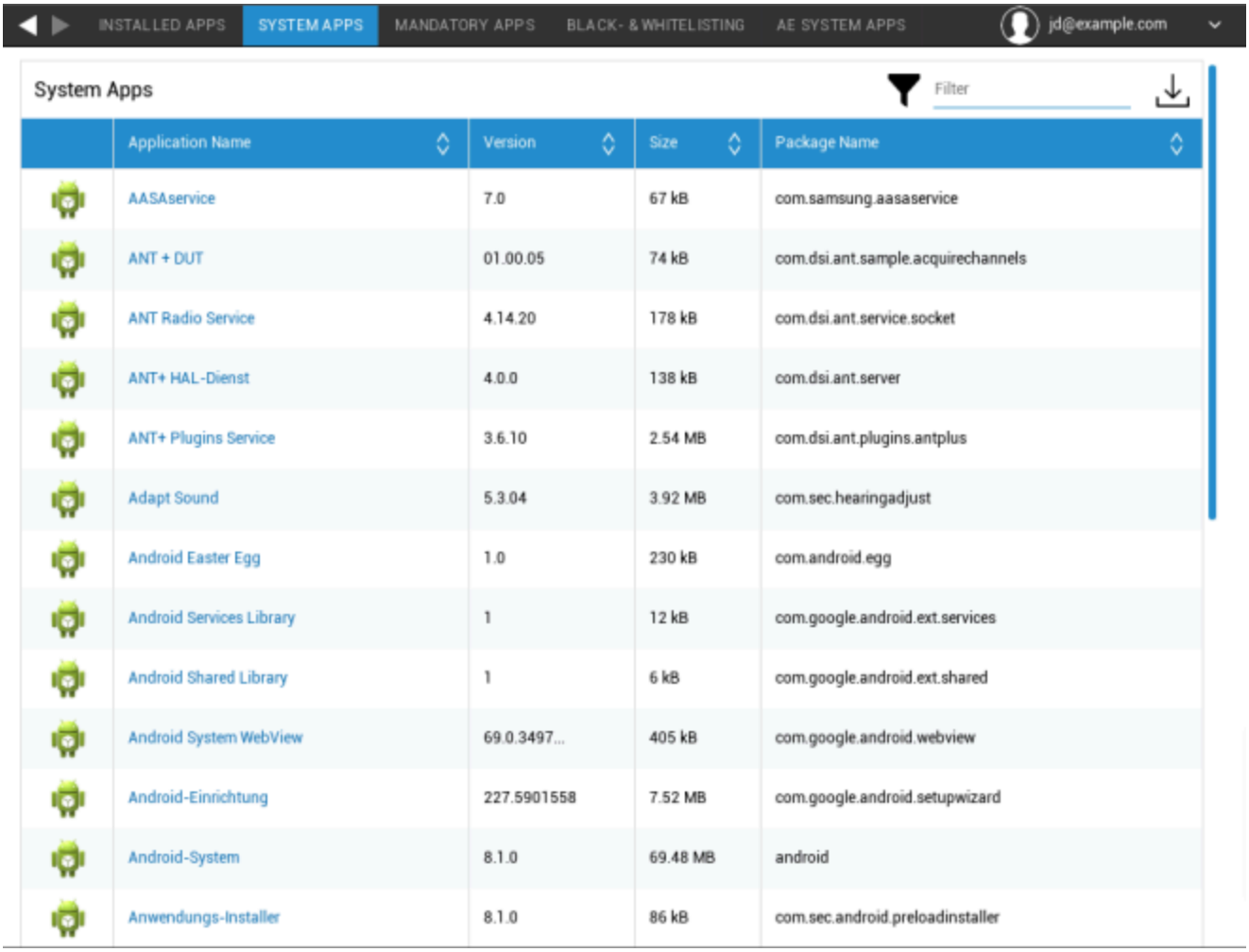
Aplicações instaladas (apenas ao nível do dispositivo)

Aqui ser-te-ão apresentadas todas as aplicações que estão atualmente instaladas no dispositivo do utilizador final.



Aplicações de sistema (apenas ao nível do dispositivo)

Em "System Apps" (Aplicações do sistema), todas as aplicações e serviços que já foram instalados no dispositivo do utilizador final pelo fabricante do dispositivo serão listados para ti.

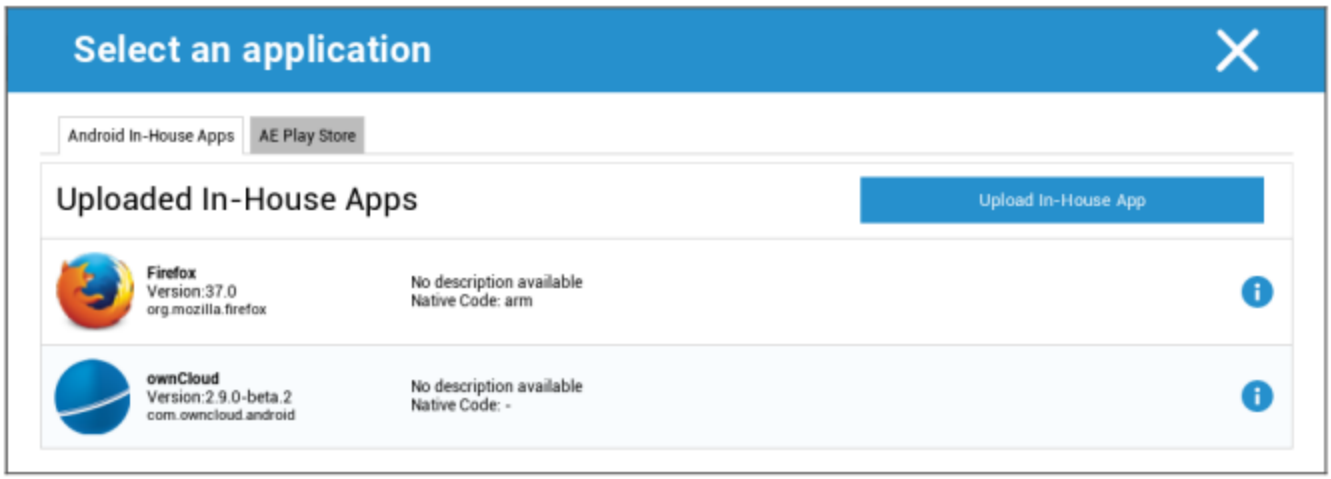


Aplicações obrigatórias

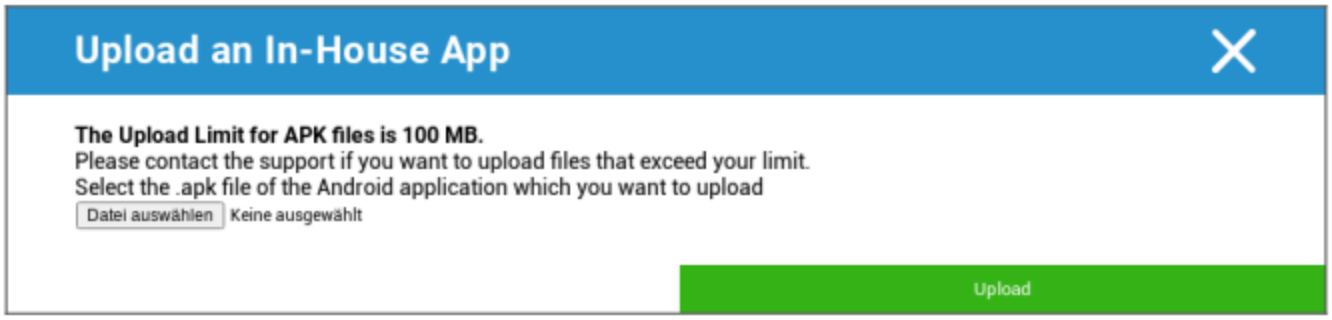
Em Aplicações obrigatórias, podes definir as aplicações obrigatórias. O utilizador será continuamente solicitado a instalar esta aplicação designada.

Através do , podes definir a aplicação obrigatória requerida.

Pode ser uma aplicação interna da lista "Aplicações internas do Android", que carregaste nas Definições gerais.

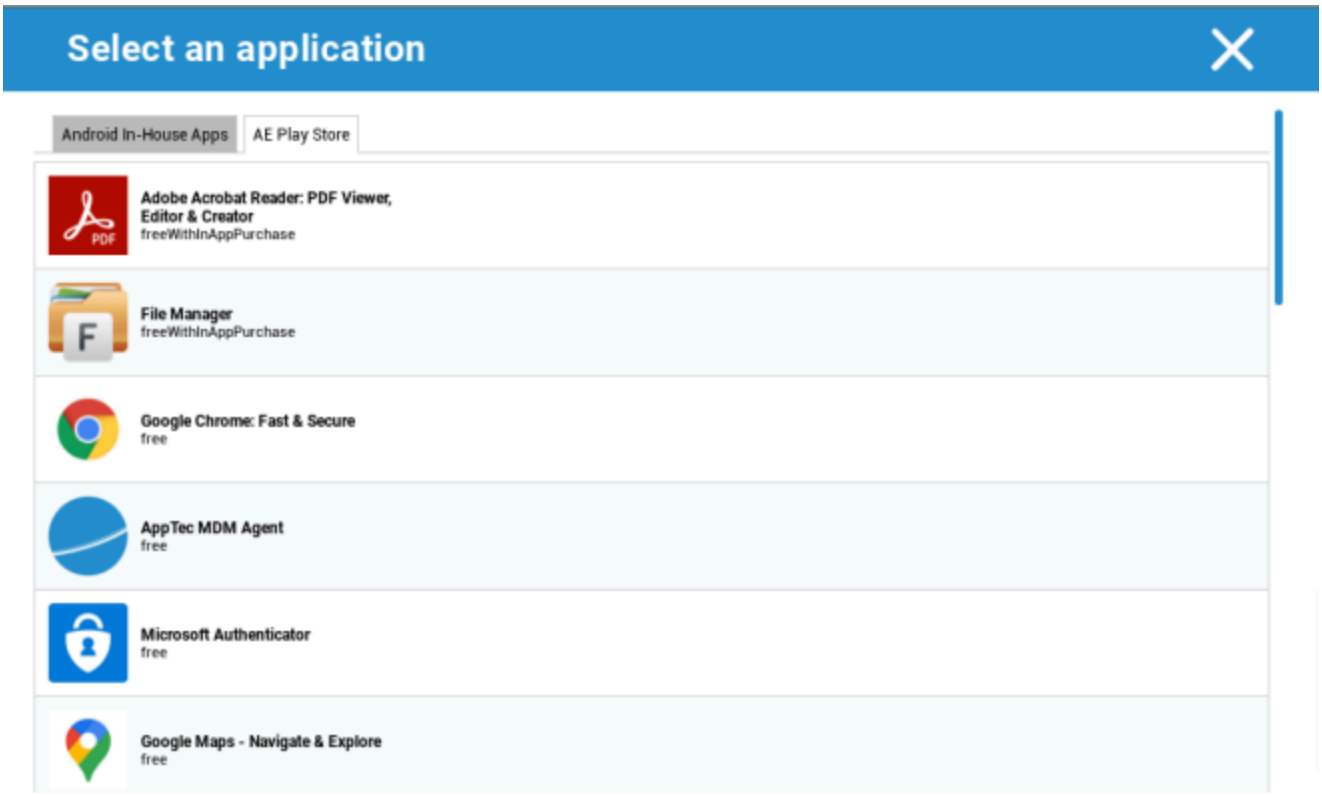


Também podes selecionar e carregar diretamente um ficheiro apk com "Carregar aplicação interna".



Se estiveres a instalar uma aplicação interna, terás a possibilidade de ativar "Manter atualizado". Se esta opção estiver activada e tiveres definido uma versão mais recente na BD de aplicações internas, a aplicação será actualizada no dispositivo.

Ou pode ser uma aplicação "AE Play Store" da Google Work Play Store.



Apenas as "Aplicações da AE Play Store" aprovadas serão mostradas neste separador.

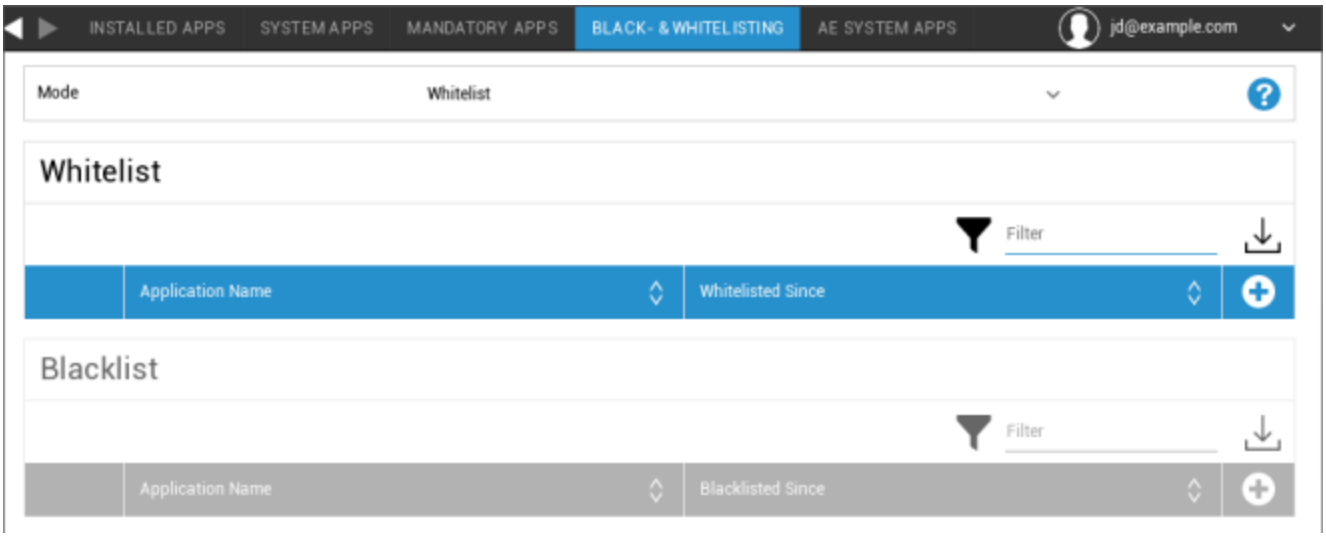
Para aprovar uma "Aplicação da AE Play Store", vai a "Definições gerais" > "Gestão de aplicações" > "AE Play

Store" e adiciona uma aplicação através do botão que te redirecciona para o separador "Play Store Apps" (ou
pode ir diretamente para o separador "Aplicações da Play Store").

No separador "Aplicações da Play Store", podes procurar aplicações. Quando clicas numa aplicação, abre-se a página da aplicação
e aqui podes aprovar a aplicação clicando em "Aprovar".

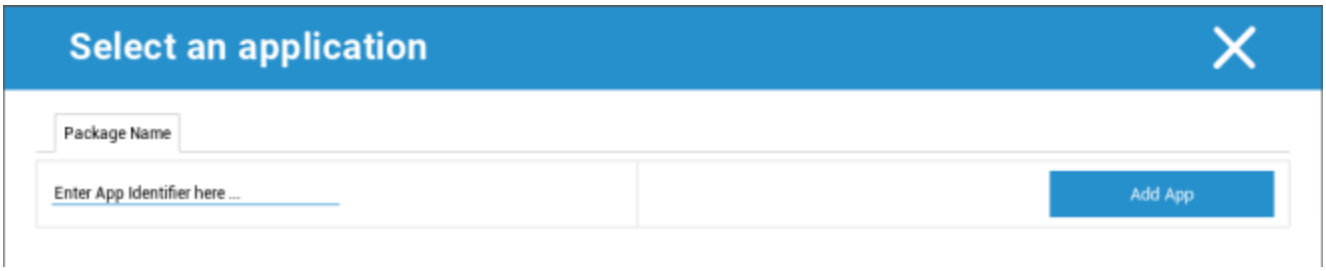
Lista negra e lista branca

Em "Black- & Whitelisting", podes escolher entre o modo "Whitelist" e o modo "Blacklist".



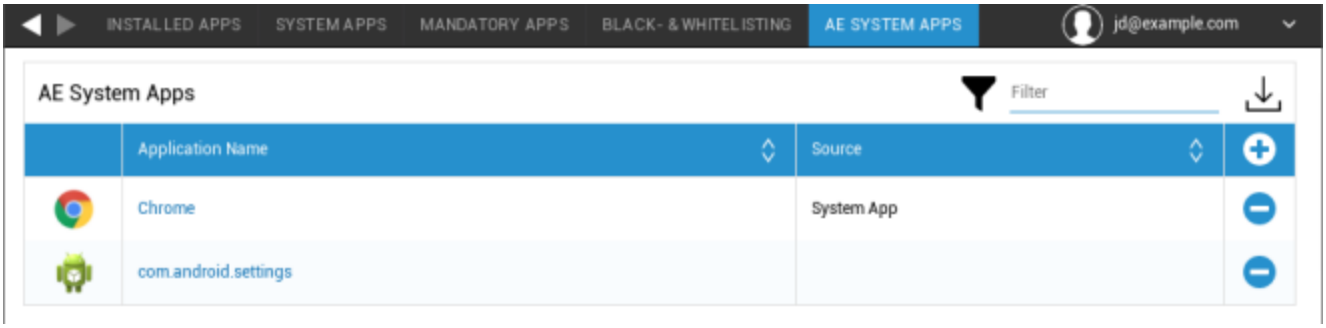
Lista branca	Apenas as aplicações e os serviços adicionados à lista podem ser instalados no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão activados e definidos, para que o utilizador os possa executar.
	Todas as outras aplicações que não sejam adicionadas à lista não podem ser instaladas no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão desactivados e definidos, para que o utilizador não os possa executar.
Lista negra	As aplicações e os serviços que são adicionados à lista não podem ser instalados no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão desactivados e definidos, para que o utilizador não os possa executar.
	Todas as outras aplicações que não são adicionadas à lista podem ser instaladas no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão activados e definidos, para que o utilizador os possa executar.

Através da tecla , adiciona mais aplicações ou serviços à lista atualmente utilizada.
Através do botão , adiciona mais aplicações ou serviços à lista atualmente inativa.
Podes definir um "Packagename":

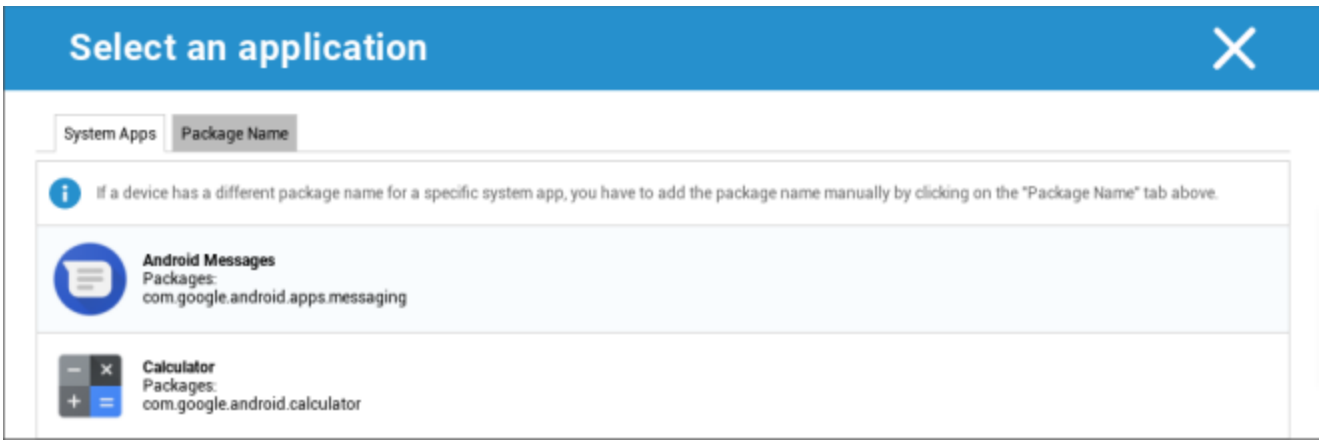

Select an application
Package Name
Enter App Identifier here ...
Add App

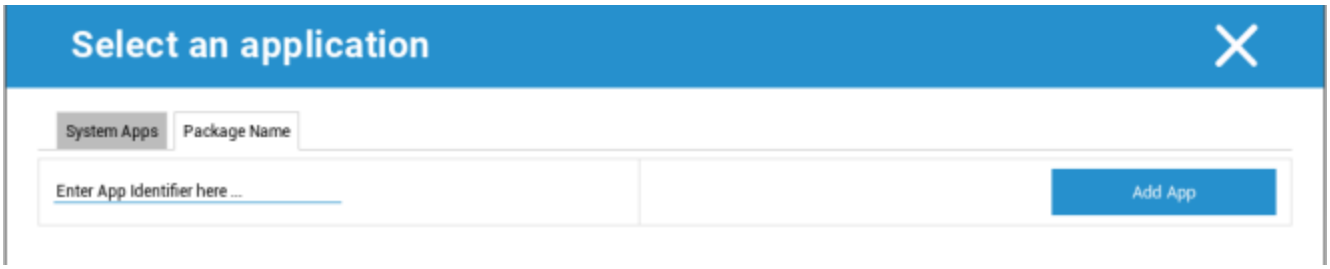
Aplicações do sistema AE

Aqui podes definir uma lista que contém aplicações de sistema específicas que devem ser activadas nos dispositivos.



Se clicares no botão, podes escolher a partir de uma lista de possíveis aplicações de sistema fornecidas pelo Google ou introduzir diretamente o nome do pacote de uma aplicação de sistema que deve ser activada.





Tem em atenção que as aplicações de sistema na lista fornecida pela Google são apenas aplicações que podem ser aplicações de sistema, mas não têm necessariamente de ser aplicações de sistema nos teus dispositivos.

No entanto, esta lista só afecta as aplicações que já estão pré-instaladas.

A adição de aplicações que não estejam pré-instaladas nos teus dispositivos não afectará os teus dispositivos, independentemente de a aplicação pertencer à lista fornecida pelo Google ou de o nome do pacote da aplicação ser introduzido diretamente.

Restrições e definições

Definições de gestão de aplicações

Aqui podes configurar o comportamento do dispositivo relativamente às actualizações de aplicações.

Atualizar a frequência de verificação	Especifica em que intervalo o Cliente AppTec360 irá procurar actualizações de aplicações. O valor predefinido é 24 horas.
Limiar Wi-Fi	As aplicações maiores do que o tamanho especificado serão descarregadas através de Wi-Fi. Se selecionar "Apenas Wi-Fi", todas as aplicações serão descarregadas através de Wi-Fi.

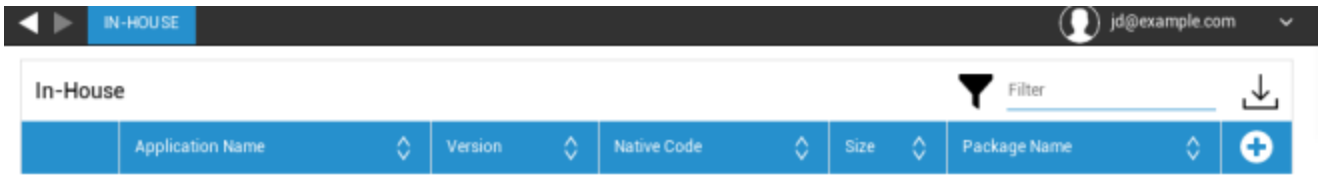
Loja de aplicações para empresas

Internamente

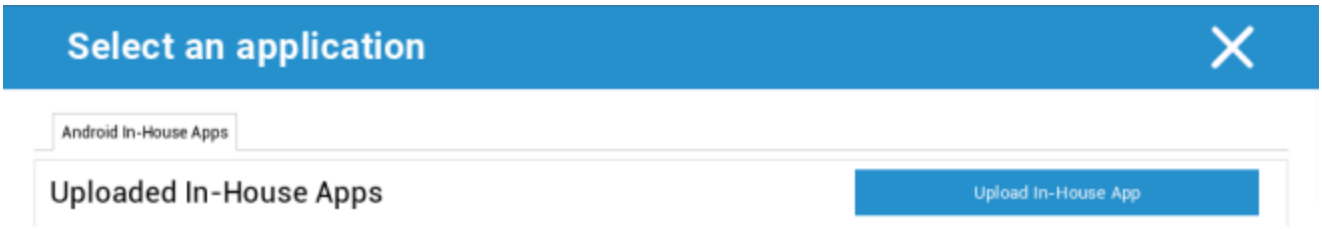
No ponto "In-House", podes carregar e distribuir aplicações desenvolvidas internamente.

Com o símbolo, podes distribuir mais aplicações internas.

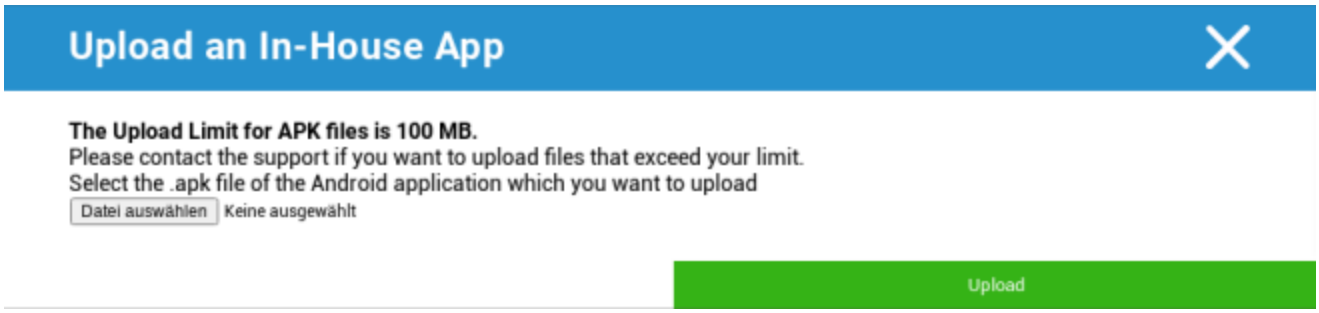
Se estiveres a instalar uma aplicação interna, terás a possibilidade de ativar "Manter atualizado". Se esta estiver activada e tiveres definido uma versão mais recente na BD de aplicações internas, a aplicação será
atualizado no dispositivo.



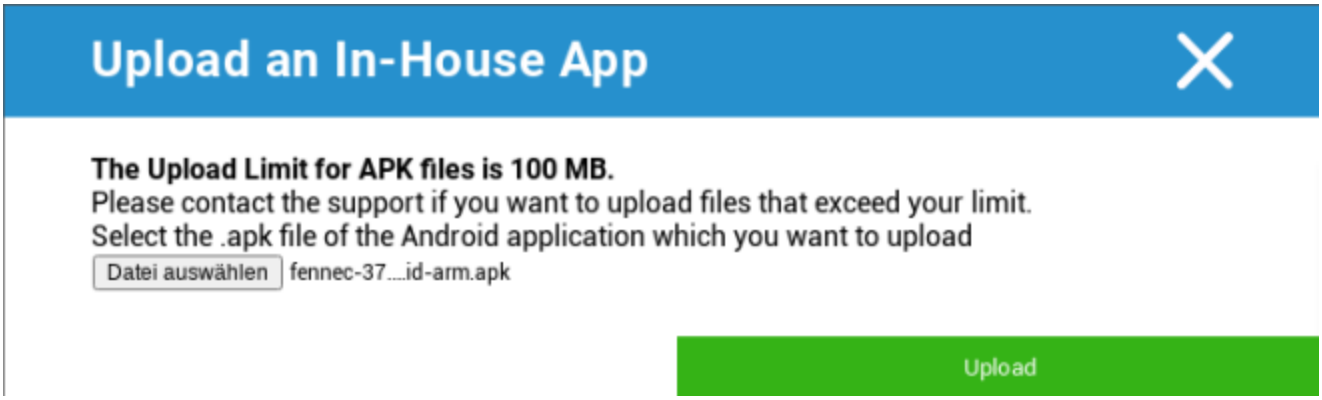
Se não tiveres distribuído aplicações internas, receberás a seguinte visão geral:



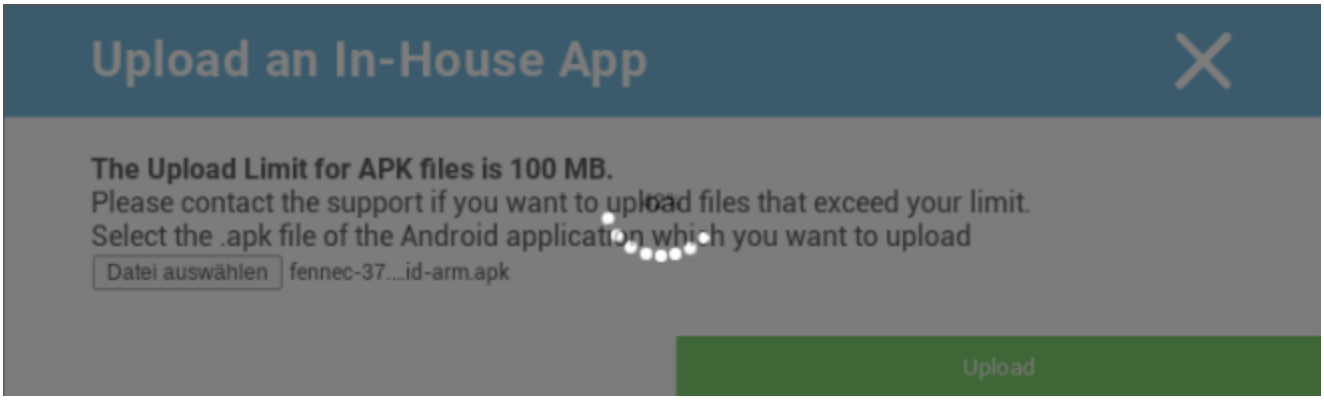
Para isso, clica em "Upload In-House App", e receberás a seguinte visão geral:



Agora, escolhe com "Procurar..." um ficheiro .apk e depois clica em "Carregar".



A tua aplicação será agora carregada e, no meio do círculo, verás um indicador de percentagem, mostrando quanto da tua aplicação já foi carregado.



Se o carregamento da tua aplicação interna tiver sido bem sucedido, podes encontrar a aplicação carregada
no teu catálogo de aplicações.

O utilizador tem agora a opção de ver e instalar esta aplicação na AppTec360 Store no utilizador final na categoria "In-House".

Devido ao facto de não se tratar de uma aplicação da Google PlayStore, o utilizador não necessita de ter uma conta Google
ID no respetivo dispositivo do utilizador final.

Empresa Play Store

AE Play Store

Aqui podes adicionar aplicações à Android Enterprise Playstore. Tem em atenção que tens de aprovar Apps com a tua Conta de Administrador AE antes de as poderes adicionar.

Para aprovares uma aplicação, consulta as instruções em Aplicações obrigatórias.

Modo de quiosque e lançador

Modo quiosque

O Modo Quiosque permite-te predefinir uma aplicação ou um URL. Então, só poderás executa/visita esta aplicação e ou URL.

Da mesma forma, vários botões de hardware podem ser desactivados no Modo Quiosque.

Início automático	Inicia automaticamente o Modo Quiosque, assim que o perfil chega ao dispositivo do utilizador final
Modo de quiosque programado?	Podes planear um horário para o Modo Quiosque, que começará e terminará automaticamente, a uma hora definida por ti
Hora de início	Hora de início
Tempo em minutos	Tempo em minutos, após o qual o Modo Quiosque deve terminar novamente

Tipo de aplicação

Aplicação única	Se quiseres iniciar a aplicação no modo Quiosque, selecciona Pacote" em "Tipo de aplicação"
Aplicação de quiosque	Clica aqui para selecionar uma aplicação que deve ser iniciada no modo de quiosque Encontrarás a visão geral habitual da Gestão de aplicações Podes selecionar entre "Google Play Store", "Android In-House Apps" e "Packagename"

Tipo de aplicação	

URL		Se quiseres lançar um URL no modo de quiosque, selecciona "URL" em "Tipo de aplicação" Em seguida, define o endereço URL pretendido
	Limpa o browser após inatividade	Aqui podes definir um intervalo de tempo em minutos, após o qual o Modo Quiosque deve ser relançado
	Limpar a cache da Web e os cookies	Se activares esta função, depois de reiniciar o Modo Quiosque, a Cache Web (cookies e imagens em cache) será apagada
	Política de mesma origem	Se esta função estiver ativa, o utilizador só pode navegar nas subpáginas de um URL definido Por exemplo, definiste o seguinte URL:www.mypage.com Depois, o utilizador pode navegar em: www.mypage.com/subpage
	URLs na lista branca	Aqui podes manter uma Whitelist, todos estes URLs são permitidos Máximo de 1 URL por linha Um URL deve começar por http:/ ou https://
	URLs na lista negra	Aqui podes manter uma lista negra, todos estes URLs não são permitidos Máximo de 1 URL por linha Um URL deve começar por http:/ ou https://
	Orientação do ecrã	Esta definição está relacionada com os ajustes do ecrã Automático = automático Retrato = formato vertical Paisagem = modo paisagem

Multi App		Se seleccionares o modo de quiosque "Multi App", a utilização do AppTec360 Launcher será obrigatória.
	Aplicações	Aplicação: Selecciona uma aplicação da Playstore ou uma aplicação interna como aplicação do quiosque. Também é possível introduzir um nome de pacote. A aplicação de quiosque selecionada tem de estar instalada no dispositivo. Não te esqueças de definir a aplicação Kiosk como obrigatória. Atalho no ecrã inicial: Se estiver definido para "Ligado", será criado um atalho no ecrã inicial. Se estiveres definido como "Desligado", a aplicação continua a aparecer na lista de aplicações.

Senha de saída activada	Se activares esta função, o utilizador pode terminar o modo de quiosque com uma palavra-passe predefinida por ti
Sair da palavra-passe	Esta é a palavra-passe, que foi predefinida por ti
Recolha automática da barra de estado	Se estiver ativado, a barra de estado será automaticamente colada. Com esta opção, os utilizadores podem ver as informações na barra de estado, mas não podem aceder às suas funções
Desativar a barra de estado	A barra de estado contém notificações, atalhos e informações. Apenas disponível para dispositivos Samsung com SAFE 4.0 ou superior.
Desativar as teclas de volume	Desativar as teclas de volume (apenas disponível em dispositivos Samsung com SAFE 3.0 ou superior)
Desativar o interrutor de ligar/desligar	Desativar o interrutor Ligar/Desligar (apenas disponível em dispositivos Samsung com SAFE 3.0 ou superior)
Desativar o botão Home	Desativar o botão Início. Se esta função estiver activada, então o Modo Quiosque só pode ser terminado na Consola AppTec360 (apenas disponível em dispositivos Samsung com SAFE 3.0 ou superior)
Desativar a barra de navegação	Com esta opção, podes desativar a barra de navegação (Voltar / Menu) Se esta função estiver activada, então o Modo Quiosque só pode ser terminado na Consola AppTec360 (apenas disponível em dispositivos Samsung com SAFE 3.0 ou superior)

Lançador AppTec360

Ativar o AppTec360 Launcher	Liga: Ativa o AppTec360 Launcher. O utilizador tem de o definir como Launcher predefinido uma vez. Nota: Se o Modo Quiosque estiver ativado e o Modo Quiosque estiver definido para "Multi-Apps", a utilização do lançador AppTec360 será obrigatória.
Ícones grandes	Liga: Mostra uma versão maior dos ícones de aplicações no Launcher
Ocultar o ícone da AppTec360	Liga: Oculta completamente a aplicação AppTec360
Ocultar o ícone da AppTec360 Store	Ativa: Oculta completamente a AppTec360 Enterprise AppStore

Definições da AppTec360

Ativar a aplicação AppTec360 Settings	A aplicação de definições AppTec360 permite controlar as ligações WiFi e Bluetooth
Ativar as definições em Multi-Apps Modo quiosque	Se estiver ativado, os utilizadores podem aceder à AppTec360 Settings App enquanto o Multi App Kiosk Mode estiver ativo

Controlo remoto

Splashtop

Para iniciares uma sessão de controlo remoto para o teu dispositivo, a aplicação "Splashtop Streamer" tem de ser instalada no dispositivo, adicionando-a a App **Management → Enterprise App Manager → Mandatory Apps**.

Em seguida, configura as seguintes definições para o Splashtop:

Ativar o Splashtop	Se estiver ativado, o AppTec360 configurará a aplicação Splashtop para permitir o controlo remoto
Implementar código	Vai a https://my.splashtop.com e entra na tua conta Splashtop. Clica em "Adicionar computador" e copia o código de implantação de 12 dígitos da página resultante.
Definir Gateway de implantação personalizado?	Implementa a Gateway
Implantar domínio / host do gateway	Implementa a Gateway
Verificação de certificados	Verificação de certificados

Em seguida, podes utilizar a opção Controlo Remoto Splashtop no menu de contexto (engrenagem junto à barra de pesquisa, quando o dispositivo é selecionado ou clicar com o botão direito do rato no dispositivo na árvore) para iniciar a sessão de controlo remoto.

TeamViewer

Para iniciar uma sessão de controlo remoto para o teu dispositivo, a aplicação "TeamViewer QuickSupport" tem de ser instalada no dispositivo, adicionando a aplicação à **Gestão de aplicações → Gestor de aplicações empresariais → Aplicações obrigatórias**.

Em seguida, podes utilizar a opção **Controlo remoto do TeamViewer** no menu de contexto (engrenagem junto à barra de pesquisa, quando o dispositivo é selecionado ou clicar com o botão direito do rato no dispositivo na árvore) para iniciar a sessão de controlo remoto.

Gestão de conteúdos

ContentBox

Aqui podes ativar a ContentBox.

Assim que mudares a opção "Enable ContentBox" para "On", será instalada uma aplicação ContentBox separada
automaticamente no dispositivo do utilizador final.

Navegador seguro

Aqui podes configurar as definições para o AppTec360 Secure Browser.

Assim que mudares a secção "Navegador seguro" para "Ligado", será criada uma aplicação de navegador separada.
instalado automaticamente no dispositivo do utilizador final.

Requerer palavra-passe	Exige que o utilizador defina e utilize uma palavra-passe para aceder ao browser.
Comprimento mínimo exigido para a palavra-passe	Define o número necessário de caracteres para a palavra-passe
Qualidade da palavra-passe necessária	Define a qualidade da palavra-passe necessária
Restringir transferências / Abrir em	
Restringir carregamentos	
Carregar lista branca	Uma lista de URLs para os quais o carregamento será sempre permitido.
Permitir cópia	Permite copiar, cortar ou partilhar texto dentro das páginas Web.
Permite a captura de ecrã	Permite a captura de imagens de ecrã.
Frequência da limpeza de dados	Selecciona com que frequência TODOS os dados do utilizador (histórico, cache, etc.) devem ser automaticamente removidos.
Marcadores da empresa	Os marcadores aparecerão na pasta "Marcadores da empresa" nos marcadores do navegador. Não são editáveis pelo utilizador.
Ocultar a barra de endereços	
Lista branca no navegador (sem Universal Gateway)	Ativa a lista branca de URLs do lado do cliente. • Os marcadores da empresa são sempre colocados na lista branca • Suportado apenas para 100 URLs • Utiliza o Universal Gateway para a criação ilimitada de listas negras e brancas

URLs na lista branca	Uma lista de URLs permitidos.
Lista negra e lista branca baseadas em gateway	A inclusão na lista negra tem os seguintes requisitos: • Um AppTec360 Universal Gateway a funcionar ("Definições gerais" → "Universal Gateway") • Uma configuração VPN em funcionamento com um servidor DNS especificado ("Definições gerais" → "Gateway universal" → "Definições VPN") • Configuração de uma lista negra ("Definições gerais" → "Universal Gateway" → "Lista negra de domínios") • Uma ligação VPN válida no perfil ("Gestão de ligações" → "VPN")

API adicional

Samsung KNOX

Restrições

Permitir cartão SD	
Permite a escrita no cartão SD	
Permite a captura de ecrã	
Permite a área de transferência	
Faz a cópia de segurança das definições e dos dados da aplicação no Google Cloud	
Restaurar definições do Google Cloud ao reinstalar uma aplicação	
Permite a depuração USB	
Permite o relatório de falhas do Google	
Permite a reposição de fábrica	
Permite a atualização OTA	
Permite o armazenamento no anfitrião USB	Se estiver ativado, o utilizador pode ligar qualquer pen drive (armazenamento USB portátil), HD externo ou leitor de cartões Secure Digital (SD), que é montado como uma unidade de armazenamento no dispositivo.
Permite o leitor multimédia USB (MTP, PTP)	
Permite o microfone	Desativa o microfone para aplicações de terceiros
Permite NFC (Near Field Communication)	
Permitir fontes desconhecidas (APK Sideloading)	Se estiver ativado, permite o carregamento lateral de aplicações (ficheiros APK). Se esta definição estiver desactivada, o utilizador tem de a ativar manualmente quando permitires a instalação de APKs de fontes desconhecidas.

Permitir a criação de utilizadores	Se estiver ativado, o utilizador pode criar várias contas no dispositivo, por exemplo, contas de convidado

Correio eletrónico

Endereço de correio eletrónico	
Protocolo do servidor de entrada	
Endereço do servidor de entrada	
Porta do servidor de entrada	
Nome de utilizador/login do servidor de entrada	
Palavra-passe do servidor de entrada	
O servidor de entrada utiliza SSL	
O servidor de entrada utiliza TLS	
O servidor de entrada aceita todos os certificados	
Protocolo do servidor de saída	
Endereço do servidor de saída	
Porta do servidor de saída	
O servidor de saída utiliza credenciais adicionais	Se estiver desactivada, o sistema utiliza as credenciais de entrada também para o servidor de saída.
Nome de utilizador/login do servidor de saída	
Palavra-passe do servidor de saída	
O servidor de saída utiliza SSL	
O servidor de saída utiliza TLS	
O servidor de saída aceita todos os certificados	
Definir assinatura	
Assinatura	Nota: Para alguns dispositivos, a assinatura tem de ser especificada em formato HTML.
Notifica o utilizador quando recebe um novo e-mail	

Troca

Endereço de correio eletrónico	
Nome de anfitrião do servidor	O nome do anfitrião do Exchange Server
Nome de utilizador	O nome de utilizador que é utilizado para iniciar sessão no Exchange Server
Domínio	Se uma ACL Gateway Configuration estiver activada e o campo Domain não estiver vazio, o AppTec360 Universal Gateway autenticará o dispositivo com o seguinte nome "Domain\Login Name
Palavra-passe	
Número de dias anteriores a sincronizar	
Frequência de sincronização do eMail	
Sincronizar em roaming	
Definir assinatura	
Assinatura	Nota: Para alguns dispositivos, a assinatura tem de ser especificada em formato HTML.
Conta por defeito	
Utiliza Secure Sockets Layer (SSL)	
Utiliza a segurança da camada de transporte (TLS)	
Aceita todos os certificados	

APN

Nome de exibição do APN	
Nome do ponto de acesso	Nome da APN
Protocolo do servidor de saída	
MCC - Código de país móvel	Deixa em branco para utilizar o mmc do SIM instalado
MNC - Código de Rede Móvel	Deixa em branco para utilizar o mnc do SIM instalado
Endereço do servidor	
Número da porta do servidor	
Endereço do servidor proxy	
Endereço do servidor MMS	Deixa em branco por defeito
Número da porta MMS	Deixa em branco por defeito
Endereço proxy MMS	Deixa em branco por defeito
Nome de utilizador	
Palavra-passe	
Tipo de ponto de acesso	Os tipos aceites são "default", "mms", "supl".
	Se for passado null ou vazio, por defeito é utilizado "default,supl,mms".
	Deixa em branco por defeito.
APN preferida	

Bluetooth

Permite a descoberta de dispositivos via Bluetooth	
Permitir o emparelhamento Bluetooth	
Permitir dispositivos com auscultadores Bluetooth	
Permite dispositivos mãos-livres Bluetooth	
Permite dispositivos Bluetooth A2DP	A2DP, perfil de distribuição de áudio avançado, permite a transmissão de áudio entre dispositivos
Permitir chamadas efectuadas	
Permite a transferência de dados via Bluetooth	
Permite o Bluetooth Tethering	
Permite a ligação ao computador através de Bluetooth	

Ligação

Permitir apenas chamadas de emergênciaPermitir Wi-Fi	
Nível mínimo de segurança da rede Wi-Fi	
Proíbe o utilizador de adicionar redes Wi-Fi	Esta restrição só pode ser activada se pelo menos um perfil Wi-Fi ativo estiver definido em Gestão de ligações
Permite SMS e MMS	
Permitir sincronização durante o roaming	
Permitir roaming de voz	

Android Enterprise – Dispositivo totalmente gerido com perfil de trabalho (COPE)

Explicação geral do COPE

COPE é uma abreviatura de **Corporate Owned Personally Enabled**.

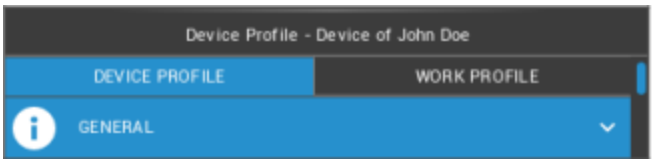
O modo COPE permite que um dispositivo Android seja registado como um **dispositivo Android Enterprise - Fully Managed Device** com perfil **Android Enterprise - Container** integrado.

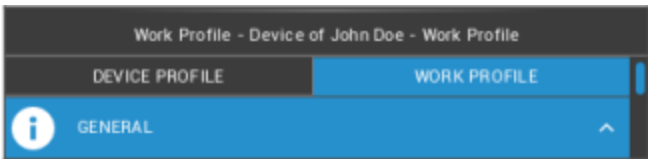
Este pode ser um dispositivo Android que já está registado como um **Android Enterprise - Dispositivo totalmente gerido** e na qual o **Android Enterprise - Contentor** é configurado adicionalmente, ou um dispositivo Android recém-inscrito que é diretamente inscrito como um **Android Enterprise - Dispositivo totalmente gerido** juntamente com o **Android Enterprise - Contentor** em cima dela.

O modo COPE está disponível apenas para dispositivos com Android 8, 9 e 10

Configuração de perfis para dispositivos COPE

Uma vez que não existe um perfil de configuração para o modo COPE propriamente dito, a configuração do **Android Enterprise - Dispositivo totalmente gerido** e do **Android Enterprise - Contentor** é separada em dois perfis dentro do perfil COPE. É possível alternar entre os dois perfis para a configuração de cada perfil, clicando no respetivo botão no lado esquerdo da consola:





Ambos os perfis podem ser configurados conforme descrito para cada perfil individual:

Android Enterprise - Dispositivo totalmente gerido

Android Enterprise - Contentor

Reverter para um dispositivo totalmente gerido pela AE

O perfil **Android Enterprise - Container** pode ser removido conforme descrito em **Gestão de dispositivos móveis**.

Ao remover o perfil Container, o perfil COPE será transformado num perfil **Android Enterprise - Fully Managed Device**.

Android Enterprise – Configuração de contentores

Dependendo de teres selecionado um perfil de grupo ou um dispositivo, a síntese e os seus subpontos são diferentes - tem isto em atenção!

Geral

Síntese do perfil (apenas ao nível do perfil)

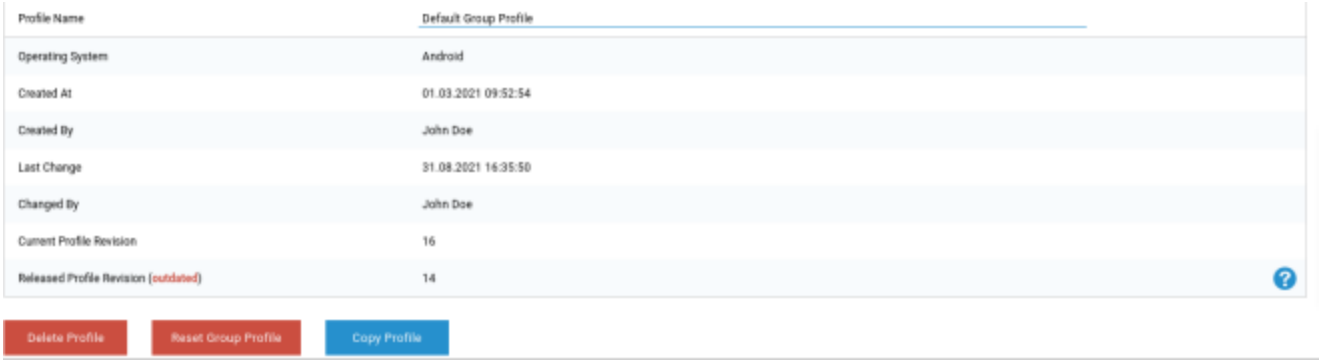
Se estiveres num perfil, receberás uma breve descrição do perfil, no que diz respeito ao nome, SO, data de criação, autor, etc.

Nome do perfil	Nome do perfil - pode ser diretamente renomeado aqui
Sistema operativo	SO válido para o perfil
Criado em	Data de criação
Criado por	Criado por
Última alteração	Data da última alteração
Alterado por	O utilizador que efectuou as últimas alterações a este perfil
Revisão do perfil atual	Número de vezes que o perfil já foi atualizado
Revisão do perfil lançado	Número de vezes que o perfil já foi atualizado e lhe foram atribuídos dispositivos

Eliminar perfil	Eliminar perfil
Repor o perfil do grupo	Repor o perfil do grupo
Copia o perfil	Copia o perfil

Síntese do perfil do grupo (apenas a nível do grupo)

Ao abrires um perfil de grupo, terás uma visão geral rápida do perfil.



Nome do perfil	Nome do perfil (pode ser alterado aqui)
Sistema operativo	Sistema operativo para o qual o perfil se destina
Criado em	Tempo de criação
Criado por	O criador do perfil
Última alteração	Hora da última modificação do perfil
Alterado por	Conta que efectuou as últimas alterações
Revisão do perfil atual	Revisão do estado do perfil guardado
Revisão do perfil lançado	Revisão do perfil atribuído ("Atribuir agora"). Se a etiqueta apresentar " (desatualizado)" por trás do texto, significa que guardaste o perfil mas ainda não o atribuíste, pelo que os dispositivos continuarão a receber uma versão mais antiga.

Síntese do dispositivo (apenas ao nível do dispositivo)

Se estiveres num dispositivo, receberás uma recapitulação geral do dispositivo selecionado, que contém o seguinte:

Nome do dispositivo	Nome do dispositivo
Localização	Coordenadas de localização
Número de telefone	Número de telefone
Atribuição de aplicações obrigatórias	Número de aplicações obrigatórias atribuídas
Versão do SO	Versão do sistema operativo do dispositivo
Sistema operativo	Sistema operativo (Android Enterprise)
Número de série	Número de série do dispositivo
Propriedade do dispositivo	Dispositivo empresarial ou privado
Tipo de dispositivo	Dispositivo gerido pelo AE Work
Enraizado	Estado, indicando se o dispositivo foi enraizado
Conformidade	Em conformidade com as directrizes
Endereço IP	Endereço IP do dispositivo
Visto pela última vez	Ponto no tempo, quando o dispositivo se ligou pela última vez à AppTec
Último empurrão	Ponto no tempo, quando o último push foi enviado para o dispositivo
Atribuição de utilizadores	O utilizador ou grupo a que este dispositivo está atribuído

Revisão da configuração

Aqui tens uma visão geral do perfil de grupo que está atribuído ao aparelho.

Se clicares no perfil de grupo, terás acesso direto a esse perfil e poderás efetuar definições.

Com este símbolo, podes reverter as aplicações distribuídas para as definições do perfil de grupo.

Com este símbolo, podes reverter todas as aplicações utilizadas para as definições do perfil de grupo.

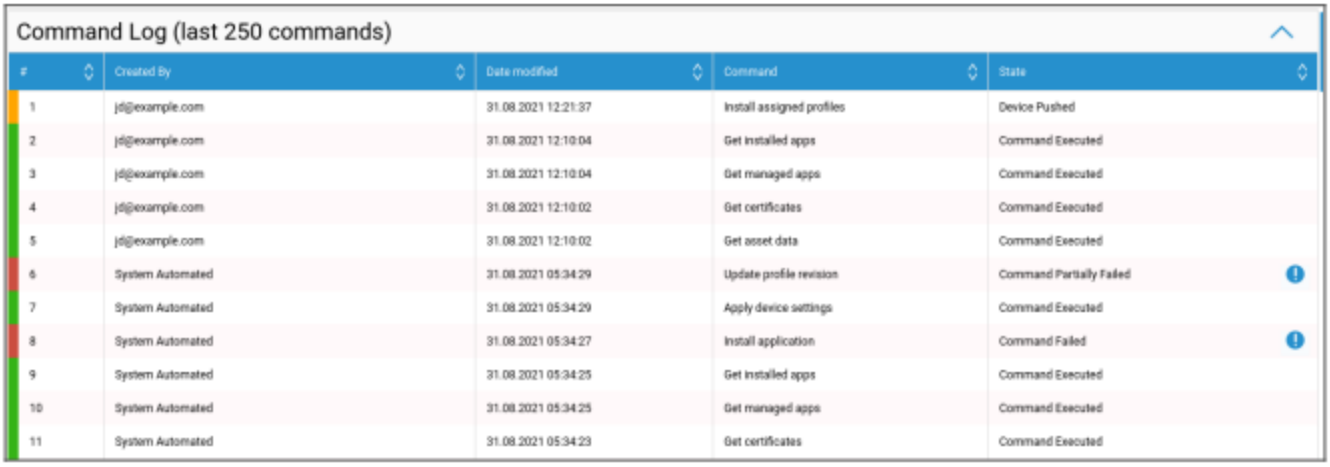
"Newer Revision available" indica que o perfil de grupo foi alterado e guardado, mas não atribuído. O perfil de grupo tem de ser atribuído com "Atribuir agora" ao nível do grupo para aplicar as alterações aos dispositivos.

Registo do dispositivo (apenas ao nível do dispositivo)

Aqui receberás vários registos de dispositivos. Se necessário, podes descobrir diretamente a causa de um erro aqui.

Registo de comandos

Aqui podes ver quais os comandos que foram emitidos para o dispositivo e qual o seu estado.



Status de comando possíveis

Dispositivo empurrado	Foi enviado um pedido push para o serviço push (por exemplo, APNS) para dizer ao dispositivo para se ligar novamente ao servidor EMM.
Comando criado	O comando foi criado no sistema.
Comando enviado	O comando foi enviado para o dispositivo depois de este se ter ligado ao servidor.
Comando Executado	O comando foi executado com sucesso.
Falha no comando	O comando falhou. *
Comando parcialmente falhado	Dependendo do sistema operativo do dispositivo, alguns comandos podem ser agrupados. Neste caso, algumas partes deste grupo de comandos falharam. *
Comando executado, eventualmente falhou	O comando foi executado, mas talvez não o tenha sido.
Comando repuxado	O comando foi reenviado por um utilizador.
Descartado	O comando foi rejeitado. Por exemplo, porque foi substituído por outro comando ou porque o dispositivo foi registado novamente e os comandos antigos foram removidos

*Se houver um ponto de exclamação por trás da mensagem, podes obter mais informações passando o cursor sobre o ícone.

Definições do dispositivo

Configuração do cliente

Aqui podes efetuar as seguintes configurações no teu dispositivo Android:

Tempo fora de conformidade	O limite de tempo limite de resposta do utilizador após o qual a ação de execução é aplicada.
Ação de execução após o tempo limite de cumprimento	Ação de execução quando um utilizador não executa acções que conduzam a um estado de dispositivo conforme
Frequência da recolha de dados	Frequência com que as informações do dispositivo/GPS devem ser recolhidas
Frequência de batimento cardíaco do dispositivo	Intervalo em que o dispositivo deve contactar o Servidor AppTec Min. 1 minuto Máximo. 24 horas
Ativar actualizações de localização	Se estiver ativado, o dispositivo envia actualizações de localização para o Servidor AppTec
Localização Hora de atualização	Determina em que intervalos de tempo o dispositivo envia actualizações de localização para a AppTec
Utilizar a precisão da localização do Google para a atualização da localização	Se estiver activada, a localização da rede será utilizada para actualizações de localização (se estiver desactivada em "Restrições", esta definição não afectará nada)
Utilizar a localização GPS para atualizar a localização	Se estiver ativado, o GPS será utilizado para atualizar a localização
Permitir locais simulados (falsos)	Permite a falsificação de informações de localização através de aplicações de terceiros
Ação de ligação perdida	Se estiver ativado, podes especificar uma ação para o caso de um dispositivo não obter uma ligação ao servidor MDM no intervalo de pulsação. Por exemplo, se o dispositivo tiver um tempo de pulsação de 5 minutos, liga ao servidor às 10:35 AM. Depois disso, o dispositivo sai do alcance do Wi-Fi. O próximo heartbeat às 10:40 AM falhará e a ação especificada será executada.
Ação	A ação que deve ser tomada assim que um dispositivo se torna não-conforme.

	• Lock Dispositivo = bloqueia o dispositivo • Limpar dispositivo = o dispositivo será restaurado para as definições de fábrica • Limpar dispositivo e cartão SD = o dispositivo será restaurado para as definições de fábrica e o armazenamento do cartão SD será eliminado
Limiar	Podes especificar um limite de batimentos cardíacos falhados que são necessários para desencadear a ação especificada.

Modo de aplicação da política	Não cumpre a norma:	Os utilizadores serão solicitados periodicamente a executar acções pendentes
	Aplicação de política preguiçosa:	Nunca será pedido aos utilizadores que executem acções pendentes. Todas as acções abertas serão mostradas no Cliente AppTec
	Aplicação agressiva de políticas:	Os utilizadores serão solicitados ininterruptamente a executar acções pendentes
AppTec Version Lock	Se ativado, pode ser especificado um código de versão para a aplicação AppTec. O cliente AppTec só actualizará para a versão especificada. As versões mais recentes serão ignoradas. NÃO é possível fazer um downgrade.	
Código da versão	Código da versão para a aplicação AppTec a ser bloqueada.	
Desativar a notificação AppTec	Se estiveres desativado, o Cliente AppTec não mostrará uma Notificação na Barra de Notificações. Assim, os utilizadores podem fechar o cliente AppTec através do gestor de tarefas. Se o cliente AppTec estiver fechado, várias funcionalidades, incluindo o Modo Kiosk e a lista negra/branca de aplicações, não funcionarão corretamente. Os dispositivos Samsung oferecem um mecanismo de proteção para o Cliente AppTec. A notificação está desactivada por predefinição nos dispositivos Samsung que suportam as APIs KNOX. A notificação não deve ser desactivada em dispositivos com Android 8.0 ou superior.	

Papel de parede

Define um papel de parede personalizado	Ativar/desativar o papel de parede personalizado
Papel de parede	Define o modo de papel de parede para utilizar um código de cores ou uma imagem
Especifica uma cor	Especifica uma cor de fundo como valor hexadecimal, por exemplo, #000000 para preto ou #ffffff para branco
Definir imagem como papel de parede	Carrega o ficheiro de imagem que pretendes utilizar como papel de parede

Gestão de activos (apenas a nível do dispositivo)

Informações sobre o dispositivo

Modelo	Designação do modelo do aparelho
Sistema operativo	SO
Versão do SO	Versão do SO
Número de série	Número de série
Nome do dispositivo	Nome do dispositivo
Estado da bateria	Estado da bateria
Memória livre / total	Memória livre / total
Samsung Safe	Interface Samsung SAFE, necessária para uma variedade de opções de definição
Cartão SD disponível	Cartão SD disponível
Emulação de cartão SD	Cartão SD emulado
Cartão SD amovível	Cartão SD amovível
SD Livre / Memória Total	SD Free / Memória total do cartão SD

Wi-Fi

Endereço IP	Endereço IP do dispositivo
WiFi MAC	Endereço MAC WiFi

Celular

Estado	Estado (cartão SIM instalado)
Número de telefone	Número de telefone
Roaming (Voz / Dados)	Roaming para voz / dados
Estado do roaming	Estado atual do roaming
Endereço IP	Endereço IP
Operador/Carrier	Operador/Carrier
Tecnologia celular	Tecnologia celular
IMEI	Número IMEI
ICCID	Esta é a identificação do cartão SIM, muitas vezes também um Smartcard ou um cartão de circuito integrado (ICC)
IMSI	O International Mobile Subscriber Identity (IMSI) fornece, nas redes móveis GSM e UMTS, uma identificação definitiva dos utilizadores da rede O IMSI é composto por um máximo de 15 dígitos e é configurado da seguinte forma: • Código de país móvel (MCC), 3 dígitos • Código de rede móvel (MNC), 2 ou 3 dígitos • Número de identificação do assinante móvel (MSIN), 1-10 dígitos
Atual MCC/MNC	Ver "SIM MCC/MNC"
SIM MCC/MNC	O código de país móvel é um identificador de país estabelecido, definido pela UIT de acordo com a norma E.212 Padrão. Trabalha em conjunto com o código de rede móvel (MNC) para a identificação da rede móvel. Significa o país/código de rede móvel do cartão SIM. Se fizeres roaming para outra rede móvel, logicamente, o "Current MCC/MNC" e o "SIM MCC/MNC" serão diferentes.

Bluetooth

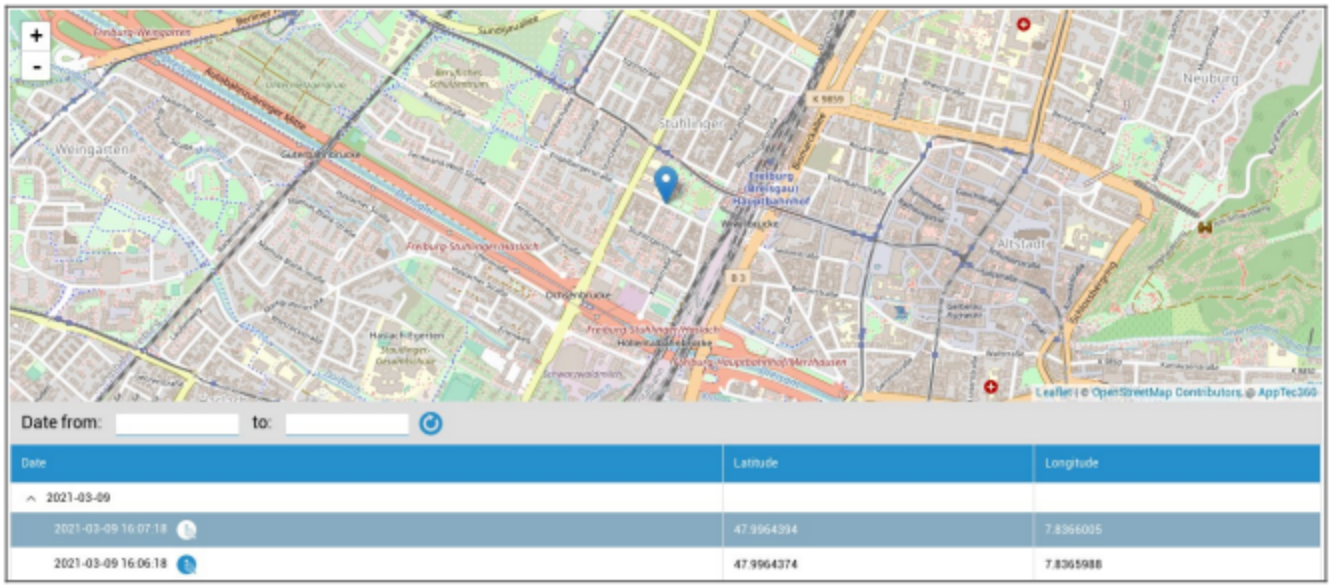
Bluetooth MAC	Endereço MAC Bluetooth

Gestão da segurança

Antirroubo (apenas ao nível do dispositivo)

Informação GPS (apenas ao nível do dispositivo)

Aqui podes determinar a localização atual/última do aparelho. A localização pode ser protegida com uma ou até duas palavras-passe - Vê: Definições gerais - Privacidade - Acesso ao GPS



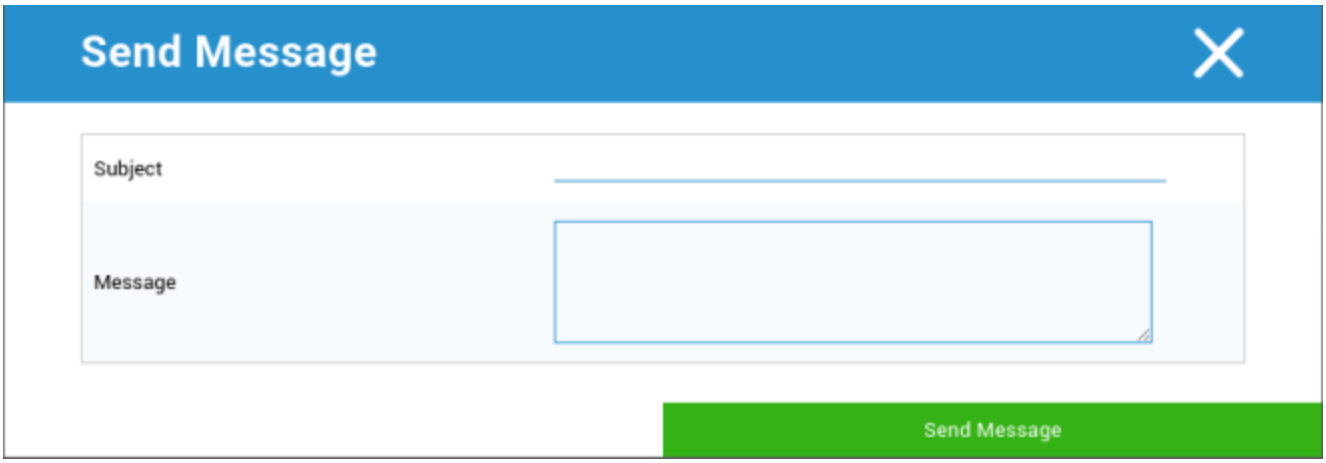
Limpa e bloqueia (apenas ao nível do dispositivo)

Em "Limpar e bloquear", podes realizar as três acções seguintes:

Limpeza total	O dispositivo é restaurado para as definições de fábrica (os dados empresariais e pessoais são eliminados). Só funciona para o Perfil de Trabalho Avançado
Limpeza da empresa	Apenas os dados empresariais são removidos do dispositivo do utilizador final (todas as aplicações, dados, etc. que foram fornecidos pela AppTec)
Bloqueio do ecrã	Se o bloqueio do ecrã estiver ativado, basta desbloquear o dispositivo com a palavra-passe/PIN do dispositivo

Mensagem (apenas a nível do aparelho)

Aqui podes preencher o assunto e uma mensagem e enviá-la para um dispositivo de utilizador final



Configuração de segurança

Código de acesso do dispositivo

Em "Código de acesso" podes definir uma palavra-passe para o dispositivo, estando disponíveis as seguintes opções de definição

Comprimento mínimo da palavra-passe	Estabelece o número mínimo de símbolos que uma palavra-passe deve ter	
Qualidade da palavra-passe	Não especificado	Esta política não prevê requisitos para a palavra-passe.
	Biometria Fraca	Esta política permite a utilização de tecnologia de reconhecimento biométrico de baixa segurança. Isto implica tecnologias que possam reconhecer a identidade de um indivíduo até cerca de um PIN de 3 dígitos (a deteção falsa é inferior a 1 em 1.000).
	Alguma coisa	Esta política requer a definição de algum tipo de palavra-passe ou padrão, mas não impõe quaisquer regras específicas.
	Alfabético	O utilizador deve ter introduzido uma palavra-passe que contenha pelo menos caracteres alfabéticos (ou outro símbolo).
	Alfanumérico	O utilizador deve ter introduzido uma palavra-passe que contenha, pelo menos, caracteres numéricos e alfabéticos (ou outro símbolo).
	Complexo	O utilizador deve ter introduzido uma palavra-passe que contenha pelo menos uma letra, um dígito numérico e um símbolo especial, por defeito. Com esta qualidade de palavra-passe, as palavras-passe podem ser restringidas a conter vários conjuntos de caracteres, como pelo menos uma letra maiúscula, etc.
Comprimento mínimo da palavra-passe	Define o número necessário de caracteres para a palavra-passe. Por exemplo, podes exigir que o PIN ou as palavras-passe tenham pelo menos seis caracteres.	
Mínimo de dígitos numéricos exigidos na palavra-passe	Mínimo de dígitos numéricos exigidos na palavra-passe	

Mínimo de letras minúsculas exigidas na palavra-passe	Mínimo de letras minúsculas exigidas na palavra-passe
Mínimo de letras maiúsculas exigidas na palavra-passe	Mínimo de letras maiúsculas exigidas na palavra-passe
Mínimo de caracteres não alfabéticos exigidos na palavra-passe	Mínimo de caracteres não alfabéticos exigidos na palavra-passe
Símbolos mínimos exigidos na palavra-passe	Símbolos mínimos exigidos na palavra-passe

Bloqueio do tempo máximo de inatividade	Inatividade máxima do utilizador até ao bloqueio de tempo
Tempo limite de expiração da palavra-passe	Estabelece, após o que a palavra-passe expira e tem de ser emitida uma nova palavra-passe
Restrição do histórico de palavras-passe	Número de palavras-passe utilizadas anteriormente que não são permitidas
Máximo de tentativas falhadas da palavra-passe	Estabelece a frequência com que uma palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo
Permite a autenticação biométrica	Permite a autenticação através da leitura de impressões digitais ou da íris. Apenas para Samsung KNOX 2.1 e superior

Código de acesso do contentor

Em "Código de acesso", podes definir uma palavra-passe para o contentor, com as seguintes opções de definição
disponível para ti

Comprimento mínimo da palavra-passe	Estabelece o número mínimo de símbolos que uma palavra-passe deve ter	
Qualidade da palavra-passe	Não especificado	Esta política não prevê requisitos para a palavra-passe.
	Biometria Fraca	Esta política permite a utilização de tecnologia de reconhecimento biométrico de baixa segurança. Isto implica tecnologias que possam reconhecer a identidade de um indivíduo até cerca de um PIN de 3 dígitos (a deteção falsa é inferior a 1 em 1.000).
	Alguma coisa	Esta política requer a definição de algum tipo de palavra-passe ou padrão, mas não impõe quaisquer regras específicas.
	Alfabético	O utilizador deve ter introduzido uma palavra-passe que contenha pelo menos caracteres alfabéticos (ou outro símbolo).
	Alfanumérico	O utilizador deve ter introduzido uma palavra-passe que contenha, pelo menos, caracteres numéricos e alfabéticos (ou outro símbolo).
	Complexo	O utilizador deve ter introduzido uma palavra-passe que contenha pelo menos uma letra, um dígito numérico e um símbolo especial, por defeito. Com esta qualidade de palavra-passe, as palavras-passe podem ser restringidas a conter vários conjuntos de caracteres, como pelo menos uma letra maiúscula, etc.
Comprimento mínimo da palavra-passe	Define o número necessário de caracteres para a palavra-passe. Por exemplo, podes exigir que o PIN ou as palavras-passe tenham pelo menos seis caracteres.	
Mínimo de dígitos numéricos exigidos na palavra-passe	Mínimo de dígitos numéricos exigidos na palavra-passe	
Mínimo de letras minúsculas exigidas	Mínimo de letras minúsculas exigidas na palavra-passe	

na palavra-passe	
Mínimo de letras maiúsculas exigidas na palavra-passe	Mínimo de letras maiúsculas exigidas na palavra-passe
Mínimo de caracteres não alfabéticos exigidos na palavra-passe	Mínimo de caracteres não alfabéticos exigidos na palavra-passe
Símbolos mínimos exigidos na palavra-passe	Símbolos mínimos exigidos na palavra-passe

Bloqueio do tempo máximo de inatividade	Inatividade máxima do utilizador até ao bloqueio de tempo
Tempo limite de expiração da palavra-passe	Estabelece, após o que a palavra-passe expira e tem de ser emitida uma nova palavra-passe
Restrição do histórico de palavras-passe	Número de palavras-passe utilizadas anteriormente que não são permitidas
Máximo de tentativas falhadas da palavra-passe	Estabelece a frequência com que uma palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo

AntiVírus

Verificação automática	Ativar as verificações automáticas periódicas
Intervalo de digitalização	Intervalo para exame (rápido / completo)
Verificação automática completa	Ativar as verificações automáticas completas
Actualizações automáticas	Ativar actualizações automáticas
Intervalo de verificação de atualização	Com que frequência a aplicação e a sua base de dados devem ser actualizadas (vírus / código danificado)
Proteção de aplicações	Ativar a verificação automática de aplicações
Proteção do cartão SD	Ativar a verificação automática do cartão SD
Atualização apenas de Wi-Fi	Quando ativado, as actualizações só serão aplicadas quando o dispositivo estiver ligado com êxito a uma rede Wi-Fi

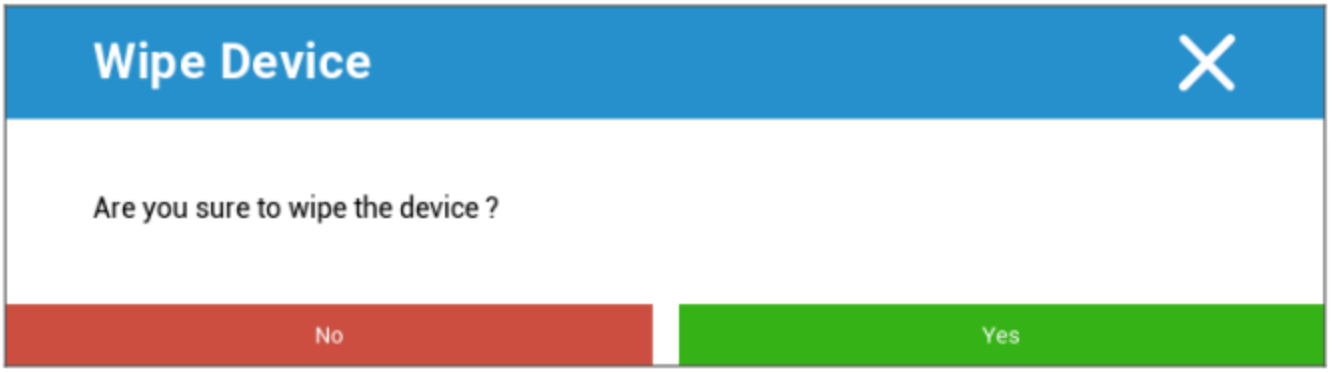
Fim de vida (apenas a nível do dispositivo)

Limpa (apenas ao nível do dispositivo)

Em "Limpar", podes repor as definições de fábrica do dispositivo (apenas no perfil de trabalho melhorado).

Aqui, os dados empresariais, bem como os dados privados, serão eliminados no dispositivo do utilizador final.

Ao clicar no "Símbolo de Menos" recebes a seguinte mensagem:



Com "Sim" podes fazer a limpeza.

Em "Relatório de limpeza", podem ser apresentados os seguintes itens

Limpado por	Histórico de quem realizou a limpeza
Data	Data
Estado	Estado (por exemplo, se a limpeza foi efectuada com êxito)

Definições de restrições

Restrições

Aqui, é possível restringir e bloquear uma série de coisas.

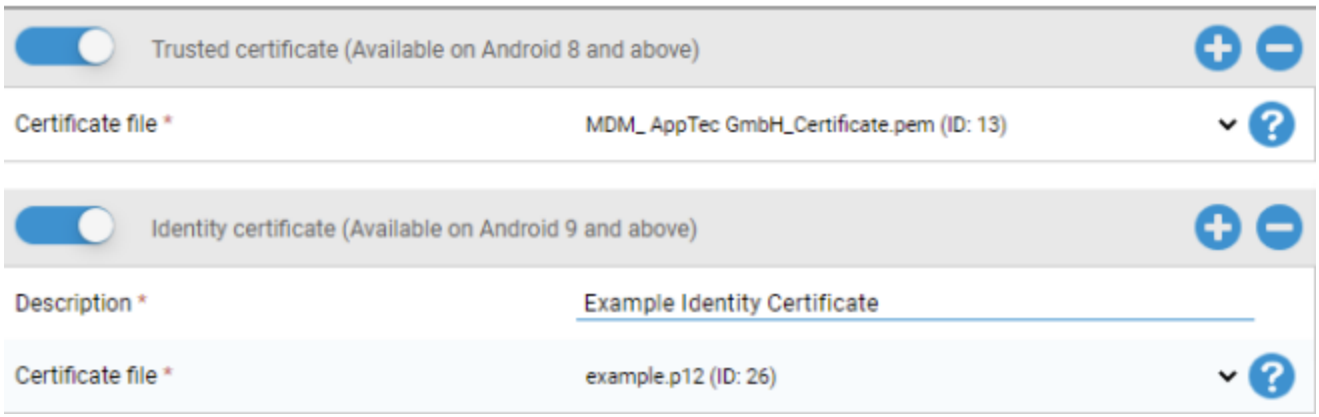
Aplicação da conformidade	Modo Avisar o utilizador - O utilizador será avisado para realizar as acções necessárias. Contentor de bloqueio de modo - Oculta todas as aplicações até que todos os requisitos sejam cumpridos
Política de permissão de tempo de execução	Avisa o utilizador para novos pedidos de autorização Concede sempre novos pedidos de autorização Recusa sempre novos pedidos de autorização Avisa: Algumas aplicações têm problemas em reconhecer as permissões se estas forem definidas automaticamente. Se concederes sempre permissões e tiveres problemas com aplicações que dizem que faltam permissões, define esta opção para "solicitar ao utilizador" e reinstala a aplicação
Permite a saída da área de transferência	Permite copiar e colar do interior do contentor para o exterior
Permite a resolução do identificador de chamadas	Mostra o nome de uma chamada recebida com base nos contactos do contentor
Permitir a resolução da pesquisa de contactos	Permite procurar nomes nos contactos do contentor ao fazer chamadas
Permitir a partilha de contactos Bluetooth	Permite o acesso ao contacto do contentor no automóvel
Não permitir o feixe NFC de saída	Desactiva o NFC para o contentor
Permitir fontes desconhecidas	Se estiver ativado, os utilizadores podem fazer o sideload de aplicações instalando um ficheiro .apk.
Permite a depuração USB	Se estiver ativado, os utilizadores podem ativar a Depuração USB.
Não permitir a modificação da conta	Não permite a criação, eliminação e modificação de contas no contentor Tem em atenção que algumas aplicações precisam de criar ou modificar contas para funcionarem como esperado

Restrições do perfil de trabalho. Disponível apenas em dispositivos Android 11 e superior, com Perfil de trabalho melhorado	
Não permitir a câmara	Especifica se a câmara não é permitida no perfil de trabalho.
Não permitir Bluetooth	Especifica se o bluetooth não é permitido no perfil de trabalho.
Ativar a proteção contra reposição de fábrica	Ativa esta opção para substituir a proteção contra reposição de fábrica do Android pela conta Google que definiste em "Definições gerais" → "Configuração do Android" → "Android Enterprise" → "Proteção contra reposição de fábrica" Se esta opção estiver activada e reiniciares o dispositivo, terás de fornecer a conta Google configurada para configurar novamente o dispositivo.
Atualização do SO de controlo	Ativa esta opção para definir o comportamento de atualização como automático, em janelas ou adiado.
Atualizar a política	Automático: instala automaticamente assim que uma atualização estiver disponível. Em janela: Instala automaticamente dentro de uma janela de manutenção diária. Isto também configura as aplicações do Play para serem actualizadas dentro da janela. Isto é fortemente recomendado para dispositivos de quiosque, porque esta é a única forma de as aplicações persistentemente fixadas no primeiro plano poderem ser actualizadas pelo Play. Adiar: Adia a instalação automática até um máximo de 30 dias.

Restrições do perfil pessoal. Disponível apenas em dispositivos Android 11 e superior, com Perfil de trabalho melhorado	
Não permitir a câmara	Especifica se a câmara não é permitida no perfil pessoal.
Não permitir Bluetooth	Especifica se o bluetooth não é permitido no perfil pessoal.
Permitir fontes desconhecidas	Se estiver ativado, os utilizadores de perfis de trabalho podem fazer o sideload de aplicações instalando um ficheiro .apk.

Gestão de certificados

Aqui podes distribuir Certificados de Confiança e Certificados de Identidade aos teus dispositivos. O Android 8 ou superior é necessário para distribuir Certificados Fidedignos e o Android 9 ou superior é necessário para distribuir Certificados de Identidade.



Com o "+" podes adicionar vários certificados.

Os certificados de confiança têm de estar no formato PEM.

Os certificados de identidade têm de estar no formato PKCS12.

Gestão de ligações

Wifi

Para esta definição, efectua a pré-configuração dos dispositivos do utilizador final, para aceder ao acesso interno
Pontos

Identificador do conjunto de serviços (SSID)	SSID da rede a ser conectada
Rede oculta	Ativar, no caso de o AP não transmitir o SSID

Tipo de segurança

Estabelece o tipo de segurança do PA

WEP

Palavra-passe	Palavra-passe para o PA

WPA/WPA2

Palavra-passe	Palavra-passe para o PA

802.1x EAP

Método EAP

PWD	Identidade	Identidade
	Palavra-passe	Palavra-passe

PEAP	Protocolo de autenticação de fase 2	nenhum	Nenhum protocolo adicional
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidade	Identidade	
	Identidade anónima	Identidade anónima	
	Palavra-passe	Palavra-passe	

TTLS	Protocolo de autenticação de fase 2	nenhum	Nenhum protocolo adicional
		PAP	Protocolo PAP
		MSCHAP	Protocolo MSCHAP
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidade	Identidade	
	Identidade anónima	Identidade anónima	
	Palavra-passe	Palavra-passe	

TLS	Certificado CA	Certificado CA
	Identidade	Identidade
	Palavra-passe	Palavra-passe

VPN

Nome da ligação	Nome da ligação VPN

Tipo de VPN

VPN

Cliente VPN

Cliente VPN AppTec	
Configuração da porta de entrada	Selecciona a Configuração VPN da Gateway (Ver **Definições Gerais > Gateway Universal > Definições VPN**)
VPN sempre ativa	Ativar o bloqueio nativo
Ativar o AppTec Lockdown	Ativar o AppTec Lockdown

Integrado (apenas disponível em dispositivos Samsung)			
Tipo de ligação	PPTP	Servidor	Servidor
		Ativar a encriptação PPTP	Ativar a encriptação PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Ativar o segredo L2TP	Ativar o segredo L2TP
		Segredo L2TP	Segredo L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
Domínios de pesquisa DNS	Domínios de pesquisa DNS		
Definições de especialistas	Servidores DNS	Servidores DNS	
	Encaminhamento de rotas	Encaminhamento de rotas	

Abre a VPN		
Servidor	Servidor	
Perfil OpenVPN	Perfil OpenVPN	
Aplicação OpenVPN	OpenVPN para Android (recomendado)	
	Ligação OpenVPN	
Definições de especialistas	Servidores DNS	Servidores DNS
	Encaminhamento de rotas	Encaminhamento de rotas

Samsung / Strong Swan			
Tipo de ligação	PPTP	Servidor	Servidor
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar a encriptação PPTP	Ativar a encriptação PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar o segredo L2TP	Segredo L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
Definições de especialistas	Servidores DNS	Servidores DNS	
	Encaminhamento de rotas	Encaminhamento de rotas	

Cisco Any Connect		
Servidor	Servidor	
Modo de certificado	Desativado	Desativado
	Automático	Automático
Definições de especialistas	Servidores DNS	Servidores DNS
	Encaminhamento de rotas	Encaminhamento de rotas

VPN por aplicação

Cliente VPN

Cliente VPN AppTec		
Configuração da porta de entrada	Selecciona a Configuração VPN da Gateway (Ver **Definições Gerais > Gateway Universal > Definições VPN**)	
Aplicações VPN	Aplicações VPN	
VPN sempre ativa	Ativar o bloqueio nativo	VPN sempre ativa
Ativar o AppTec Lockdown	Ativar o AppTec Lockdown	

Samsung / Strong Swan			
Tipo de ligação	PPTP	Servidor	Servidor
		Aplicações VPN	Aplicações VPN
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar a encriptação PPTP	Ativar a encriptação PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Aplicações VPN	Aplicações VPN
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
		Ativar o segredo L2TP	Segredo L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Aplicações VPN	Aplicações VPN
		Identificador IPSec	Identificador IPSec
		Chave pré-partilhada IPSec	Chave pré-partilhada IPSec
		Nome de utilizador	Nome de utilizador
		Palavra-passe	Palavra-passe
Definições de especialistas	Servidores DNS	Servidores DNS	
	Encaminhamento de rotas	Encaminhamento de rotas	

Restrições

Aqui podes definir as restrições, em relação à gestão da ligação

Permitir roaming de dados	Permitir dados móveis em roaming
Forçar Roaming de Dados	Se estiver ativado, o roaming para dados móveis é permanentemente ativado (não recomendado!) Esta definição substitui a definição "Permitir Roaming de Dados"!
Utiliza o servidor proxy http do sistema	A utilização de um servidor proxy HTTP, que é fornecido pelas definições do sistema nas definições, depende da rede ligada (WiFi ou APN)

Gestão PIM

Gmail Exchange

Informação: Esta Configuração será aplicada à aplicação Gmail. Por isso, tens de aprovar e instalar o Gmail.

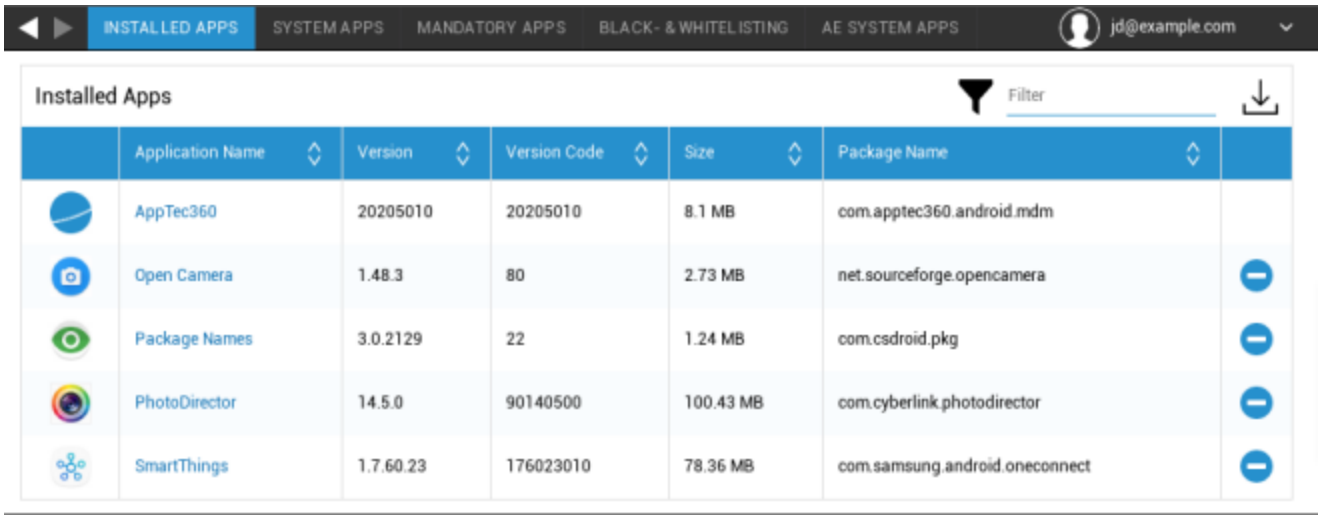
Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique, podes ver por ti próprio
Nome de anfitrião do servidor	Endereço do servidor dos teus Servidores Exchange
Nome de utilizador	O nome de utilizador (Login-Name) do respetivo dispositivo do utilizador final, tem também em atenção os "Placeholders here
Assinatura	Podes anexar uma assinatura (Dica: alguns dispositivos exigem formatação HTML para a assinatura)
Número de dias anteriores a sincronizar	Número de dias, determinando quando os e-mails são sincronizados de volta
Identificador do dispositivo	Uma cadeia de caracteres que contém o ID do dispositivo EAS. Faz parte do protocolo EAS e está disponível em algumas regiões
Utiliza Secure Sockets Layer (SSL)	Utiliza uma ligação SSL
Aceita todos os certificados	Todos os certificados são aceites. Selecciona esta opção, se o teu Exchange Server utilizar um certificado auto-assinado
Permitir contas não geridas	Permite que os utilizadores adicionem ou removam qualquer conta do Exchange, que não seja a conta especificada nesta configuração gerida. Se esta definição estiver activada, não podes impedir os utilizadores de adicionarem outras contas do Exchange ao Gmail. Também não podes controlar a partilha de dados entre outras aplicações e contas Exchange adicionadas pelos utilizadores. Esta definição só deve ser activada se os teus utilizadores precisarem de manter mais do que uma conta Exchange de trabalho no Gmail.
Certificado de cliente	Certificado de cliente. Só é necessário se o teu servidor de correio eletrónico esperar que isto esteja presente.

Gestão de aplicações

Gestor de aplicações empresariais

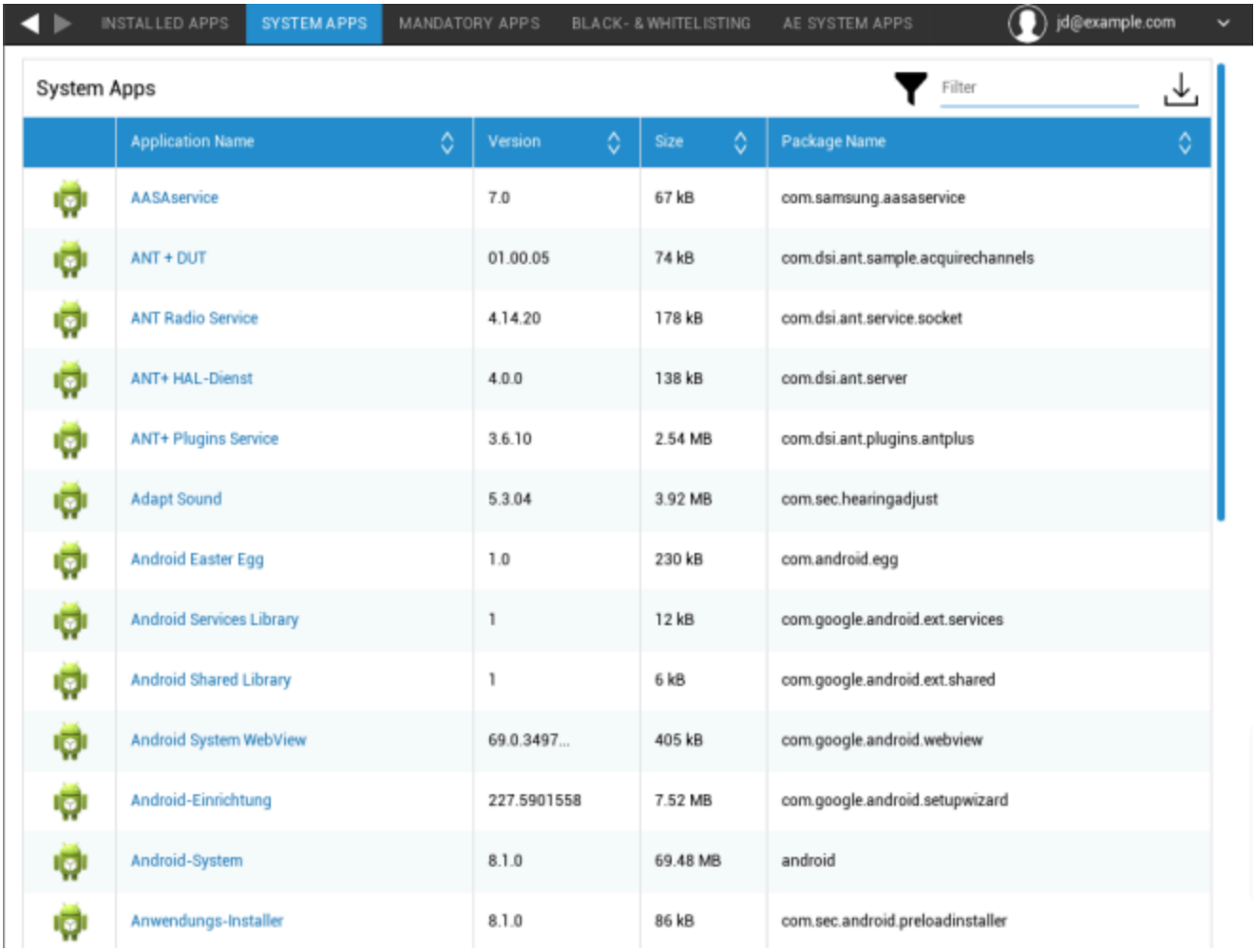
Aplicações instaladas (apenas ao nível do dispositivo)

Aqui, todas as aplicações que estão atualmente instaladas no contentor serão apresentadas para ti.



Aplicações de sistema (apenas ao nível do dispositivo)

Em "System Apps" (Aplicações do sistema), todas as aplicações e serviços que já foram instalados no dispositivo do utilizador final pelo fabricante do dispositivo serão listados para ti.

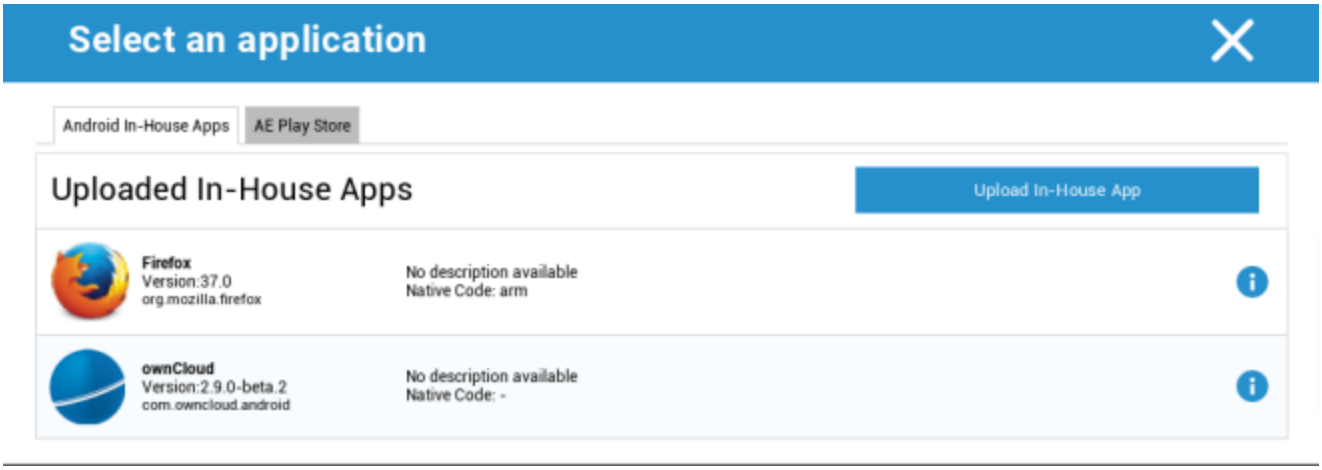


Aplicações obrigatórias

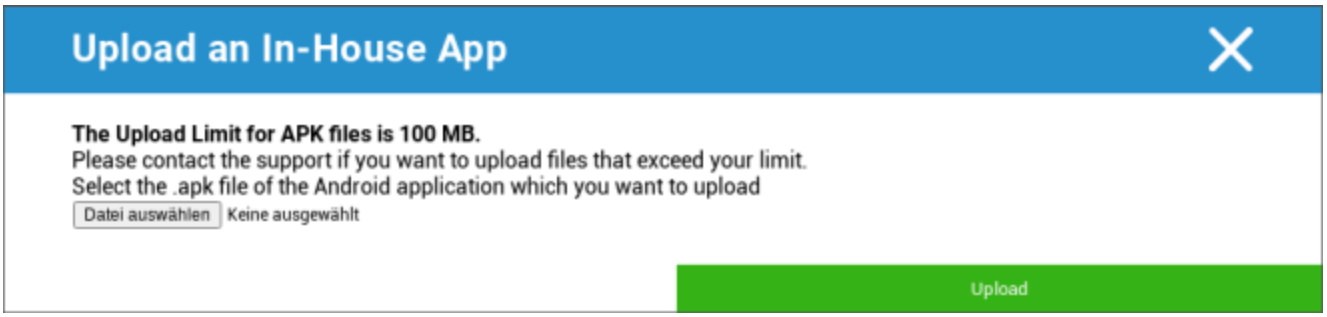
Em Aplicações obrigatórias, podes definir as aplicações obrigatórias. O utilizador será continuamente solicitado a instalar esta aplicação designada, se for uma aplicação interna. As aplicações da Play Store serão instaladas automaticamente.

Através do , podes definir a aplicação obrigatória requerida.

Pode ser uma aplicação interna da lista "Aplicações internas do Android", que carregaste nas Definições gerais.

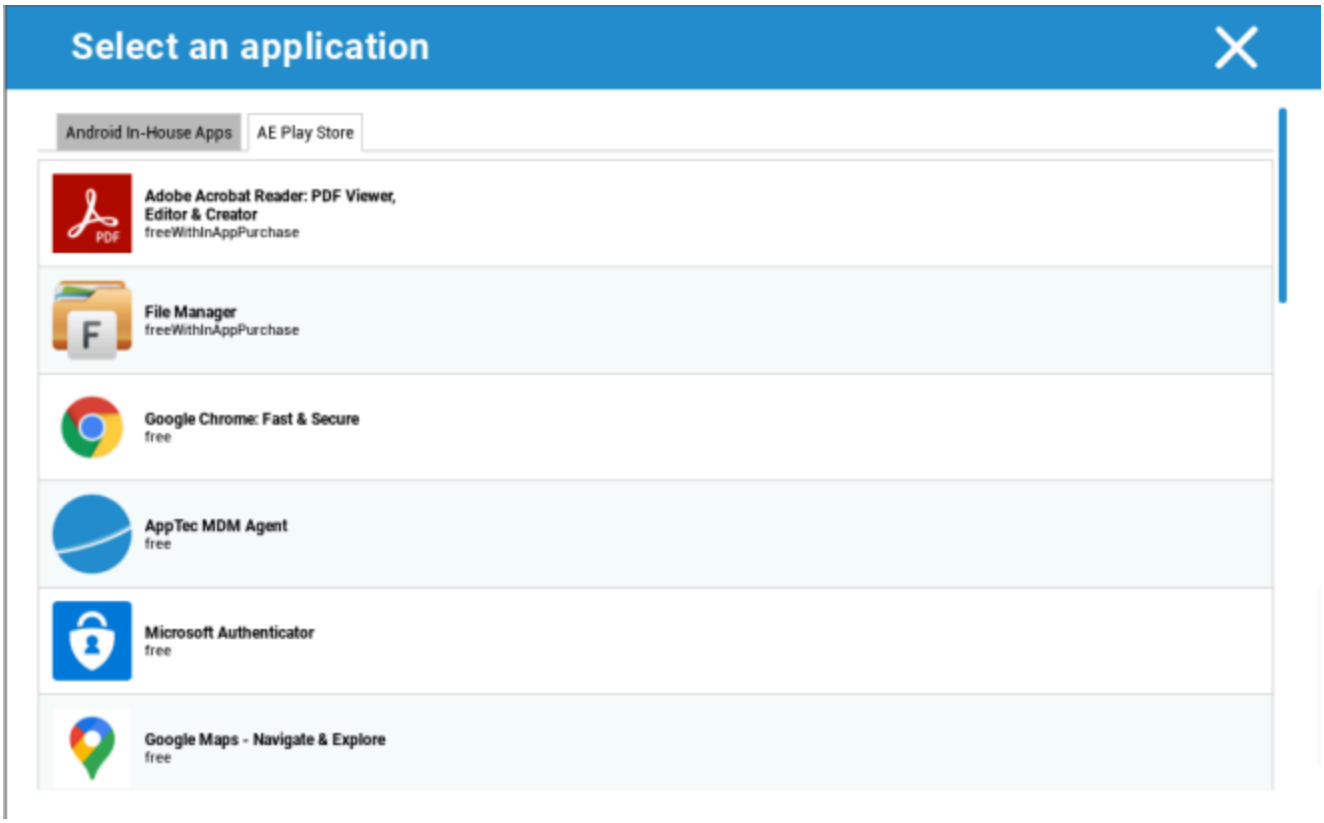


Também podes selecionar e carregar diretamente um ficheiro apk com "Carregar aplicação interna".



Se estiveres a instalar uma aplicação interna, terás a possibilidade de ativar "Manter atualizado". Se esta opção estiver activada e tiveres definido uma versão mais recente na BD de aplicações internas, a aplicação será actualizada no dispositivo.

Ou pode ser uma aplicação "AE Play Store" da Google Work Play Store.



Apenas as "Aplicações da AE Play Store" aprovadas serão mostradas neste separador.

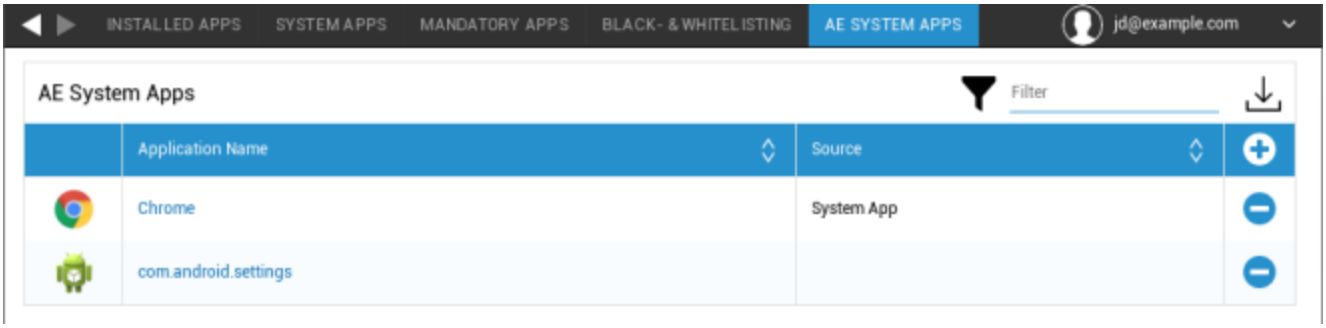
Para aprovar uma "Aplicação da AE Play Store", vai a "Definições gerais" > "Gestão de aplicações" > "AE Play

Store" e adiciona uma aplicação através do botão que te redirecciona para o separador "Play Store Apps" (ou podes ir diretamente para o separador "Play Store Apps").

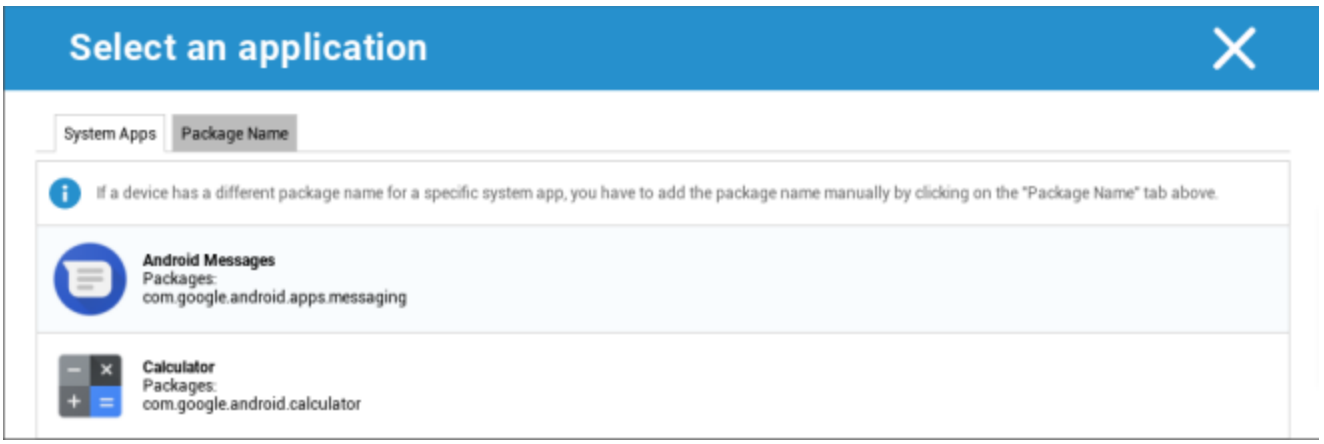
No separador "Aplicações da Play Store", podes procurar aplicações. Quando clicas numa aplicação, a página da aplicação abre-se e aqui podes aprovar a aplicação clicando em "Aprovar".

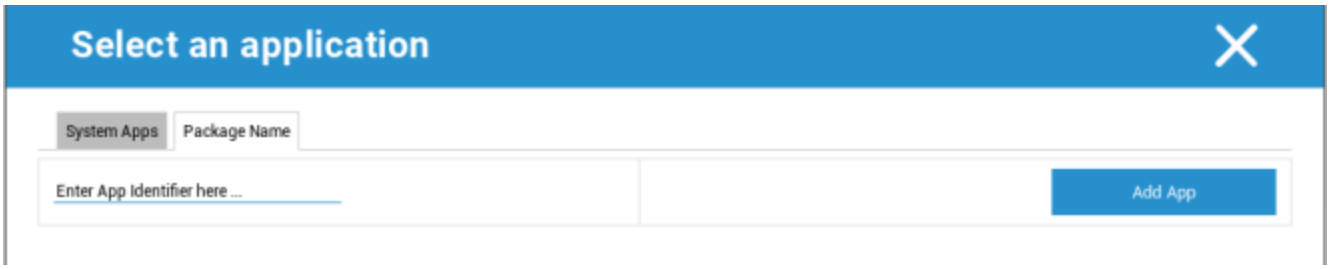
Aplicações do sistema AE

Aqui podes definir uma lista que contém aplicações de sistema específicas que devem ser activadas nos dispositivos.



Se clicares no botão, podes escolher a partir de uma lista de possíveis aplicações de sistema fornecidas pelo Google ou introduzir diretamente o nome do pacote de uma aplicação de sistema que deve ser activada.





Tem em atenção que as aplicações de sistema na lista fornecida pela Google são apenas aplicações que podem ser aplicações de sistema, mas não têm necessariamente de ser aplicações de sistema nos teus dispositivos.

No entanto, esta lista só afecta as aplicações que já estão pré-instaladas.

A adição de aplicações que não estejam pré-instaladas nos teus dispositivos não afectará os teus dispositivos, independentemente de a aplicação pertencer à lista fornecida pelo Google ou de o nome do pacote da aplicação ser introduzido diretamente.

Restrições e definições

Definições de gestão de aplicações

Aqui podes configurar o comportamento do dispositivo relativamente às actualizações de aplicações.

Atualizar a frequência de verificação	Especifica em que intervalo o Cliente AppTec irá procurar actualizações de aplicações. O valor predefinido é 24 horas.
Limiar Wi-Fi	As aplicações maiores do que o tamanho especificado serão descarregadas através de Wi-Fi. Se selecionar "Apenas Wi-Fi", todas as aplicações serão descarregadas através de Wi-Fi.

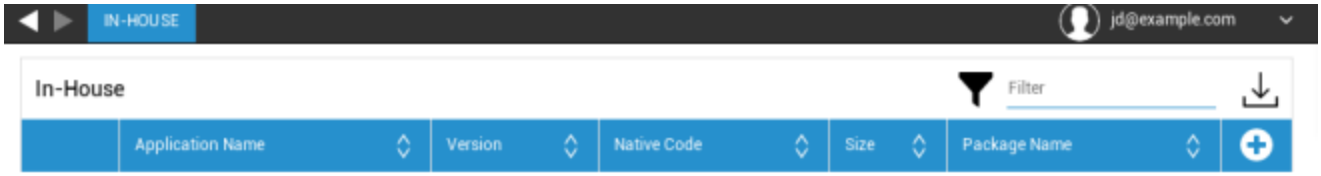
Loja de aplicações para empresas

Internamente

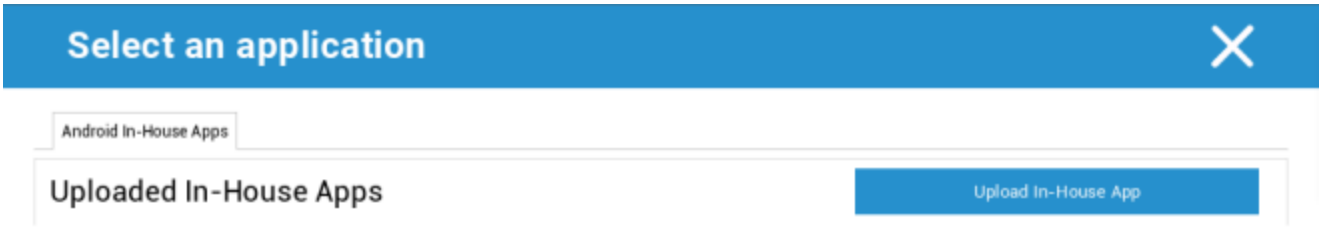
No ponto "In-House", podes carregar e distribuir aplicações desenvolvidas internamente.

Com o símbolo, podes distribuir mais aplicações internas.

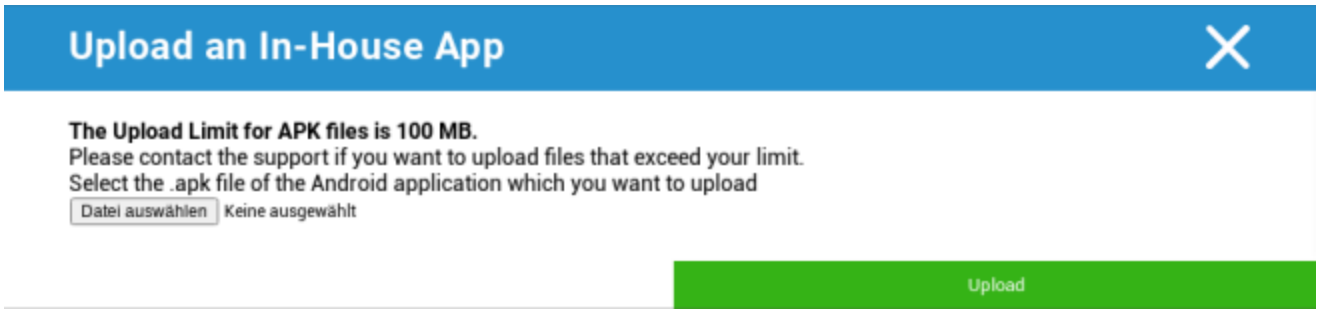
Se estiveres a instalar uma aplicação interna, terás a possibilidade de ativar "Manter atualizado". Se esta opção estiver activada e tiveres definido uma versão mais recente na BD de aplicações internas, a aplicação será actualizada no dispositivo.



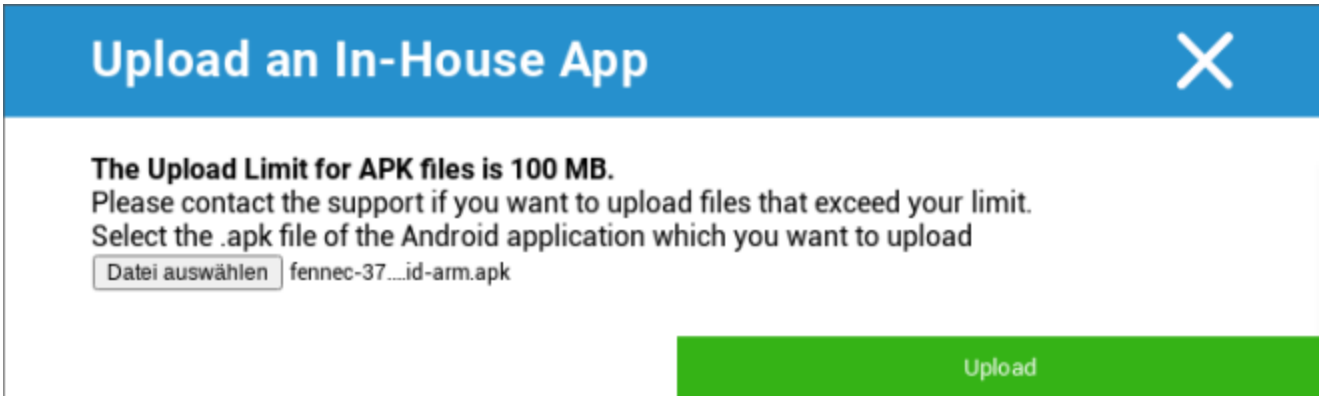
Se não tiveres distribuído aplicações internas, receberás a seguinte visão geral:



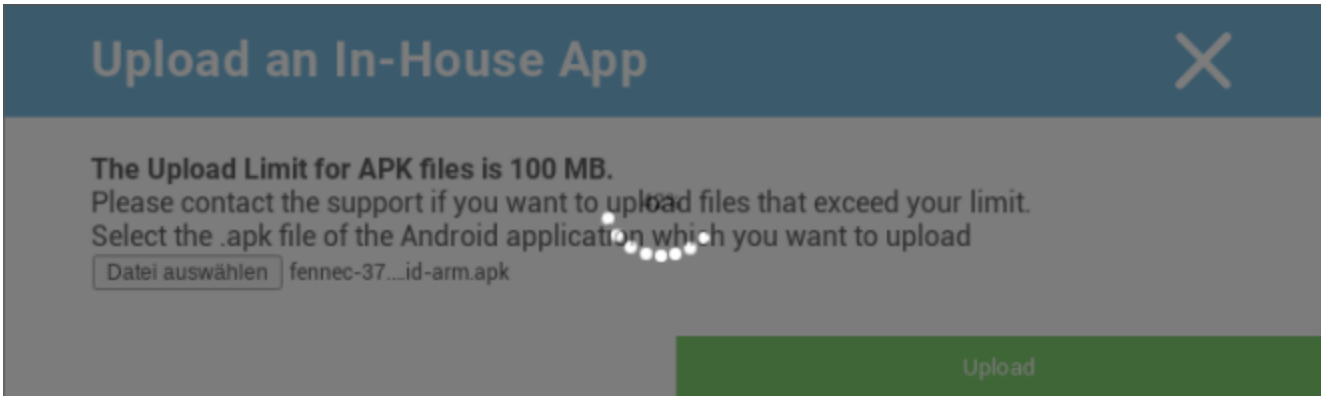
Para isso, clica em "Upload In-House App", e receberás a seguinte visão geral:



Agora, escolhe com "Procurar..." um ficheiro .apk e depois clica em "Carregar".



A tua aplicação será agora carregada. No meio do círculo, verás um indicador de percentagem, que mostra a parte da tua aplicação que já foi carregada.



Se o carregamento da tua aplicação interna tiver sido bem sucedido, podes encontrar a aplicação carregada no teu Catálogo de Aplicações.

O utilizador tem agora a opção de ver e instalar esta aplicação na AppTec Store no dispositivo do utilizador final, na categoria "In-House".

Uma vez que não se trata de uma aplicação da Google PlayStore, o utilizador não necessita de um ID Google armazenado no respetivo dispositivo do utilizador final.

Empresa Play Store

AE Play Store

Aqui podes adicionar aplicações à Android Enterprise Playstore. Tem em atenção que tens de aprovar as aplicações com a tua conta de administrador AE antes de as poderes adicionar.

Para aprovares uma aplicação, consulta as instruções em Aplicações obrigatórias.

Gestão de conteúdos

ContentBox

Aqui podes ativar a ContentBox.

Assim que mudares "Enable ContentBox" (Ativar ContentBox) para "On" (Ligado), será automaticamente instalada uma aplicação ContentBox separada no dispositivo do utilizador final.

Navegador seguro

Aqui podes configurar as definições para o AppTec Secure Browser.

Assim que mudares a secção do "Secure Browser" para "On", será automaticamente instalada uma aplicação de browser separada no dispositivo do utilizador final.

Requerer palavra-passe	Exige que o utilizador defina e utilize uma palavra-passe para aceder ao browser.
Comprimento mínimo exigido para a palavra-passe	Define o número necessário de caracteres para a palavra-passe
Qualidade da palavra-passe necessária	Define a qualidade da palavra-passe necessária
Restringir transferências / Abrir em	
Restringir carregamentos	
Carregar lista branca	Uma lista de URLs para os quais o carregamento será sempre permitido.
Permitir cópia	Permite copiar, cortar ou partilhar texto dentro das páginas Web.
Permite a captura de ecrã	Permite a captura de imagens de ecrã.
Frequência da limpeza de dados	Selecciona com que frequência TODOS os dados do utilizador (histórico, cache, etc.) devem ser automaticamente removidos.
Marcadores da empresa	Os marcadores aparecerão na pasta "Marcadores da empresa" nos marcadores do navegador. Não são editáveis pelo utilizador.
Ocultar a barra de endereços	
Lista branca no navegador (sem Universal Gateway)	Ativa a lista branca de URLs do lado do cliente. • Os marcadores da empresa são sempre colocados na lista branca • Suportado apenas para 100 URLs • Utiliza o Universal Gateway para a criação ilimitada de listas negras e brancas
URLs na lista branca	Uma lista de URLs permitidos.

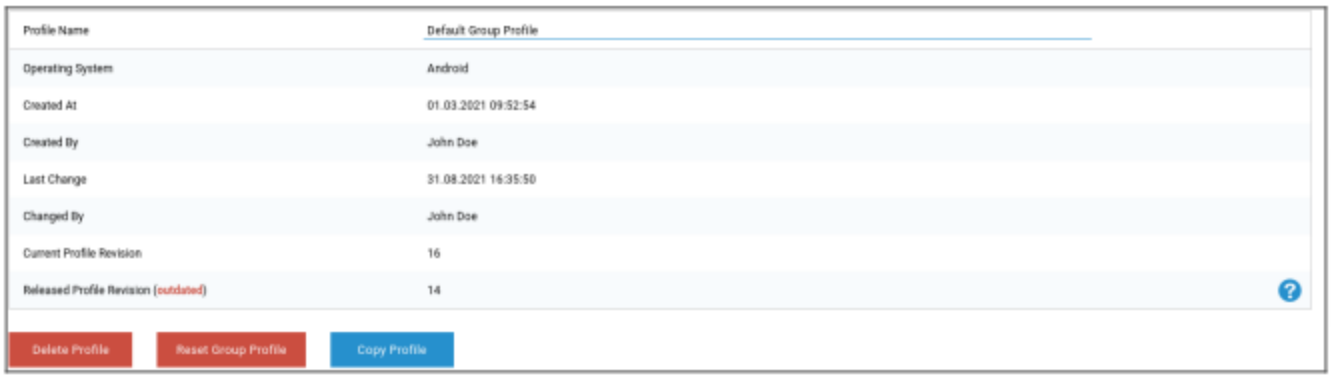
Lista negra e lista branca baseadas em gateway	A inclusão na lista negra tem os seguintes requisitos: • Um AppTec Universal Gateway a funcionar ("Definições gerais" → "Universal Gateway") • Uma configuração VPN em funcionamento com um servidor DNS especificado ("Definições gerais" → "Gateway universal" → "Definições VPN") • Configuração de uma lista negra ("Definições gerais" → "Universal Gateway" → "Lista negra de domínios") • Uma ligação VPN válida no perfil ("Gestão de ligações" → "VPN")

Configuração do Android

Geral

Síntese do perfil do grupo (apenas a nível do grupo)

Ao abrires um perfil de grupo, terás uma visão geral rápida do perfil.



Nome do perfil	Nome do perfil (pode ser alterado aqui)
Sistema operativo	Sistema operativo para o qual o perfil se destina
Criado em	Tempo de criação
Criado por	O criador do perfil
Última alteração	Hora da última modificação do perfil
Alterado por	Conta que efectuou as últimas alterações
Revisão do perfil atual	Revisão do estado do perfil guardado
Revisão do perfil lançado	Revisão do perfil atribuído ("Atribuir agora"). Se a etiqueta apresentar " (desatualizado)" por trás do texto, significa que guardaste o perfil mas ainda não o atribuíste, pelo que os dispositivos continuarão a receber uma versão mais antiga.

Síntese do dispositivo (apenas ao nível do dispositivo)

Se estiveres num dispositivo, receberás uma recapitulação geral do dispositivo selecionado, que contém o seguinte:

Nome do dispositivo	Nome do dispositivo
Última localização conhecida	As últimas coordenadas GPS conhecidas
Número de telefone	Número de telefone
Atribuição de aplicações obrigatórias	O número de aplicações obrigatórias atribuídas
Versão do SO	Versão do sistema operativo do dispositivo
Sistema operativo	Sistema operativo (Android / iOS / Windows Phone)
Número de série	Número de série do dispositivo
Propriedade do dispositivo	Dispositivo empresarial ou privado
Tipo de dispositivo	Telefone ou Tablet
Enraizado	Estado, indicando se o dispositivo foi enraizado
Conformidade	Em conformidade com as directrizes
Endereço IP	Endereço IP
Visto pela última vez	Ponto no tempo, quando o dispositivo se ligou pela última vez à AppTec
Último empurrão	Ponto no tempo, quando o servidor enviou um push para o dispositivo
Atribuição de utilizadores	Um menu suspenso para atribuir o dispositivo a outro utilizador

Config Revision (apenas a nível do dispositivo)

Aqui tens uma visão geral do perfil de grupo que está atribuído ao aparelho.

Se clicares no perfil de grupo, acederás diretamente ao perfil e poderás efetuar definições.

Com o símbolo, podes reverter as aplicações atribuídas para as definições do perfil de grupo.

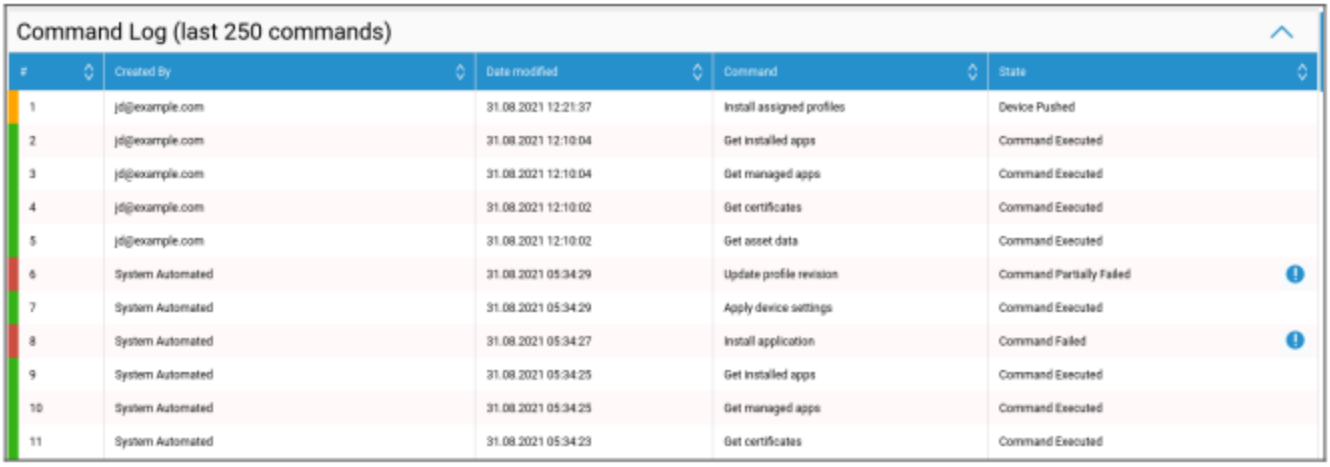
Com o símbolo, podes repor o perfil do dispositivo para que não tenha quaisquer definições.

"Newer Revision available" indica que o perfil de grupo foi alterado e guardado, mas não atribuído. O perfil de grupo tem de ser atribuído com "Atribuir agora" ao nível do grupo para aplicar as alterações aos dispositivos.

Registo do dispositivo (apenas ao nível do dispositivo)

Registo de comandos

Aqui podes ver quais os comandos que foram emitidos para o dispositivo e qual o seu estado.



Os comandos criados por "Sistema automatizado" são automaticamente criados pelo sistema.

Status de comando possíveis

Dispositivo empurrado	Foi enviado um pedido push para o serviço push (por exemplo, APNS) para dizer ao dispositivo para se ligar novamente ao servidor EMM.
Comando criado	O comando foi criado no sistema.
Comando enviado	O comando foi enviado para o dispositivo depois de este se ter ligado ao servidor.
Comando Executado	O comando foi executado com sucesso.
Falha no comando	O comando falhou. *
Comando parcialmente falhado	Dependendo do sistema operativo do dispositivo, alguns comandos podem ser agrupados. Neste caso, algumas partes deste grupo de comandos falharam. *
Comando executado, eventualmente falhou	O comando foi executado, mas talvez não o tenha sido.
Comando repuxado	O comando foi reenviado por um utilizador.
Descartado	O comando foi rejeitado. Por exemplo, porque foi substituído por outro comando ou porque o dispositivo foi registado novamente e os comandos antigos foram removidos

*Se houver um ponto de exclamação por trás da mensagem, podes obter mais informações passando o cursor sobre o ícone.

Definições do dispositivo

Configuração do cliente

Aqui podes efetuar as seguintes configurações no teu dispositivo Android:

Mensagem de aviso após desativar a Gestão de Dispositivos	Mensagem de aviso estabelecida depois de desativar a Gestão de Dispositivos
Tempo fora de conformidade	Limite de tempo, após o qual será executada a "Ação de execução após conformidade", se o dispositivo não estiver em conformidade. Min. 1 minuto Máximo. 24 horas
Ação de execução após o tempo limite de cumprimento	A ação que deve ser tomada assim que um dispositivo se torna não-conforme. • não fazer nada = não agir • Bloquear dispositivo = bloqueia o dispositivo • Limpar dispositivo = o dispositivo será restaurado para as definições de fábrica
Frequência da recolha de dados	Frequência com que as informações do dispositivo/GPS devem ser recolhidas
Frequência de batimento cardíaco do dispositivo	Intervalo em que o dispositivo deve contactar o servidor AppTec360 Min. 1 minuto Máximo. 24 horas
Ativar actualizações de localização	Se estiver ativado, o dispositivo envia actualizações de localização para o servidor AppTec360
Localização Hora de atualização	Determina em que intervalos de tempo o dispositivo envia actualizações de localização para a AppTec
Utilizar a precisão da localização do Google para a atualização da localização	Se estiver activada, a Precisão da localização do Google (anteriormente conhecida como localização da rede) será utilizada para actualizações de localização (se tiver sido desactivada em "Restrições", esta definição não afectará nada)
Utilizar a localização GPS para atualizar a localização	Se estiver ativado, o GPS será utilizado para atualizar a localização

Permitir locais simulados (falsos)	Permite a falsificação de informações de localização através de aplicações de terceiros
Ação de ligação perdida	Permite-te definir uma determinada ação que será executada após um determinado número de batimentos cardíacos falhados
Modo de aplicação da política	Define o grau de agressividade com que o Cliente AppTec360 pede ao utilizador para executar determinadas acções que requerem a entrada do utilizador. Intervalo (Predefinição) = pergunta em intervalos, para que o utilizador possa colocar isto em segundo plano durante algum tempo. Sem alerta = não aparece nenhum pop-up para qualquer interação necessária. Tens de abrir manualmente o AppTec360 Client para verificar se existe uma ação necessária Alerta constante = O utilizador só pode executar a ação pretendida. O cliente AppTec360 forçar-se-á a ficar em primeiro plano se o utilizador tentar evitá-lo
AppTec360 Version Lock	Permite-te definir uma versão do Cliente AppTec360 que é a versão máxima para a qual o cliente se actualiza.

Papel de parede

Aqui podes definir um papel de parede personalizado.

"Especificar uma cor" permite-te definir uma cor em formato hexadecimal (por exemplo, #000000). Só são permitidos valores hexadecimais.

"Definir imagem como papel de parede" permite-te carregar uma imagem. Tem em atenção que diferentes dispositivos com diferentes lançadores e versões do sistema operativo funcionam de forma diferente. Não existe uma linha de orientação geral para o tamanho e o rácio, uma vez que isso depende do dispositivo.

Utiliza JPG (ou JPEG) ou PNG para o formato de ficheiro.

Gestão de activos (apenas a nível do dispositivo)

Gestão de activos

Informações sobre o dispositivo

Modelo	**Designação do modelo do aparelho**
Sistema operativo	SO
Versão do SO	Versão do SO
Apoio AE	Suporte para Android Enterprise (contentor e totalmente gerido)
Número de série	Número de série
Nome do dispositivo	Nome do dispositivo
Estado da bateria	Estado da bateria
Memória livre / total	Memória livre / total
Samsung KNOX	Nível de API do Samsung KNOX
Cartão SD disponível	Cartão SD disponível
Emulação de cartão SD	Cartão SD emulado
Cartão SD amovível	Cartão SD amovível
SD Livre / Memória Total	SD Free / Memória total do cartão SD

Wi-Fi

Endereço IP	Endereço IP do dispositivo
WiFi MAC	Endereço MAC WiFi

Celular

Estado	Estado (cartão SIM instalado)
Número de telefone	Número de telefone
Roaming (Voz / Dados)	Roaming para voz / dados
Estado do roaming	Estado atual do roaming
Endereço IP	Endereço IP
Operador/Carrier	Operador/Carrier
Tecnologia celular	Tecnologia celular
IMEI	Número IMEI
ICCID	Esta é a identificação do cartão SIM, muitas vezes também um Smartcard ou um cartão de circuito integrado (ICC)
IMSI	O International Mobile Subscriber Identity (IMSI) fornece, nas redes móveis GSM e UMTS, uma identificação definitiva dos utilizadores da rede O IMSI é composto por um máximo de 15 dígitos e é configurado da seguinte forma: • Código de país móvel (MCC), 3 dígitos • Código de rede móvel (MNC), 2 ou 3 dígitos • Número de identificação do assinante móvel (MSIN), 1-10 dígitos
Atual MCC/MNC	Ver "SIM MCC/MNC"
SIM MCC/MNC	O código de país móvel é um identificador de país estabelecido, definido pela UIT de acordo com a norma E.212 Padrão. Trabalha em conjunto com o código de rede móvel (MNC) para a identificação da rede móvel. Significa o país/código de rede móvel do cartão SIM. Se fizeres roaming para outra rede móvel, logicamente, o "Current MCC/MNC" e o "SIM MCC/MNC" serão diferentes.

Bluetooth

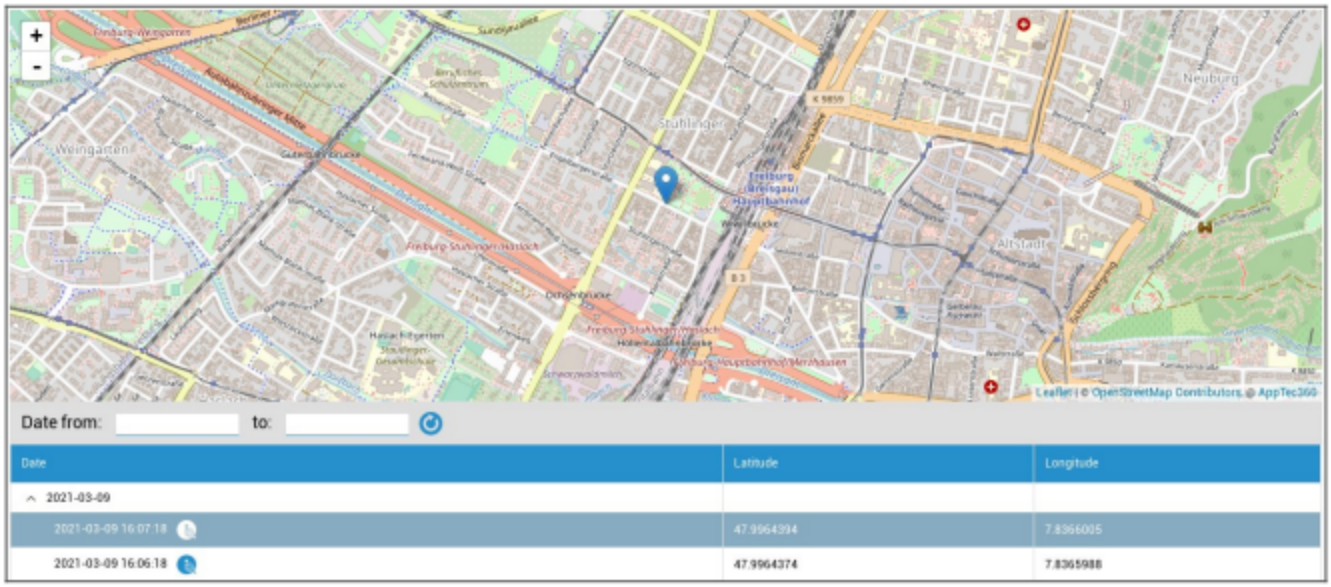
Bluetooth MAC	Endereço MAC Bluetooth

Gestão da segurança

Antirroubo (apenas ao nível do dispositivo)

Informação GPS (apenas ao nível do dispositivo)

Aqui podes determinar a localização atual/última do aparelho. A localização pode ser protegida com uma ou até duas palavras-passe - Vê: Definições gerais - Privacidade - Acesso ao GPS



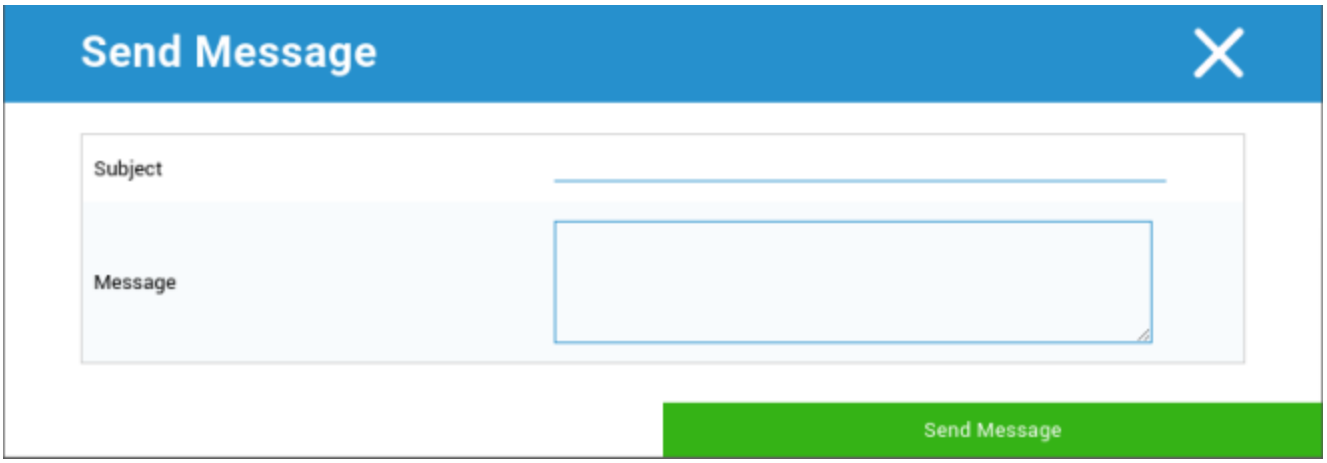
Limpa e bloqueia (apenas ao nível do dispositivo)

Em "Limpar e bloquear", podes realizar as três acções seguintes:

Limpeza total	O dispositivo é restaurado para as definições de fábrica (os dados empresariais e pessoais são eliminados)
Limpeza da empresa	Apenas os dados empresariais são removidos do dispositivo do utilizador final (todas as aplicações, dados, etc. que foram fornecidos pela AppTec360)
Bloqueio do ecrã	Se o bloqueio do ecrã estiver ativado, basta desbloquear o dispositivo com a palavra-passe/PIN do dispositivo

Mensagem (apenas a nível do aparelho)

Podes preencher o assunto e uma mensagem e enviá-la para um dispositivo de utilizador final. Esta mensagem será apresentada no Cliente AppTec360.



Configuração de segurança

Código de acesso

Em "Código de acesso" podes definir uma palavra-passe para o dispositivo, estando disponíveis as seguintes opções de definição

Comprimento mínimo da palavra-passe	Estabelece o número mínimo de símbolos que uma palavra-passe deve ter
Qualidade da palavra-passe	Força da palavra-passe Não especificado = não especificado Todas as palavras-passe são aceitáveis = todas as palavras-passe são aceitáveis pelo menos caracteres numéricos = deve conter pelo menos caracteres numéricos pelo menos caracteres complexos = deve conter pelo menos caracteres especiais at least alphanumerical characters = deve conter pelo menos caracteres alfanuméricos pelo menos caracteres alfabéticos = deve conter pelo menos caracteres alfabéticos
Bloqueio do tempo máximo de inatividade	Tempo máximo de espera no ecrã. Configura apenas o valor máximo que pode ser selecionado pelo utilizador
Mínimo de letras minúsculas exigidas na palavra-passe	Mínimo de letras minúsculas exigidas na palavra-passe
Mínimo de letras maiúsculas exigidas na palavra-passe	Mínimo de letras maiúsculas exigidas na palavra-passe
Mínimo de caracteres não alfabéticos exigidos na palavra-passe	Mínimo de caracteres não alfabéticos exigidos na palavra-passe
Mínimo de dígitos numéricos exigidos na palavra-passe	Mínimo de dígitos numéricos exigidos na palavra-passe
Símbolos mínimos exigidos na palavra-passe	Símbolos mínimos exigidos na palavra-passe
Tempo limite de expiração da palavra-passe	Estabelece, após o que a palavra-passe expira e tem de ser emitida uma nova palavra-passe
Restrição do histórico de palavras-passe	Número de palavras-passe utilizadas anteriormente que não são permitidas
Máximo de tentativas falhadas da palavra-passe	Estabelece a frequência com que uma palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo

Encriptação

Neste ponto, podes encriptar a memória interna do dispositivo, bem como a memória do cartão SD.

Exige encriptação do armazenamento	Se esta definição for activada, a memória do dispositivo será encriptada, desde que o dispositivo suporte esta funcionalidade. Depois de a memória do dispositivo ter sido encriptada pela primeira vez, já não é possível voltar a encriptá-la. Da mesma forma, a Política de Palavra-passe será automaticamente alterada para 6 símbolos alfanuméricos
Requer a encriptação do cartão SD	Esta definição só se aplica a dispositivos Samsung! Se esta definição estiver activada, o cartão SD externo pode ser encriptado e só pode ser desencriptado manualmente no dispositivo do utilizador final. Da mesma forma, a Política de Palavra-passe será automaticamente alterada para 6 símbolos alfanuméricos

AntiVírus

Ao ativar o AntiVirus, instala o Ikarus nos dispositivos. Tem em atenção que isto requer uma licença separada que pode ser introduzida em Definições gerais → Gestão de aplicações → Aplicações de terceiros.

Verificação automática	Define se o Ikarus efectua ou não uma análise automática e com que frequência a efectua Se ativar a opção "Verificação automática completa", efectua uma verificação completa. Caso contrário, efectua uma verificação rápida
Actualizações automáticas	Ativa as actualizações automáticas da base de dados de vírus e define a frequência com que isso acontece
Proteção de aplicações	Permite a verificação de aplicações para além da verificação normal, que apenas verifica ficheiros
Proteção do cartão SD	Ativa a proteção do cartão SD. Sem isso, a verificação fica limitada ao armazenamento local
Atualização apenas de Wi-Fi	Limita a atualização para Wi-Fi

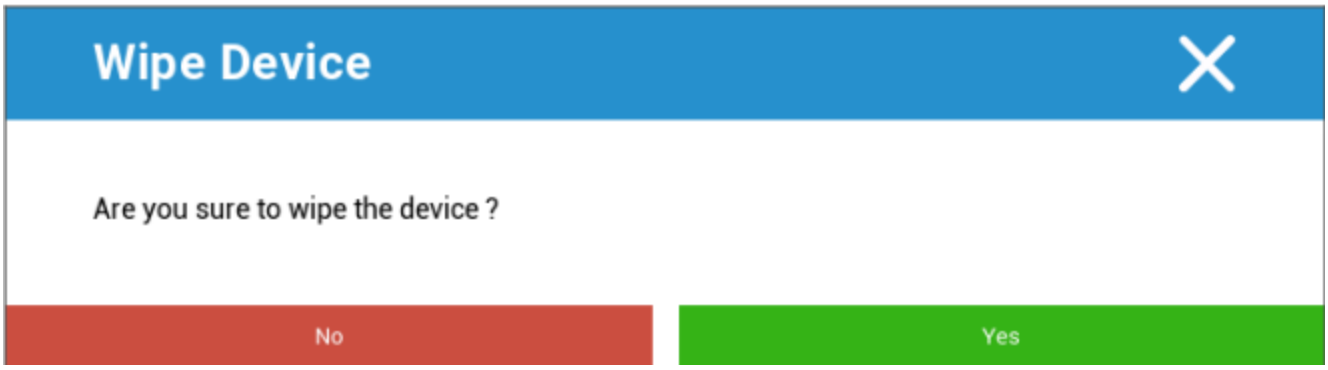
Fim de vida (apenas a nível do dispositivo)

Limpa (apenas ao nível do dispositivo)

Em "Limpar", podes restaurar o dispositivo para as definições de fábrica. Aqui, os dados empresariais, bem como os dados privados, serão eliminados no dispositivo do utilizador final.

Ao clicar no "Símbolo de Menos", deves receber a seguinte mensagem

Limpa também o cartão SD?	A memória do cartão SD também será apagada



Com "Sim" podes fazer a limpeza.

Em "Relatório de limpeza", podem ser apresentados os seguintes itens

Limpado por	Histórico de quem realizou a limpeza
Data	Data
Estado	Estado (por exemplo, se a limpeza foi efectuada com êxito)

Definições de restrições

Restrições

Aqui, é possível restringir e bloquear uma série de coisas.

Ativar a câmara	Permite a utilização da câmara
Forçar sincronização automática	Relaciona com a interface "Sync Ligado = a sincronização está permanentemente activada Desligado = a sincronização está permanentemente desactivada Escolha do utilizador = selecionado pelo utilizador
Forçar Bluetooth	Ligado = o Bluetooth está permanentemente ativado Desligado = Bluetooth está permanentemente desativado Escolha do utilizador = selecionado pelo utilizador
Forçar GPS	Ligado = o GPS está permanentemente ativado Desligado = o GPS está permanentemente desativado Escolha do utilizador = selecionado pelo utilizador
Forçar a precisão da localização do Google	Ligado = Localização permanente na Internet Desligado = Desativação permanente da localização na Internet Escolha do utilizador = selecionado pelo utilizador

Para os aparelhos Samsung com a interface KNOX 1.0 ou superior, estão disponíveis as seguintes opções de configuração.

Permitir cartão SD	Permitir cartão SD
Permite a escrita no cartão SD	Permite "escrever" no cartão SD
Permite a captura de ecrã	Permite a captura de ecrã
Permite a área de transferência	Permite a área de transferência
Faz a cópia de segurança das definições e dos dados da aplicação no Google Cloud	Desligado = desativar a Cópia de segurança do Google Ligado = ativa a Cópia de segurança do Google Escolha do utilizador = selecionado pelo utilizador
Permite a depuração USB	Permitir a depuração USB (é utilizado, por exemplo, para a criação de registos de dispositivos (ADB))
Permite o relatório de falhas do Google	Permite que o Relatório de falhas do Google seja enviado a partir das aplicações
Permite a reposição de fábrica	Permite ao utilizador restaurar o dispositivo para as definições de fábrica
Permite a atualização OTA	Permite actualizações "Over-The-Air
Permite o armazenamento no anfitrião USB	Se estiveres ativado, é possível ligar uma memória USB, sob a forma de um leitor de cartões HD ou SD
Permite o leitor multimédia USB (MTP, PTP)	Permite o leitor multimédia USB (MTP, PTP)
Permite o microfone	Ligado = permite o microfone para aplicações de terceiros Desligado = bloqueia o microfone para aplicações de terceiros Escolha do utilizador = os utilizadores podem selecionar, se a aplicação de terceiros tiver acesso ao microfone
Permite NFC (Near Field Communication)	Permitir NFC
Permitir fontes desconhecidas (APK Sideloading)	Se estiver ativado, permite o carregamento lateral de aplicações (ficheiros APK). Se esta definição estiver desactivada, o utilizador tem de a ativar manualmente quando permitires a instalação de APKs de fontes desconhecidas.
Permitir a criação de utilizadores	Permite a criação de vários utilizadores

Proprietário do dispositivo AE

(O dispositivo tem de estar no modo de proprietário do dispositivo Android Enterprise) Recomenda-se que cries os dispositivos como dispositivo "Android Enterprise" e não como dispositivo "Android".

Segurança	
Não permitir a localização da partilha	Especifica se um utilizador não está autorizado a ativar a partilha de local.
Não permitir o arranque seguro	Especifica se o utilizador não tem permissão para reiniciar o dispositivo no modo de arranque seguro.
Não permitir a reinicialização da rede	Especifica se um utilizador não está autorizado a repor as definições de rede a partir das Definições.
Não permitir a reposição de fábrica	Especifica se um utilizador não está autorizado a repor o dispositivo.
Ativar ADB	Permite a ligação a um PC através de ADB
Desativar o Keyguard	Desactiva o Keyguard
Proprietário do dispositivo Informações do ecrã de bloqueio	Define a informação do proprietário do dispositivo a ser mostrada no ecrã de bloqueio.
Aplicação da conformidade	Modo Avisar o utilizador - O utilizador será avisado para realizar as acções necessárias. Contentor de bloqueio de modo - Oculta todas as aplicações até que todos os requisitos sejam cumpridos

Gestão de aplicações	
Permitir ligações entre aplicações de perfil	Permite que as aplicações no perfil principal tratem de ligações Web a partir do perfil gerido.
Não permitir o controlo de aplicações	Especifica se um utilizador não está autorizado a modificar aplicações nas Definições ou nos lançadores.
Não permitir a instalação de aplicações	Especifica se um utilizador não está autorizado a instalar aplicações.
Não permitir a desinstalação de aplicações	Especifica se um utilizador não está autorizado a desinstalar aplicações.
Política de permissão de tempo de execução	Especifica como serão tratados os novos pedidos de permissão das aplicações.

Permitir fontes desconhecidas	Se estiver ativado, os utilizadores podem fazer o sideload de aplicações instalando um ficheiro .apk.

Conectividade	
Não permitir a configuração da rede móvel	Especifica se um utilizador não está autorizado a configurar redes móveis.
Desautoriza a configuração de Tethering	Especifica se um utilizador não está autorizado a configurar o Tethering e os hotspots portáteis.
Não permitir a configuração VPN	Especifica se um utilizador não está autorizado a configurar uma VPN.
Não permitir a configuração Wifi	Especifica se um utilizador não está autorizado a alterar os pontos de acesso WiFi.
Não permitir o feixe NFC de saída	Especifica se o utilizador não está autorizado a utilizar NFC para transmitir dados de aplicações.
Bloqueia a configuração WiFi	Esta definição controla se as configurações de WiFi criadas por uma aplicação Proprietário do dispositivo devem ser bloqueadas (ou seja, ser editáveis ou removíveis apenas pela aplicação Proprietário do dispositivo, nem mesmo pela aplicação Definições).
Ativar o roaming de dados	Ativa o Roaming de dados

Bluetooth	
Não permitir Bluetooth	Especifica se o bluetooth não é permitido no dispositivo. Necessita do Android 8.0
Não permitir a partilha Bluetooth	Especifica se a partilha Bluetooth de saída não é permitida no dispositivo. Necessita do Android 8.0
Não permitir a configuração Bluetooth	Especifica se um utilizador não está autorizado a configurar o Bluetooth.

Gestão de contas	
Não permitir a adição de perfil gerido	Especifica se um utilizador não está autorizado a adicionar perfis geridos. Necessita do Android 8.0
Não permitir a adição de utilizadores	Especifica se um utilizador não está autorizado a adicionar novos utilizadores.
Não permitir Remover perfil gerido	Especifica se os perfis geridos deste utilizador podem ser removidos, exceto pelo respetivo proprietário do perfil. Necessita do Android 8.0
Não permitir a modificação da conta	Especifica se um usuário não pode adicionar e remover contas, a menos que elas sejam adicionadas programaticamente pelo Authenticator.

Telefonia	
Não permitir chamadas de saída	Especifica que o utilizador não está autorizado a fazer chamadas telefónicas de saída.
Não permitir SMS	Especifica que o utilizador não está autorizado a enviar ou receber mensagens SMS.

Sistema	
Não permitir a criação de janelas	Especifica que as janelas para além das janelas da aplicação não devem ser criadas.
Não permitir definir o ícone do utilizador	Especifica se um utilizador não está autorizado a alterar o seu ícone.
Não permitir definir papel de parede	Restrição de utilizador para não permitir a definição de um papel de parede.
Desativar a barra de estado	A desativação da barra de estado bloqueia as notificações, as definições rápidas e outras sobreposições de ecrã que permitem escapar a um dispositivo de utilização única.
Ativar a hora automática	Define a hora automaticamente.
Ativar o fuso horário automático	Define o fuso horário automaticamente.
Mantém-se ligado enquanto estiver ligado à corrente	O dispositivo mantém-se ativo enquanto estiver ligado a uma fonte de alimentação.

Armazenamento

Não permitir a desativação da verificação da aplicação	Especifica se um utilizador não está autorizado a desativar a verificação da aplicação.
Não permite a montagem de suportes físicos	Especifica se um utilizador não está autorizado a montar suportes físicos externos.
Ativar o serviço de cópia de segurança	O serviço de cópia de segurança gere todos os mecanismos de cópia de segurança e de restauro no dispositivo. Se definir este valor como falso, impede a criação de cópias de segurança ou o restauro de dados. O serviço de cópia de segurança está desativado por predefinição. Necessita do Android 8.0
Ativar o armazenamento em massa USB	Ativa a utilização do armazenamento em massa USB.

Teclado	
Não permitir o preenchimento automático	Especifica se um utilizador não está autorizado a utilizar os serviços de preenchimento automático. Necessita do Android 8.0
Não permitir copiar e colar entre perfis	Especifica se o que é copiado na área de transferência deste perfil pode ser colado em perfis relacionados.

Som	
Não permitir o ajustamento do volume	Especifica se um utilizador não está autorizado a ajustar o volume principal.
Desativar o microfone	Especifica se um utilizador não está autorizado a ajustar o volume do microfone.
Silenciar dispositivo	Silencia o dispositivo.

Política de atualização do sistema	
Controla as actualizações do SO	Ativa esta opção para definir o comportamento de atualização como automático, em janelas ou adiado.

Contentor BYOD

Android Enterprise

Android Enterprise

Ativar o Android Enterprise	Ativa o Android Enterprise (AE). O AE é suportado desde o Android 5.1 e superior.
Aplicação da conformidade	Modo Avisar o utilizador - O utilizador será avisado para realizar as acções necessárias. Contentor de bloqueio de modo - Oculta todas as aplicações até que todos os requisitos sejam cumpridos
Política de permissão de tempo de execução	Avisa o utilizador para novos pedidos de autorização Concede sempre novos pedidos de autorização Recusa sempre novos pedidos de autorização Avisa: Algumas aplicações têm problemas em reconhecer as permissões se estas forem definidas automaticamente. Se concederes sempre permissões e tiveres problemas com aplicações que dizem que faltam permissões, define esta opção para "solicitar ao utilizador" e reinstala a aplicação
Permite a saída da área de transferência	Permite copiar e colar do interior do contentor para o exterior
Permite a resolução do identificador de chamadas	Mostra o nome de uma chamada recebida com base nos contactos do contentor
Permitir a resolução da pesquisa de contactos	Permite procurar nomes nos contactos do contentor ao fazer chamadas
Permitir a partilha de contactos Bluetooth	Permite o acesso ao contacto do contentor no automóvel
Não permitir o feixe NFC de saída	Desactiva o NFC para o contentor
Permitir fontes desconhecidas	Se estiver ativado, os utilizadores podem fazer o sideload de aplicações instalando um ficheiro .apk.
Permite a depuração USB	Se estiver ativado, os utilizadores podem ativar a Depuração USB.

Não permitir a modificação da conta	Não permite a criação, eliminação e modificação de contas no contentor Tem em atenção que algumas aplicações precisam de criar ou modificar contas para funcionarem como esperado

Gmail Exchange

Permite-te configurar o Gmail no Contentor. Tem em atenção que a ativação desta configuração não instala automaticamente a aplicação. Continua a ter de adicionar esta aplicação como aplicação obrigatória.

Endereço de e-mail	Endereço de e-mail
Nome de anfitrião do servidor	Nome de anfitrião do servidor
Nome de utilizador	Nome de utilizador
Assinatura	Assinatura
Número de dias anteriores a sincronizar	Número de dias anteriores a sincronizar.
Identificador do dispositivo	Identificador EAS. Mantém este campo vazio se o teu ambiente não o exigir
Utiliza Secure Sockets Layer (SSL)	Ativa a utilização de SSL. Desativar esta opção pode diminuir a segurança
Aceita todos os certificados	Aceita todos os certificados. A ativação desta opção pode diminuir a segurança
Permitir contas não geridas	Permite ao utilizador adicionar contas adicionais
Certificado de cliente	Carrega o certificado do cliente se o teu servidor Exchange o exigir

Aplicações do sistema AE

Aqui podes ativar as aplicações de sistema para o Android Enterprise Container. Tem em atenção que a aplicação especificada tem de estar no armazenamento do sistema, caso contrário não acontece nada.

Código de acesso do contentor

Apenas para Android 7.0 ou superior

Permite-te definir um requisito de palavra-passe específico para o contentor.

Comprimento mínimo da palavra-passe	Estabelece o número mínimo de símbolos que uma palavra-passe deve ter
Qualidade da palavra-passe	Força da palavra-passe Não especificado = não especificado Todas as palavras-passe são aceitáveis = todas as palavras-passe são aceitáveis pelo menos caracteres numéricos = deve conter pelo menos caracteres numéricos pelo menos caracteres complexos = deve conter pelo menos caracteres especiais at least alphanumerical characters = deve conter pelo menos caracteres alfanuméricos pelo menos caracteres alfabéticos = deve conter pelo menos caracteres alfabéticos
Bloqueio do tempo máximo de inatividade	Tempo máximo até o contentor ficar bloqueado. Configura apenas o valor máximo que pode ser selecionado pelo utilizador
Mínimo de letras minúsculas exigidas na palavra-passe	Mínimo de letras minúsculas exigidas na palavra-passe
Mínimo de letras maiúsculas exigidas na palavra-passe	Mínimo de letras maiúsculas exigidas na palavra-passe
Mínimo de caracteres não alfabéticos exigidos na palavra-passe	Mínimo de caracteres não alfabéticos exigidos na palavra-passe
Mínimo de dígitos numéricos exigidos na palavra-passe	Mínimo de dígitos numéricos exigidos na palavra-passe
Símbolos mínimos exigidos na palavra-passe	Símbolos mínimos exigidos na palavra-passe
Tempo limite de expiração da palavra-passe	Estabelece, após o que a palavra-passe expira e tem de ser emitida uma nova palavra-passe
Restrição do histórico de palavras-passe	Número de palavras-passe utilizadas anteriormente que não são permitidas
Máximo de tentativas falhadas da palavra-passe	Determina quantas vezes uma palavra-passe pode ser introduzida incorretamente, antes de o contentor ser eliminado

Samsung KNOX

Ativação

Aqui podes ativar o Samsung KNOX Container. Tem em atenção que esta funcionalidade já não é suportada pela Samsung no Android 10 ou superior. Utiliza o Android Enterprise Container no Android 10 ou superior

Código de acesso Knox

Estabelece as orientações relativas às definições da palavra-passe do aparelho

Comprimento mínimo da palavra-passe	Estabelece o número de símbolos que a palavra-passe deve ter
Qualidade da palavra-passe	Força da palavra-passe Todas as palavras-passe estão bem = Todas as palavras-passe estão bem Pelo menos caracteres numéricos = Deve existir um mínimo de caracteres numéricos Pelo menos caracteres complexos = Deve haver um mínimo de caracteres especiais Pelo menos caracteres alfanuméricos = Deve existir um mínimo de caracteres alfanuméricos Pelo menos caracteres alfabéticos = Deve existir um mínimo de caracteres alfabéticos
Mínimo de caracteres complexos necessários	Deve existir um mínimo de caracteres complexos
Tempo limite máximo de inatividade	Tempo máximo de inatividade do utilizador, antes do bloqueio do teclado
Permite a autenticação por impressão digital	Permite a autenticação por impressão digital
Permite a autenticação da íris	Permite a autenticação por reconhecimento da íris
Idade máxima da palavra-passe	Estabelece o tempo após o qual a senha expira e uma nova senha deve ser emitida
Histórico de senhas armazenadas	Número de palavras-passe anteriores que não são permitidas
Máximo de tentativas falhadas da palavra-passe	Estabelece o número de vezes que a palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo

Segurança Knox

Limita as funcionalidades específicas do dispositivo

Ativar a câmara	Permite a utilização da câmara
Permite a Samsung KNOX App Store	Permite a utilização da Samsung KNOX App Store
Permitir o Google Play Services	Permitir o Google Play Services
Permitir navegador	Permite a utilização do browser nativo
Permitir capturas de ecrã	Permite a criação de capturas de ecrã
Permitir a importação de contactos	Se estiver ativado, é permitido o acesso aos contactos do dispositivo a partir do contentor KNOX
Permitir a exportação de contactos	Se estiver ativado, é permitido o acesso aos contactos KNOX a partir do dispositivo
Permite a importação de calendários	Se estiver ativado, é permitido o acesso ao calendário do dispositivo a partir do contentor KNOX
Permitir a exportação do calendário	Se estiver ativado, é permitido o acesso ao calendário KNOX a partir do dispositivo
Permitir teclado não seguro	Permitir a utilização de um teclado não seguro
Ativar a importação de ficheiros	Ativar a importação de ficheiros para o contentor KNOX
Ativar a exportação de ficheiros	Ativar a exportação de ficheiros a partir do contentor KNOX

Bolsa de Valores de Knox

Aqui podes configurar o Exchange-Profile para o contentor KNOX

Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique em **Mostrar marcadores de posição**, podes visualizá-los para ti
Nome de anfitrião do servidor	Endereço do servidor dos teus Servidores Exchange
Nome de utilizador	O nome de utilizador (Login-Name) do respetivo dispositivo do utilizador final, tem também em atenção os "Placeholders" aqui
Domínio	Endereço do domínio
Palavra-passe (apenas ao nível do aparelho)	Opcionalmente, pode ser fornecida uma palavra-passe a um dispositivo individual; se esta estiver vazia, será pedido ao utilizador que introduza a sua palavra-passe do Exchange
Número de dias anteriores a sincronizar	Número de dias, determinando quando os e-mails são sincronizados de volta
Assinatura	Podes anexar uma assinatura
Conta por defeito	Estabelece que esta conta de e-mail é a conta padrão
Utiliza Secure Sockets Layer (SSL)	Utiliza uma ligação SSL
Utiliza a segurança da camada de transporte (TLS)	Utiliza uma ligação TLS
Aceita todos os certificados	Todos os certificados são aceites. Selecciona esta opção, se o teu Exchange Server utilizar um certificado auto-assinado

Knox eMail

Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique em **Mostrar marcadores de posição**, podes visualizá-los para ti
Protocolo do servidor de entrada	Protocolo do servidor de entrada IMAP ou POP
Endereço do servidor de entrada	Endereço do servidor de entrada
Porta do servidor de entrada	Porta do servidor de entrada
Nome de utilizador/login do servidor de entrada	Nome de utilizador/login do servidor de entrada
Palavra-passe do servidor de entrada	Palavra-passe do servidor de entrada
O servidor de entrada utiliza SSL	O servidor de entrada utiliza SSL
O servidor de entrada utiliza TLS	O servidor de entrada utiliza TLS
O servidor de entrada aceita todos os certificados	O servidor de entrada aceita todos os tipos de certificados
Protocolo do servidor de saída	Protocolo do servidor de saída SMTP
Porta do servidor de saída	Porta do servidor de saída
O servidor de saída utiliza credenciais adicionais	Credenciais adicionais para o servidor de saída. Se esta opção estiver definida como "off", serão utilizadas as definições do servidor de entrada
Nome de utilizador/login do servidor de saída	Nome de utilizador/login do servidor de saída
Palavra-passe do servidor de saída	Palavra-passe do servidor de saída
O servidor de saída utiliza SSL	O servidor de saída utiliza SSL

O servidor de saída utiliza TLS	O servidor de saída utiliza TLS
O servidor de saída aceita todos os certificados	O servidor de saída aceita todos os tipos de certificados
Assinatura	Aqui podes anexar uma assinatura
Notifica o utilizador quando recebe um novo e-mail	Notifica o utilizador quando recebe um novo e-mail

Aplicações Knox

Estabelece aqui as aplicações que pretendes distribuir pelos dispositivos dos utilizadores finais. Estes estarão então disponíveis no contentor KNOX. Para adicionar uma aplicação, procede como no menu Aplicações obrigatórias

Nome da aplicação	Nome da aplicação
Obrigatório Desde	Ponto no tempo, quando a aplicação foi adicionada
Fonte	Fonte da aplicação (Play Store | In-House)

Ao clicar no símbolo, a respectiva aplicação pode ser removida novamente

Gestão de ligações

Wifi

Para esta definição, efectua a pré-configuração dos dispositivos do utilizador final, para acesso aos pontos de acesso internos

Identificador do conjunto de serviços (SSID)	SSID da rede a ser conectada
Rede oculta	Ativar, no caso de o AP não transmitir o SSID
Tipo de segurança	Estabelece o tipo de segurança do PA

Tipo de segurança

WEP

Palavra-passe	Palavra-passe para o PA

WPA/WPA2

Palavra-passe	Palavra-passe para o PA

802.1x EAP

Método EAP	

PWD	Identidade	Identidade	
	Palavra-passe	Palavra-passe	

PEAP	Protocolo de autenticação de fase 2	nenhum	Nenhum protocolo adicional
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidade	Identidade	
	Identidade anónima	Identidade anónima	
	Palavra-passe	Palavra-passe	

Método EAP	

TTLS	Protocolo de autenticação de fase 2	nenhum	Nenhum protocolo adicional
		PAP	Protocolo PAP
		MSCHAP	Protocolo MSCHAP
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidade	Identidade	
	Identidade anónima	Identidade anónima	
	Palavra-passe	Palavra-passe	

TLS	Certificado CA	Certificado CA
	Identidade	Identidade
	Palavra-passe	Palavra-passe

VPN

Tipo de ligação	Estabelece o tipo de ligação VPN

Se seleccionares "VPN por aplicação" como tipo de VPN, os clientes VPN disponíveis serão alterados. A VPN por aplicação limita a VPN a determinadas aplicações e inicia a ligação VPN automaticamente se uma aplicação específica for iniciada.

Cliente VPN AppTec360	Usa o AppTec360 VPN Client em combinação com o Universal Gateway
Nome da ligação	Nome da ligação VPN
Configuração da porta de entrada	Selecciona a Configuração VPN do Universal Gateway
Sempre ligado à VPN	Força a VPN a estar sempre ativa, para que todo o tráfego passe pela VPN.
Ativar o bloqueio nativo	Bloqueia todas as redes quando o dispositivo não está ligado à VPN. Utiliza-o com cuidado, uma vez que pode provocar a perda total da ligação se não for configurado corretamente. Apenas para Android Enterprise no Android 7 ou superior
Ativar o bloqueio do AppTec360	Bloqueia a utilização de todas as aplicações até que a ligação VPN seja iniciada

Cisco AnyConnect	
Nome da ligação	Nome da ligação VPN
Servidor	Endereço do servidor
Modo de certificado	Desativado = desativado Automático = automático

L2TP (apenas KNOX)	Apenas disponível em dispositivos Samsung
Nome da ligação	Nome da ligação
Servidor	Endereço do servidor
Ativar o segredo L2TP	
Domínios de pesquisa DNS	Domínios de pesquisa DNS

Tipo de ligação	**Estabelece o tipo de ligação VPN**

PPTP (apenas KNOX)	Apenas disponível em dispositivos Samsung
Nome da ligação	Nome da ligação VPN
Servidor	Endereço do servidor
Ativar a encriptação	Ativar a encriptação
Domínios de pesquisa DNS	Domínios de pesquisa DNS

L2TP / IPSec PSK (apenas KNOX)	Apenas disponível em dispositivos Samsung
Nome da ligação	Nome da ligação VPN
Servidor	Endereço do servidor
Chave pré-partilhada IPSec	Chave pré-partilhada para autenticação
Ativar o segredo L2TP	
Segredo L2TP	
Domínios de pesquisa DNS	Domínios de pesquisa DNS

IPSec XAuth PSK (apenas KNOX)	Apenas disponível em dispositivos Samsung
Nome da ligação	Nome da ligação VPN
Servidor	Endereço do servidor
Identificador IPSec	Nome de utilizador para a ligação
Chave pré-partilhada IPSec	Palavra-passe para a ligação
Domínios de pesquisa DNS	Domínios de pesquisa DNS

OpenVPN	

Nome da ligação	Nome da ligação
Perfil OpenVPN	Aqui é onde o conteúdo do arquivo .ovpn será copiado
Aplicação OpenVPN	Existem duas aplicações diferentes para a utilização do OpenVPN Recomendamos-te a aplicação "OpenVPN para Android". Mas, em alternativa, podes utilizar a aplicação "OpenVPN Connect"

Restrições

Aqui podes definir as restrições, em relação à gestão da ligação.

Permitir roaming de dados	Permitir dados móveis em roaming
Forçar Roaming de Dados	Se estiver ativado, o roaming para dados móveis é permanentemente ativado (não recomendado!) Esta definição substitui a definição "Permitir Roaming de Dados"!
As seguintes definições só estão disponíveis no Samsung KNOX 2.0 ou superior	
Permitir apenas chamadas de emergência	Permitir apenas chamadas de emergência
Permitir WiFi	Permitir WiFi
Nível mínimo de segurança da rede WiFi	Nível mínimo de segurança da rede WiFi Aberto = todos os tipos de WiFi são permitidos
Proibir o utilizador de adicionar redes WiFi	O utilizador não pode adicionar ele próprio uma rede WiFi Esta definição só é possível se tiveres definido um perfil WiFi em "Gestão de ligações"
Permite SMS e MMS	Todos = Todo o tráfego SMS e MMS é permitido Apenas SMS de entrada = Apenas são permitidas mensagens SMS de entrada Apenas SMS de saída = Apenas são permitidas mensagens SMS de saída Nenhum = Não é permitido qualquer tráfego SMS / MMS
Permitir sincronização durante o roaming	Permitir sincronização durante o roaming Ligado = ativado Desligado = desativado Escolha do utilizador = escolha do utilizador
Permitir roaming de voz	Permitir roaming de voz Ligado = ativado Desligado = desativado Escolha do utilizador = escolha do utilizador
Utiliza o servidor proxy http do sistema	A utilização de um servidor proxy HTTP, que é fornecido pelas definições do sistema nas definições, depende da rede ligada (WiFi ou APN)

APN

As definições seguintes só estão disponíveis no Samsung SAFE 2.0 ou superior!

Nome de exibição do APN	Nome de exibição do APN	
Nome do ponto de acesso	Nome da APN	
Protocolo do servidor de saída	Não definido	
	Não tens	
	PAP	Protocolo PAP
	CHAP	Protocolo CHAP
	PAP ou CHAP	O protocolo PAP ou CHAP
MCC - Código de país móvel	O MCC é introduzido aqui, deixa este campo em branco, se for utilizado o MCC do cartão SIM inserido	
MNC - Código de Rede Móvel	O MNC é introduzido aqui, deixa este campo em branco, se for utilizado o MCC do cartão SIM inserido	
Endereço do servidor	Endereço do servidor	
Número da porta do servidor	Número da porta do servidor	
Endereço do servidor proxy	Endereço do servidor proxy	
Endereço do servidor MMS	Endereço do servidor MMS, para Standard deixa em branco	
Número da porta MMS	Número da porta MMS	
Endereço proxy MMS	Endereço proxy MMS	
Nome do utilizador	Nome do utilizador	
Palavra-passe	Palavra-passe	
Tipo de ponto de acesso	Os tipos permitidos são: "default", "mms", "supl" Se este campo for deixado em branco, serão utilizados "default,supl,mms".	
APN preferida	Dá preferência à APN	

Bluetooth

Aqui, podes efetuar uma variedade de definições Bluetooth.

As seguintes definições só estão disponíveis no Samsung KNOX 1.0 ou superior!

Permite a descoberta de dispositivos via Bluetooth	Permite a descoberta de dispositivos através de Bluetooth
Permitir o emparelhamento Bluetooth	Permite o emparelhamento Bluetooth
Permitir dispositivos com auscultadores Bluetooth	Permitir dispositivos com auscultadores Bluetooth
Permite dispositivos mãos-livres Bluetooth	Permite dispositivos mãos-livres Bluetooth
Permite dispositivos Bluetooth A2DP	Permite a transmissão de áudio Bluetooth A2DP entre dispositivos
Permitir chamadas efectuadas	Permite a realização de chamadas viaBT
Permite a transferência de dados via Bluetooth	Permite a transferência de dados através de Bluetooth
Permite o Bluetooth Tethering	Permite utilizar o dispositivo como um modem (ligação Bluetooth à Internet)
Permite a ligação ao computador através de Bluetooth	Permite a ligação ao computador através de Bluetooth

Gestão PIM

Troca

Apenas disponível para Samsung KNOX 1.0 ou superior!

Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique em **Mostrar marcadores de posição**, podes visualizá-los para ti
Nome de anfitrião do servidor	Endereço do servidor dos teus Servidores Exchange
Nome de utilizador	O nome de utilizador (Login-Name) do respetivo dispositivo do utilizador final, tem também em atenção os "Placeholders here
Domínio	Endereço do domínio
Palavra-passe (apenas ao nível do aparelho)	Opcionalmente, pode ser fornecida uma palavra-passe a um dispositivo individual; se esta estiver vazia, será pedido ao utilizador que introduza a sua palavra-passe do Exchange
Número de dias anteriores a sincronizar	Número de dias, determinando quando os e-mails são sincronizados de volta
Assinatura	Podes anexar uma assinatura (Dica: alguns dispositivos exigem formatação HTML para a assinatura)
Conta por defeito	Estabelece que esta conta de correio é a conta padrão
Utiliza Secure Sockets Layer (SSL)	Utiliza uma ligação SSL
Utiliza a segurança da camada de transporte (TLS)	Utiliza uma ligação TLS
Aceita todos os certificados	Todos os certificados são aceites. Selecciona esta opção, se o teu Exchange Server utilizar um certificado auto-assinado

eMail

Aqui, podes distribuir contas IMAP e POP pelos respectivos dispositivos do utilizador final.

As seguintes definições só estão disponíveis no Samsung KNOX 1.0 ou superior!		
Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique em **Mostrar marcadores de posição**, podes visualizá-los para ti	
Protocolo do servidor de entrada	Protocolo do servidor de entrada	IMAP ou POP
Endereço do servidor de entrada	Endereço do servidor de entrada	
Porta do servidor de entrada	Porta do servidor de entrada	
Nome de utilizador/login do servidor de entrada	Nome de utilizador/login do servidor de entrada	
Palavra-passe do servidor de entrada (apenas ao nível do dispositivo)	Palavra-passe do servidor de entrada (apenas ao nível do dispositivo)	
O servidor de entrada utiliza SSL	O servidor de entrada utiliza SSL	
O servidor de entrada utiliza TLS	O servidor de entrada utiliza TLS	
O servidor de entrada aceita todos os certificados	O servidor de entrada aceita todos os tipos de certificados	
Protocolo do servidor de saída	Protocolo do servidor de saída	SMTP
Porta do servidor de saída	Porta do servidor de saída	
O servidor de saída utiliza credenciais adicionais	Credenciais adicionais para o servidor de saída. Se esta opção estiver definida como "off", serão utilizadas as definições do servidor de entrada	
Nome de utilizador/login do servidor de saída	Nome de utilizador/login do servidor de saída	
Palavra-passe do servidor de saída (apenas ao nível do dispositivo)	Palavra-passe do servidor de saída	
O servidor de saída utiliza SSL	O servidor de saída utiliza SSL	
O servidor de saída utiliza TLS	O servidor de saída utiliza TLS	

O servidor de saída aceita todos os certificados	O servidor de saída aceita todos os tipos de certificados
Assinatura	Podes anexar uma assinatura aqui (Dica: alguns dispositivos exigem formatação HTML para a assinatura)
Notifica o utilizador quando recebe um novo e-mail	Notifica o utilizador quando recebe um novo e-mail

AE Gmail Exchange

Informação: Esta Configuração será aplicada à aplicação Gmail. Por isso, tens de aprovar e instalar o Gmail.

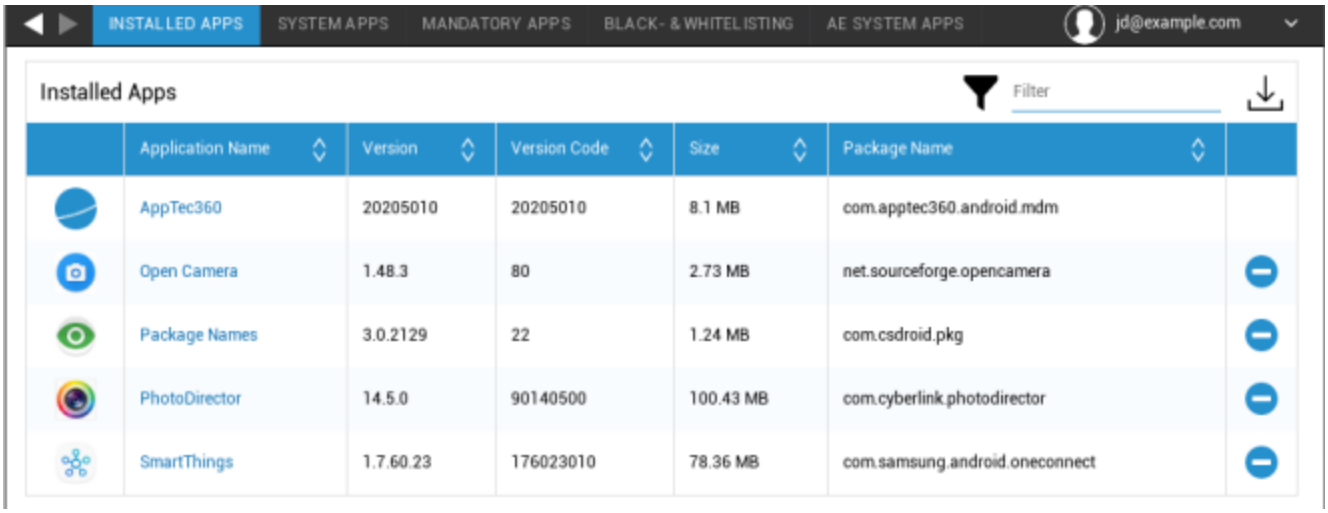
Endereço de correio eletrónico	O endereço de correio eletrónico do utilizador fornecido Tem em atenção os "marcadores de posição", que podes utilizar para trabalhar com credenciais e não realizar alterações manualmente em cada dispositivo Com um clique em Mostrar marcadores de posição, podes visualizá-los para ti
Nome de anfitrião do servidor	Endereço do servidor dos teus Servidores Exchange
Nome de utilizador	O nome de utilizador (Login-Name) do respetivo dispositivo do utilizador final, tem também em atenção os "Placeholders here
Assinatura	Podes anexar uma assinatura (Dica: alguns dispositivos exigem formatação HTML para a assinatura)
Número de dias anteriores a sincronizar	Número de dias, determinando quando os e-mails são sincronizados de volta
Identificador do dispositivo	Identificador EAS. Mantém este campo vazio se o teu ambiente não o exigir
Utiliza Secure Sockets Layer (SSL)	Utiliza uma ligação SSL
Aceita todos os certificados	Todos os certificados são aceites. Selecciona esta opção, se o teu Exchange Server utilizar um certificado auto-assinado
Permitir contas não geridas	Permite ao utilizador adicionar contas adicionais
Certificado de cliente	Carrega o certificado do cliente se o teu servidor Exchange o exigir

Gestão de aplicações

Gestor de aplicações empresariais

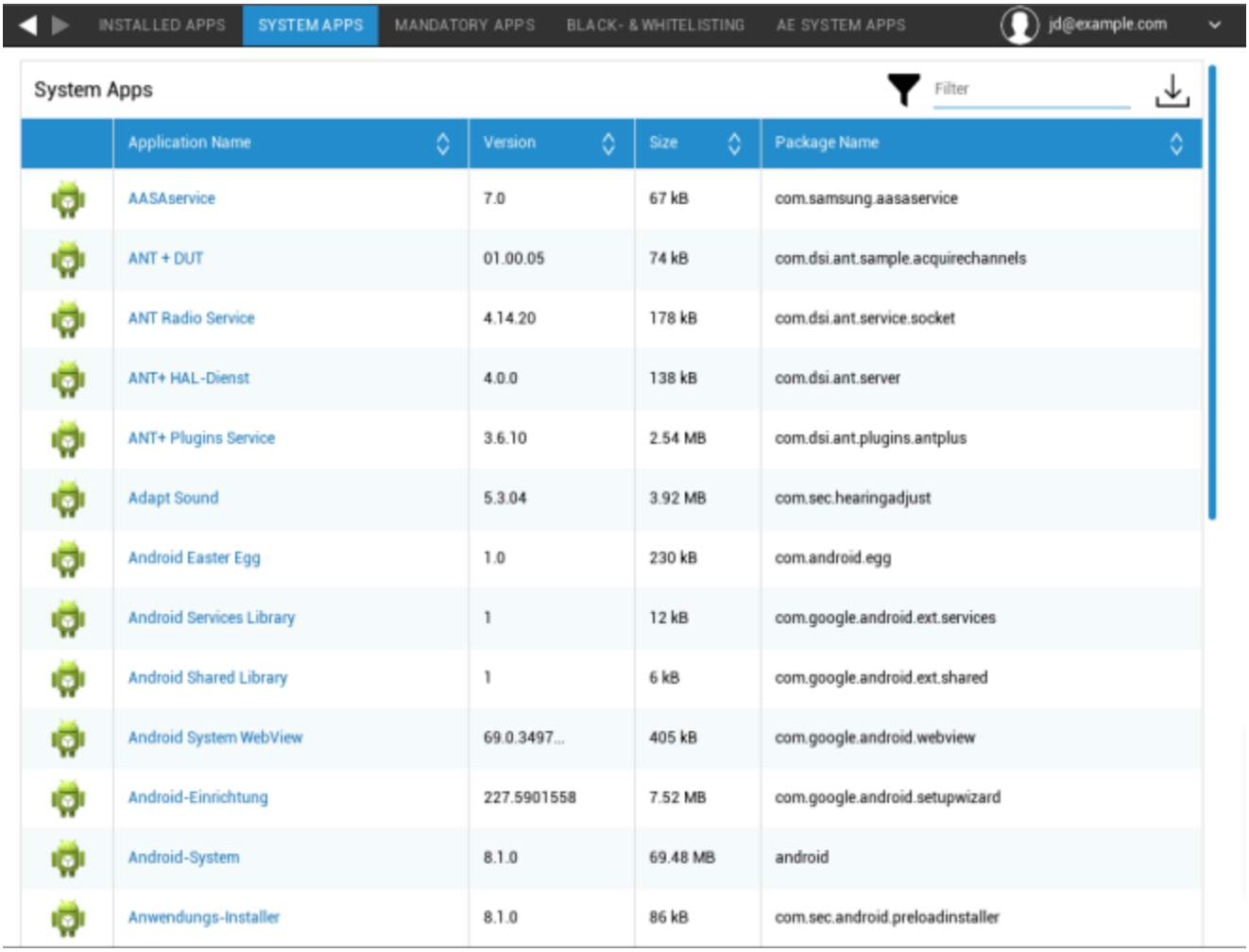
Aplicações instaladas (apenas ao nível do dispositivo)

Aqui ser-te-ão apresentadas todas as aplicações que estão atualmente instaladas no dispositivo do utilizador final.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

Aplicações de sistema (apenas ao nível do dispositivo)

Em "System Apps" (Aplicações do sistema), todos os sistemas pré-instalados serão listados com o nome do pacote e a versão.



Aplicações obrigatórias

Em Aplicações obrigatórias, podes definir as aplicações que têm de ser instaladas no dispositivo. Dependendo da tua configuração e do teu dispositivo, a aplicação será instalada automaticamente ou será pedido ao utilizador que a instale.

Tem em atenção que é recomendada a utilização do Android Enterprise para facilitar a gestão das aplicações.

Os cenários são os seguintes:

Aplicações normais da Play Store

As instalações de aplicações da Playstore necessitam sempre de uma interação do utilizador. Além disso, tem de ser configurada uma Conta Google no dispositivo.

Instalação da aplicação interna

Nos dispositivos Samsung, estas aplicações serão instaladas silenciosamente. A única exceção é o contentor, onde o utilizador tem de confirmar a instalação.

Em qualquer outro cenário, o utilizador tem de confirmar a instalação da aplicação.

Android Empresa Play Store Apps

Estas aplicações serão sempre instaladas silenciosamente, sem interação do utilizador.

Para adicionar uma aplicação obrigatória, clica no "+" e selecciona a aplicação pretendida na lista. Tem em atenção que não podes instalar aplicações a partir do separador "Google Play Store", se o dispositivo estiver configurado com o Android Enterprise como totalmente gerido ou como contentor.

Se utilizares o Android Enterprise, selecciona as aplicações na secção "AE Play Store". Para tornar as aplicações disponíveis aqui, confirma-as na loja Google Enterprise Play, indo a Definições gerais → AE Play Store → Aplicações da Play Store.

Ao remover uma aplicação obrigatória, esta também será desinstalada do dispositivo.

Podes clicar no nome de uma aplicação na lista de aplicações obrigatórias e ir para o separador "configuração" para configurar uma aplicação. Para tal, é necessário utilizar o Android Enterprise e a aplicação tem de o suportar. Por conseguinte, as opções disponíveis dependem da aplicação selecionada.

Aplicações do sistema AE

Aqui podes ativar as aplicações de sistema para os dispositivos Android Enterprise. Tem em atenção que a aplicação especificada tem de estar no armazenamento do sistema, caso contrário não acontece nada. 296

Restrições e definições

Lista negra e lista branca

Aqui podes definir uma lista negra ou uma lista branca. Todas as aplicações da lista negra serão bloqueadas. Todas as aplicações que não estejam na lista branca serão bloqueadas. Uma lista negra vazia não bloqueia nada, enquanto uma lista branca vazia bloqueia tudo*

**Todas as aplicações obrigatórias e aplicações da Enterprise App Store serão colocadas automaticamente na lista branca. Não precisas de os adicionar manualmente*

Ao clicares no "+", podes procurar uma aplicação que queiras adicionar à tua lista negra ou branca ou introduzir um nome de pacote manualmente.

Restrições da aplicação de sistema

Em "Sys App Restrictions" podes, entre outras coisas, bloquear aplicações e serviços pré-instalados, como desejares.

Desativar o navegador	Desativar o browser padrão
Desativar o calendário	Desativar o calendário nativo
Desativar a calculadora	Desativar a calculadora
Desativar o navegador Chrome	Desativar o navegador Chrome
Desativar relógio	Desativar o relógio
Desativar contactos	Desativar contactos
Desativar o marcador	Desativar o marcador nativo
Desativar o eMail	Desativar o correio eletrónico
Desativar o Exchange	Desativar contas do Exchange
Desativar o Facebook	Desativar a aplicação do Facebook
Desativar a Galeria	Desativar a aplicação nativa da galeria
Desativar o Gmail	Desativar o Gmail
Desativar a Pesquisa de livros do Google	Desativar a Pesquisa de livros do Google
Desativar o Google Play Kiosk	Desativar o Google Play Kiosk
Desativar o Google Maps	Desativar o Google Maps
Desativar o Google Music	Desativar o Google Music
Desativar o Google Filmes	Desativar o Google Filmes
Desativar a Google Play Store	Desativar a Google Play Store (App Store pública)
Desativar o Google Plus	Desativar o Google Plus
Desativar a Pesquisa Google	Desativar a Pesquisa Google
Desativar o Google Talk / Google Hangouts	Desativar o Google Talk / Google Hangouts
Desativar o leitor de música	Desativar a aplicação nativa do leitor de música
Desativar definições	Desativar as definições do dispositivo
Desativar o Sim Toolkit	Desativar os serviços do Sim Toolkit
Desativar SMS / MMS	Desativar SMS / MMS
Desativar o Street View	Desativar os serviços do Street View
Desativar o Youtube	Desativar o Youtube

Samsung Apps

Em "Samsung Apps", podes definir definições e/ou restrições adicionais para dispositivos Samsung.

Desativar o AllShare Play / Samsung Link	Desativar o AllShare Play / Samsung Link
Desativar o ChatON	Desativar o ChatON
Desativar o Game Hub	Desativar o Game Hub
Desativar o jogo em grupo	Desativar o jogo em grupo
Desativar ajuda	Desativar a Ajuda da Samsung
Desativar o KNOX	Desativar o contentor Samsung KNOX
Desativar memorando	Desativar o Memo de voz
Desativar os meus ficheiros	Desativar os meus ficheiros
Desativar o leitor ótico	Desativar o leitor ótico
Desativar o Polaris Office	Desativar o Polaris Office
Desativar o Readers Hub / Samsung Books	Desativar o Readers Hub / Samsung Books
Desativar o S Memo	Desativar a aplicação Samsung Memo
Desativar o S Translator	Desativar a aplicação Samsung Translator
Desativar a voz S	Desativar o assistente de voz S
Desativar as aplicações da Samsung	Desativar a Samsung App Store
Desativar o Samsung Hub	Desativar a Samsung Entertainment Stores
Desativar o leitor de vídeo	Desativar o leitor de vídeo
Desativar o gravador de voz	Desativar o gravador de voz
Desativar o WatchON	Desativar WatchON (simula um controlo remoto)

Aplicações Huawei

Em "Aplicações Huawei", podes definir definições e/ou restrições adicionais no dispositivo Huawei.

Desativar DLNA	Desativar DLNA
Desativar o instalador de aplicações	Desativar o instalador de aplicações
Desativar o Gestor de Ficheiros	Desativar o Gestor de Ficheiros
Desativar o Gestor de Cópias de Segurança	Desativar o Gestor de Cópias de Segurança
Desativar o atualizador do sistema	Desativar o atualizador do sistema
Desativar a caixa de ferramentas	Desativar a caixa de ferramentas
Desativar o tempo	Desativar o tempo
Desativar o rádio FM	Desativar o rádio FM

Definições de gestão de aplicações

Aqui podes definir o comportamento de atualização das aplicações internas.

Update Check Frequency define a frequência com que a AppTec360 App procura actualizações para as aplicações InHouse. Assim que for detectada uma nova versão, esta será transferida e instalada.

O Limite de Wi-Fi define se o download deve ser limitado a ligações Wi-Fi se a aplicação for maior do que o teu Limite configurado. Se o for menor ou não definires um limite, a aplicação será descarregada em Wi-Fi e numa rede celular.

Loja de aplicações para empresas

Tem em atenção que o facto de as aplicações serem adicionadas aqui (Enterprise App Store) NÃO fará com que sejam instaladas automaticamente no(s) dispositivo(s). O utilizador tem de abrir a Enterprise App Store no dispositivo e instalar a aplicação manualmente.

Se quiseres instalar automaticamente aplicações no dispositivo, vai a "Gestão de aplicações" → "Gestor de aplicações empresariais" → "Aplicações obrigatórias" e adiciona aí as aplicações pretendidas.

Neste ponto, podes distribuir aplicações opcionais aos teus utilizadores.

Playstore

Clica no "+" para adicionar uma aplicação da Play Store à loja. Se utilizares o Android Enterprise, acede a "App Management Enterprise Play Store". Tem também em atenção que tem de ser configurada uma Conta Google no → dispositivo para instalar as aplicações aqui definidas.

Internamente

No ponto "In-House", podes carregar e distribuir aplicações desenvolvidas internamente.

Clica no "+" para adicionar uma aplicação InHouse à loja de aplicações da empresa, que pode depois ser instalada pelo utilizador. Nesta caixa de diálogo, também podes carregar uma nova aplicação InHouse.

Empresa Play Store

Tem em atenção que o facto de adicionares aplicações aqui (Enterprise Play Store) NÃO fará com que sejam instaladas automaticamente no(s) dispositivo(s). O utilizador tem de abrir a Play Store no dispositivo e instalar a aplicação manualmente.

Se quiseres instalar automaticamente aplicações no dispositivo, vai a "Gestão de aplicações" → "Gestor de aplicações empresariais" → "Aplicações obrigatórias" e adiciona aí as aplicações pretendidas.

Neste ponto, podes distribuir aplicações opcionais aos teus utilizadores.

Aqui podes adicionar aplicações à Android Enterprise Playstore. Tem em atenção que tens de aprovar as aplicações em Definições gerais → AE Play Store → Aplicações da Play Store. Estas aplicações serão adicionadas à Google Play Store normal.

Tem também em atenção que, primeiro, tens de definir um esquema com aplicações em Definições gerais → Gestão de aplicações → AE Play Store → Esquema da loja.

As aplicações têm de estar num Layout antes de as poderes adicionar com êxito à loja.

Modo de quiosque e lançador

Modo quiosque

O Modo Quiosque permite-te predefinir uma aplicação ou um URL. Então, será exclusivamente possível executar/visitar esta aplicação e/ou URL.

Da mesma forma, vários botões de hardware podem ser desactivados no Modo Quiosque.

Início automático	Inicia automaticamente o Modo Quiosque, assim que o perfil chega ao dispositivo do utilizador final
Modo de quiosque programado?	Podes planear um horário para o Modo Quiosque, que começará e terminará automaticamente, a uma hora definida por ti
Hora de início	Hora de início
Tempo em minutos	Tempo em minutos, após o qual o Modo Quiosque deve terminar novamente

Tipo de aplicação

Aplicação única	Se quiseres iniciar a aplicação no modo Quiosque, selecciona Pacote" em "Tipo de aplicação"
Aplicação de quiosque	Clica aqui para selecionar uma aplicação que deve ser iniciada no modo de quiosque Encontrarás a visão geral habitual da Gestão de aplicações Podes selecionar entre "Google Play Store", "Android In-House Apps" e "Packagename"

Tipo de aplicação

URL	Se quiseres lançar um URL no modo de quiosque, selecciona "URL" em "Tipo de aplicação" Em seguida, define o endereço URL pretendido
Limpa o browser após inatividade	Aqui podes definir um intervalo de tempo em minutos, após o qual o Modo Quiosque deve ser relançado
Limpar a cache da Web e os cookies	Se activares esta função, depois de reiniciar o Modo Quiosque, a Cache Web (cookies e imagens em cache) será apagada
Política de mesma origem	Se esta função estiver ativa, o utilizador só pode navegar nas subpáginas de um URL definido Por exemplo, definiste o seguinte URL:www.mypage.com Depois, o utilizador pode navegar em: www.mypage.com/subpage
URLs na lista branca	Aqui podes manter uma Whitelist, todos estes URLs são permitidos Máximo de 1 URL por linha Um URL deve começar por http:/ ou https://
URLs na lista negra	Aqui podes manter uma lista negra, todos estes URLs não são permitidos Máximo de 1 URL por linha Um URL deve começar por http:/ ou https://
Orientação do ecrã	Esta definição está relacionada com os ajustes do ecrã Automático = automático Retrato = formato vertical Paisagem = modo paisagem

Multi App	Se seleccionares o modo de quiosque "Multi App", a utilização do AppTec360 Launcher será obrigatória.
Aplicações	Aplicação: Selecciona uma aplicação da Playstore ou uma aplicação interna como aplicação do quiosque. Também é possível introduzir um nome de pacote. A aplicação de quiosque selecionada tem de estar instalada no dispositivo. Não te esqueças de definir a aplicação Kiosk como obrigatória. Atalho no ecrã inicial: Se estiver definido para "Ligado", será criado um atalho no ecrã inicial. Se estiveres definido como "Desligado", a aplicação continua a aparecer na lista de aplicações.

Senha de saída activada	Se activares esta função, o utilizador pode terminar o modo de quiosque com uma palavra-passe predefinida por ti
Sair da palavra-passe	Esta é a palavra-passe, que foi predefinida por ti
Recolha automática da barra de estado	Se estiver ativado, a barra de estado será automaticamente colada. Com esta opção, os utilizadores podem ver as informações na barra de estado, mas não podem aceder às suas funções
Desativar a barra de estado	A barra de estado contém notificações, atalhos e informações. Apenas disponível para dispositivos Samsung com KNOX 1.0 ou superior.
Desativar as teclas de volume	Desativar as teclas de volume (apenas disponível em dispositivos Samsung com KNOX 1.0 ou superior)
Desativar o interrutor de ligar/desligar	Desativar o interrutor ligar/desligar (apenas disponível em dispositivos Samsung com KNOX 1.0 ou superior)
Desativar o botão Home	Desativar o botão Início. Se esta função estiver activada, então o Modo Quiosque só pode ser terminado na Consola AppTec360 (apenas disponível em dispositivos Samsung com KNOX 1.0 ou superior)
Desativar a barra de navegação	Com esta opção, podes desativar a barra de navegação (Voltar / Menu) Se esta função estiver activada, então o Modo Quiosque só pode ser terminado na Consola AppTec360 (apenas disponível em dispositivos Samsung com KNOX 1.0 ou superior)

Definições de atualização da aplicação	
Permitir actualizações de aplicações	Os utilizadores serão convidados a efetuar actualizações de aplicações mesmo quando o Modo Quiosque está ativo. Nos dispositivos com Samsung KNOX, as aplicações serão actualizadas silenciosamente.
Janela Atualizar	Define um intervalo em que os utilizadores serão solicitados a instalar actualizações de aplicações.

TeamViewer	
Ativar o acesso não assistido	Se estiver ativado, os administradores podem controlar remotamente o dispositivo sem a interação do utilizador. A aplicação TeamViewer Host tem de ser instalada no dispositivo.

Lançador AppTec360

Ativar o AppTec360 Launcher	Liga: Ativa o AppTec360 Launcher. O utilizador tem de o definir como Launcher predefinido uma vez. Nota: Se o Modo Quiosque estiver ativado e o Modo Quiosque estiver definido para "Multi-Apps", a utilização do lançador AppTec360 será obrigatória.
Ícones grandes	Liga: Mostra uma versão maior dos ícones de aplicações no Launcher
Ocultar o ícone da AppTec360	Liga: Oculta completamente a aplicação AppTec360
Ocultar o ícone da AppTec360 Store	Ativa: Oculta completamente a AppTec360 Enterprise AppStore

Definições da AppTec360

Ativar a aplicação AppTec360 Settings	A aplicação de definições AppTec360 permite controlar as ligações WiFi e Bluetooth
Ativar as definições em Multi-Apps Modo quiosque	Se estiver ativado, os utilizadores podem aceder à AppTec360 Settings App enquanto o Multi App Kiosk Mode estiver ativo

Controlo remoto

Splashtop

Mostra o estado atual da Configuração do Splashtop. Aqui verás os passos a seguir para acederes remotamente ao dispositivo através do Splashtop. Aqui também tens de introduzir o teu código de utilização, que podes obter no sítio Web do Splashtop. O código de implementação é necessário para te ligares ao dispositivo.

Teamviewer

Mostra o estado atual da Configuração do Teamviewer. Aqui verás os passos a seguir para acederes remotamente ao dispositivo através do Teamviewer.

Gestão de conteúdos

Caixa de conteúdo

Aqui podes ativar a Contentbox para este dispositivo. Uma vez activada, a aplicação Contentbox será instalada no dispositivo.

Navegador seguro

Aqui podes ativar o Secure Browser para este dispositivo. Uma vez activada, a aplicação Secure Browser será instalada no dispositivo. Este Browser pode ser configurado para oferecer um Web Browser no dispositivo que é limitado às tuas necessidades.

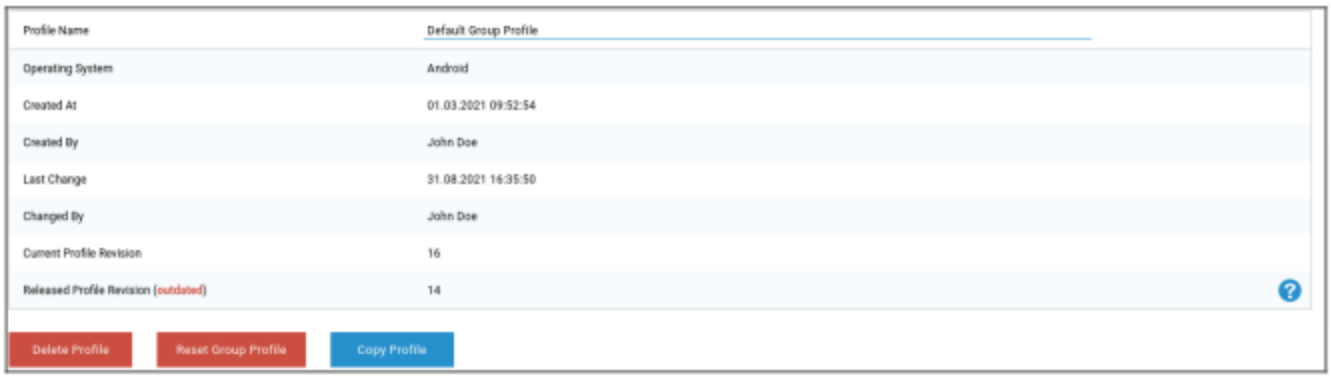
Requerer palavra-passe	Exige que o utilizador defina e utilize uma palavra-passe para aceder ao browser.
Restringir transferências / Abrir em	Bloqueia downloads de sites
Restringir carregamentos	Restringe os Uploads a determinados URLs. Não forneça nenhum URL para bloquear totalmente o Upload
Permitir cópia	Permite copiar, cortar ou partilhar texto dentro das páginas Web.
Permite a captura de ecrã	Permite a captura de imagens de ecrã.
Frequência da limpeza de dados	Selecciona com que frequência TODOS os dados do utilizador (histórico, cache, etc.) devem ser automaticamente removidos.
Marcadores da empresa	Os marcadores aparecerão na pasta "Marcadores da empresa" nos marcadores do navegador. Não são editáveis pelo utilizador.
Ocultar a barra de endereços	Oculta a barra de endereços para que o utilizador não veja o URL que está a visitar
Lista branca no navegador (sem Universal Gateway)	Ativa a lista branca de URLs do lado do cliente. - Os marcadores da empresa são sempre colocados na lista branca - Suportado apenas para 100 URLs - Utiliza o Universal Gateway para uma lista negra e branca ilimitada
Lista negra e lista branca baseadas em gateway	A lista negra tem os seguintes requisitos: - Uma configuração VPN em funcionamento com um servidor DNS especificado ("Definições gerais" → "Gateway universal" → "Definições VPN") - Uma configuração de lista negra ("Definições gerais" → "Gateway universal" → "Definições VPN") - Uma configuração de lista negra ("Definições gerais" → "Gateway universal" → "Lista negra de domínios") - Uma ligação VPN válida no perfil ("Gestão de ligações" → "VPN")

Configuração do PC com Windows 10

Geral

Síntese do perfil do grupo (apenas a nível do grupo)

Ao abrires um perfil de grupo, terás uma visão geral rápida do perfil.



Nome do perfil	Nome do perfil (pode ser alterado aqui)
Sistema operativo	Sistema operativo para o qual o perfil se destina
Criado em	Tempo de criação
Criado por	O criador do perfil
Última alteração	Hora da última modificação do perfil
Alterado por	Conta que efectuou as últimas alterações
Revisão do perfil atual	Revisão do estado do perfil guardado
Revisão do perfil lançado	Revisão do perfil atribuído ("Atribuir agora"). Se a etiqueta apresentar " (desatualizado)" por trás do texto, significa que guardaste o perfil mas ainda não o atribuíste, pelo que os dispositivos continuarão a receber uma versão mais antiga.

Síntese do dispositivo (apenas ao nível do dispositivo)

A síntese resumida do aparelho, que contém o seguinte:

Nome do PC	Nome do PC
Cliente	Os dispositivos do tipo Windows
Última localização conhecida	A latitude e longitude da última localização conhecida do dispositivo
Atribuição de aplicações obrigatórias	Número de aplicações obrigatórias atribuídas ao dispositivo
PC UID	UID do PC
Edição OS	Mostra a tua Windows Edition
Versão do SO	Versão do Windows atualmente instalada
Construção do SO	Compilação atual do Windows
Sistema operativo	Sistema operativo atualmente instalado
Número de série	Número de série do dispositivo
Propriedade do dispositivo	O tipo de propriedade configurado
Tipo de dispositivo	O tipo do dispositivo
Enraizado	Mostra se o dispositivo está enraizado
Conformidade	Mostra se o dispositivo é compatível
Visto pela última vez	Data e hora em que foram efectuadas alterações no perfil
Atribuição de utilizadores	Apresenta o utilizador ou grupo a que este dispositivo está atualmente atribuído. Podes mover o dispositivo seleccionando um utilizador ou grupo diferente na lista pendente.

Definições

Permitir atualização automática	Permite ou não permitir actualizações automáticas do sistema operativo.

Config Revision (apenas a nível do dispositivo)

Aqui tens uma visão geral do perfil de grupo que está atribuído ao aparelho.

Se clicares no perfil de grupo, acederás diretamente ao perfil e poderás efetuar definições.

Com o símbolo, podes reverter as aplicações atribuídas para as definições do perfil de grupo.

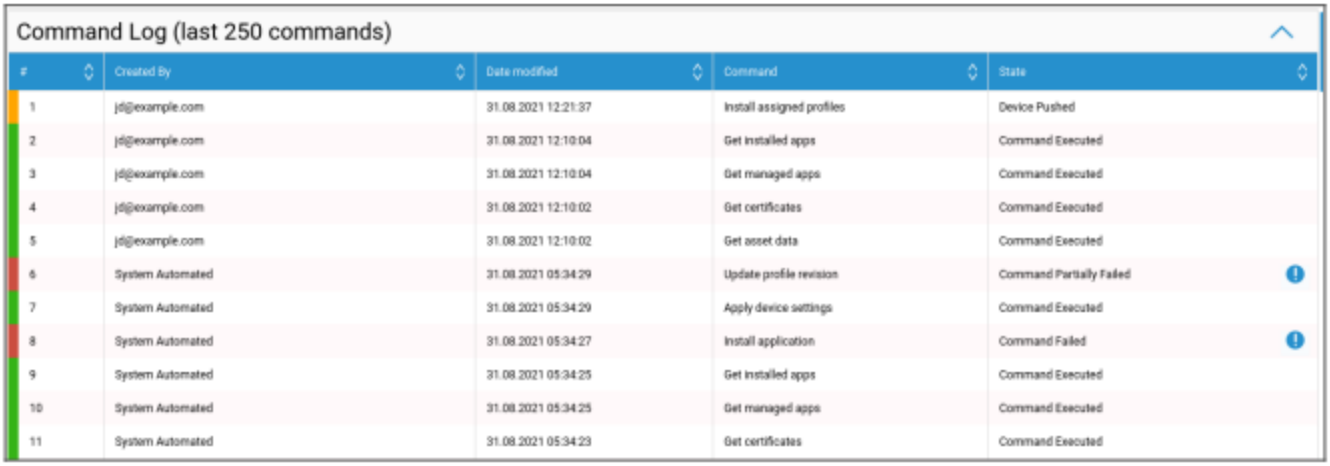
Com o símbolo, podes repor o perfil do dispositivo para que não tenha quaisquer definições.

"Newer Revision available" indica que o perfil de grupo foi alterado e guardado, mas não atribuído. O perfil de grupo tem de ser atribuído com "Atribuir agora" ao nível do grupo para aplicar as alterações aos dispositivos.

Registo do dispositivo (apenas ao nível do dispositivo)

Registo de comandos

Aqui podes ver quais os comandos que foram emitidos para o dispositivo e qual o seu estado.



Os comandos criados por "Sistema automatizado" são automaticamente criados pelo sistema.

Status de comando possíveis

Dispositivo empurrado	Foi enviado um pedido push para o serviço push (por exemplo, APNS) para dizer ao dispositivo para se ligar novamente ao servidor EMM.
Comando criado	O comando foi criado no sistema.
Comando enviado	O comando foi enviado para o dispositivo depois de este se ter ligado ao servidor.
Comando Executado	O comando foi executado com sucesso.
Falha no comando	O comando falhou. *
Comando parcialmente falhado	Dependendo do sistema operativo do dispositivo, alguns comandos podem ser agrupados. Neste caso, algumas partes deste grupo de comandos falharam. *
Comando executado, eventualmente falhou	O comando foi executado, mas talvez não o tenha sido.
Comando repuxado	O comando foi reenviado por um utilizador.
Descartado	O comando foi rejeitado. Por exemplo, porque foi substituído por outro comando ou porque o dispositivo foi registado novamente e os comandos antigos foram removidos

*Se houver um ponto de exclamação por trás da mensagem, podes obter mais informações passando o cursor sobre o ícone.

Gestão de activos (apenas a nível do dispositivo)

Informações sobre o dispositivo

Fabricante	Fabricante do dispositivo
Modelo	Modelo do dispositivo
Número do modelo	Número do modelo
Sistema operativo	Sistema operativo
Versão do SO	Versão do SO
Número de série	Número de série
ExchangeID	ExchangeID
RAM total	RAM total
Resolução do ecrã	Resolução do ecrã
Idioma do telefone	Idioma do dispositivo
Versão do firmware	Versão do firmware
Versão do cliente DM	Versão do Device Management Client
Versão do hardware	Versão de hardware do dispositivo
Arquitetura da CPU	Arquitetura da CPU (tipo de processador)

Celular

Rede da operadora SIM	Rede de operadoras
Número de telefone	Número de telefone
Estado do roaming	Estado do roaming
IMEI	IMEI
IMSI	IMSI
Firmware do modem	Firmware do modem

Informações de sincronização

Ligação DM instantânea	O dispositivo deve criar imediatamente uma ligação ao AppTec
Tempo de repetição inicial	Tempo de repetição inicial para esta primeira ligação
Tentativas de ligação	Número de novas tentativas de ligação, após uma desconexão do Gestor de Ligações ou um erro ao nível da WinInet
Tempo máximo de sono	Tempo máximo de espera após um erro de envio de pacotes
Primeiras tentativas de sincronização	Tempo para a primeira fase após a inscrição
Primeiro intervalo de repetição	Tempo para a primeira fase após a inscrição
Segunda tentativa de sincronização	Tempo para a segunda fase após o registo
Segundo intervalo de repetição	Tempo para a segunda fase após o registo
Tentativas de sincronização regulares	Tempo para as fases adicionais após a inscrição
Intervalo de repetição regular	Tempo para as fases adicionais após a inscrição

Gestão da segurança

Antirroubo (apenas ao nível do dispositivo)

Informação GPS (apenas ao nível do dispositivo)

Aqui podes determinar a localização atual/última do aparelho. A localização pode ser protegida com uma ou mesmo duas palavras-passe - Vê: "Definições gerais" > "Privacidade" > "Acesso ao GPS"

Definições GPS

Ativar a localização GPS	Permite a sincronização regular das informações GPS.
Intervalo de rastreio	Define o intervalo de sincronização da informação GPS.

Configuração de segurança

Código de acesso

Comprimento mínimo da palavra-passe	Comprimento mínimo da palavra-passe	
Composição da palavra-passe	Especifica o número de caracteres específicos que a palavra-passe deve conter São compostos por letras maiúsculas, minúsculas, números e símbolos especiais	
Qualidade da palavra-passe	Aqui podes definir a qualidade da palavra-passe	
	Alfanumérico	Apenas números e letras
	Numérico	Apenas números
	Numérico ou alfanumérico	Números ou números e letras
Bloqueio do tempo máximo de inatividade	Número de minutos de inatividade do utilizador no dispositivo, após os quais o dispositivo será bloqueado. O utilizador deve desbloquear o dispositivo após este período, introduzindo a sua palavra-passe do dispositivo.	
Expiração da palavra-passe	Define o tempo até que uma nova palavra-passe tenha de ser definida	
Restrição do histórico de senhas	Número de palavras-passe utilizadas anteriormente, que não são permitidas	
Máximo de tentativas de senha com falha	Número de vezes que a palavra-passe pode ser introduzida incorretamente, antes de ser efectuada uma limpeza completa do dispositivo	

Antivírus

Definições do antivírus - Define a configuração da verificação	
Tipo de exame	Selecciona se pretende efetuar uma verificação rápida ou uma verificação completa
Define o início da digitalização	Selecciona a hora do dia em que o Windows Defender iniciará a verificação
Frequência de varrimento	Selecciona o dia em que a verificação do Windows Defender deve ser executada
Frequência de atualização da assinatura	Especifica o intervalo em horas que será utilizado para verificar as assinaturas

Configura o tipo de ficheiros para digitalização	
Permite a verificação de ficheiros de arquivo	Permite ou não permitir a verificação de arquivos (como .zip) quando são acedidos.
Permite a verificação de scripts	Permite ou não a funcionalidade de verificação de scripts do Windows Defender.
Permite a digitalização de e-mails	Permite ou não a verificação de e-mails.
Permite a verificação de ficheiros de rede	Permite ou não a verificação de ficheiros de rede.
Permite a verificação completa das unidades de rede mapeadas	Permite ou não o rastreio de unidades de rede mapeadas (apenas ativado quando o rastreio completo está ativado).
Controla a leitura bidirecional	Controla os conjuntos de ficheiros que devem ser monitorizados.
Permite a verificação completa de unidades amovíveis	Permite ou não o rastreio completo de unidades amovíveis. Só inicia a verificação completa.

Tipo de ficheiros a excluir da verificação	
Ignora tipos de ficheiros para digitalização	Define um conjunto de tipos de extensões de ficheiros. Cada extensão de ficheiro para cada campo.
Ignora caminhos de directórios	Define um conjunto de caminhos de directórios para não os analisar. Um caminho por campo. Exemplos: "C:\Exemplo", "C:\Windows" ou "C:\Usuários".
Exclui processos da verificação	Exclui ficheiros que tenham sido abertos por processos específicos dos exames do Microsoft Defender Antivírus. . Um caminho por campo. Exemplos: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Definições adicionais	
Permite a monitorização em tempo real	Permite ou não a funcionalidade de Monitorização em Tempo Real do Windows Defender
Permite a monitorização do comportamento	Permite ou não a funcionalidade de Monitorização do Comportamento do Windows
Permite a proteção na nuvem	Permite ou não que o Windows Defender envie informações à Microsoft sobre qualquer problema que encontre. A Microsoft irá analisar essas informações, saber mais sobre o problema que afecta o dispositivo e oferecer soluções melhoradas
	Comportamento no envio de amostras
Permite a proteção IOAV do Windows Defender	Permite ou não a proteção IOAV do Windows Defender
Permite o acesso à interface de utilizador "Proteção no acesso" do Defenders	
Fator de carga médio da CPU	Representa o fator médio de carga da CPU para o exame do Windows Defender (em percentagem)

Manuseamento de malware	
Baixa gravidade	Podes definir para cada nível de gravidade a forma como o dispositivo trata o malware. As opções disponíveis são: • Limpa • Quarentena • Retira • Permite • Definido pelo utilizador • Bloqueia
Gravidade moderada	
Gravidade elevada	
Gravidade severa	
Dias para manter o malware limpo	Período de tempo em dias que os ficheiros/itens de quarentena serão armazenados no sistema. O valor predefinido é 0, o que mantém os itens em quarentena e não os remove automaticamente. O valor máximo é 90.

Centro de Segurança

Centro de Segurança do Windows - Definições para a Segurança do Windows	
Desativar a IU de proteção contra vírus e ameaças	
IU de recuperação de dados do Hide Ransomware	
Desativar a proteção de conta UI	
Desativar a Firewall e a proteção de rede UI	
Desativar a IU de controlo da aplicação e do navegador	
Não permitir alterações à proteção contra exploração	Não permite que o utilizador faça alterações às definições de proteção contra exploits
Desativar a segurança do dispositivo UI	
Ocultar a resolução de problemas do TPM	Oculta as definições de resolução de problemas do TPM
Desativar o botão Limpar TPM	
Desativar o desempenho do dispositivo e a IU de saúde	
Desativar a IU das opções de família	

Personaliza os brindes	
Ativar informações de suporte personalizadas	Permite apresentar informações de contacto de suporte personalizadas para a tua empresa no canto inferior direito da aplicação do centro de segurança.
Endereço eletrónico	Define o endereço de correio eletrónico da empresa
Nome da empresa	Define o nome da empresa
Telefone da empresa	Define o telefone da empresa
Ajuda URL	Define o URL de ajuda da empresa

Definições adicionais	
Desativar as notificações	Desativa a exibição das Notificações da Central de Segurança do Windows Defender.
Ocultar recomendações de atualização do firmware do TPM	Oculta a recomendação para atualizar o Firmware TPM quando é detectado um firmware vulnerável.
Mostra o nome da empresa e as opções de contacto	Apresenta o nome da tua empresa e as opções de contacto num cartão de contacto no Centro de Segurança do Windows Defender.
Ocultar o arranque seguro	Oculta a área de arranque de segurança.
Ocultar controlo da área de notificação de segurança	Oculta o controlo da área de notificação da Segurança do Windows.

Configuração da firewall

Configuração da firewall - Definições globais	
Ignora a autenticação definida	Ignora todo o conjunto de autenticação se não suportar todos os conjuntos de autenticação especificados no conjunto
Tipo de enfileiramento de pacotes	Especifica como o escalonamento do software no lado da receção é ativado para a receção encriptada e limpa o caminho de encaminhamento para o cenário de gateway de túnel IPsec.
Desativar a filtragem de FTP com estado	Se estiver desactivada, não efectua a filtragem do Protocolo de Transferência de Ficheiros (FTP) com estado para permitir ligações secundárias
Tempo de inatividade da associação de segurança	Este campo configura o tempo de inatividade da associação de segurança, em segundos. As associações de segurança são eliminadas depois de o tráfego de rede não ser visto durante este período de tempo especificado.
Codificação de chaves pré-partilhadas	Define a codificação da chave pré-partilhada
Excepções IPSec	Configura as excepções ao Protocolo Internet
Verificação da lista de revogação de certificados	

Perfis de firewall (perfil de domínio / perfil privado / perfil público)	
Ativar a Firewall para este perfil	
Desativar as notificações	Desactiva a apresentação de notificações ao utilizador quando uma aplicação é impedida de escutar numa porta.
Bloqueia respostas unicast a transmissões multicast	
Aplica regras de firewall de aplicações autorizadas	Se não for aplicada, as regras de firewall de aplicação autorizadas no arquivo local são ignoradas e não são aplicadas
Aplica regras globais de firewall de porta	Se não for aplicada, as regras globais de firewall de porta no repositório local são ignoradas e não são aplicadas. A definição só tem significado se for definida ou enumerada no arquivo de Política de Grupo ou se for enumerada a partir do GroupPolicyRSoPStore
Aplica regras de firewall	Se não for aplicada, as regras de firewall do armazenamento local são ignoradas e não são aplicadas
Aplica regras de segurança de ligação	Se não for aplicada, as regras de segurança da ligação do armazenamento local são ignoradas e não são aplicadas
Ação de saída predefinida	A ação que a firewall executa por defeito nas ligações de saída
Ação de entrada predefinida	A ação que a firewall executa por defeito nas ligações de entrada
Desativar o modo Stealth	O modo furtivo é um mecanismo da Firewall do Windows que ajuda a impedir que utilizadores maliciosos descubram informações sobre os computadores da rede e os serviços que executam.
Desactiva a prevenção de resposta a tráfego não solicitado	Se estiverem desactivadas, as regras do modo furtivo da firewall não devem impedir que o computador anfitrião responda a tráfego de rede não solicitado se esse tráfego estiver protegido por IPsec

Regras de firewall

Regras de firewall	
Nome	Nome da regra
Descrição	Descrição da regra
Ação	Especifica se esta regra irá bloquear o tráfego ou permiti-lo. Tem em consideração que a opção Bloquear também pode bloquear o tráfego (dependendo do resto da configuração) entre o servidor MDM e o Dispositivo
Direção	
Ativar Edge traversal (Apenas disponível quando **Direction** está definido para **tráfego de entrada**)	Indica que o tráfego de entrada específico tem permissão para fazer túneis através de NATs e outros dispositivos de borda usando a tecnologia de túneis Teredo.

Programas e serviços	
Define as aplicações, todas as outras	Se não estiver ativado, considera todas as aplicações
Nome da família do pacote	O Nome da Família de Pacotes ao qual a regra se aplicará.
Caminho do ficheiro da aplicação	A aplicação completa, como C:\Windows\System\Notepad.exe, à qual a regra se aplicará
Nome Binário Totalmente Qualificado	O Nome Binário Totalmente Qualificado ao qual a regra se aplicará. Um FQBN é uma cadeia de caracteres com o seguinte formato: {Publisher\Product\Filename,Version}
Nome do serviço	Introduz o nome de um serviço (por exemplo, "EventLog"). Podes obter uma lista de nomes de serviços no Powershell executando o comando "Get-Service".

Protocolos e portas				
Protocolo	O protocolo utilizado pela regra.			
	Valores disponíveis: - Qualquer um - Personalizado - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - Rota IPv6 - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Quando definido para Personalizado	Insere um número de protocolo entre 0 e 255	O número do protocolo
		Quando definido para TCP ou UDP	Especifica as portas locais, caso contrário serão utilizadas todas	Portas locais que a regra irá utilizar, também são permitidas portas de intervalo
			Porto local	Porta única ou um conjunto de portas. Por exemplo, 100-120, 200, 300-320.
			Especifica as portas remotas, caso contrário serão utilizadas todas	Portas remotas que a regra utilizará; também são permitidas portas de intervalo
			Porta remota	Porta única ou um conjunto de portas. Por exemplo, 100-120, 200, 300-320.

Âmbito de aplicação	
Especifica os IPs locais, caso contrário qualquer IP	Conjunto de IPs locais, também pode ser um intervalo de IPs separados por -
Endereço IP local	Conjunto de IPs individuais ou um intervalo de IPs separados por -
Especifica os IPs remotos, caso contrário, qualquer IP remoto	Especifica um conjunto de IPs remotos, que também pode ser um intervalo de IPs separados por "-".
Endereço IP remoto	Especifica IPs individuais ou um intervalo de IPs
Tokens	Tokens que podem ser definidos juntamente com Endereços Remotos. Os Tokens Intranet, RmtIntranet e Ply2Renders são suportados no Windows 10, versão 1809 e posterior.

Definições avançadas

Especifica os perfis, caso contrário serão utilizados todos	Se estiver desativado, serão utilizados todos os perfis
Domínio	Perfil do domínio
Privado	Perfil privado
Público	Perfil público
Especifica as interfaces, caso contrário serão utilizadas todas	Se estiver desativado, serão utilizadas todas as interfaces
Rede local	Interface de rede local
Acesso remoto	Interface de acesso remoto
Sem fios	Interface sem fios

Directores locais	
Adiciona utilizadores locais autorizados	Permite adicionar uma lista de utilizadores locais que utilizarão esta regra
Utilizadores autorizados	Lista de utilizadores locais autorizados para esta regra. O utilizador deve estar no formato da linguagem de definição da descrição de segurança (SDDL), por exemplo, PC_NAME\USERNAME. Este campo não deve ser preenchido se um nome de serviço estiver definido para utilizar esta regra

Definições de restrições

Funcionalidade do dispositivo

Permitir cartão SD	Permite a utilização de um cartão SD
Permitir câmara	Permite a utilização da câmara
Permitir serviço de localização	Permite o serviço de localização do dispositivo
Permitir o carregamento lateral de aplicações	Permite a instalação de aplicações de fontes desconhecidas
Permitir o modo de desenvolvedor	Permite o modo de desenvolvimento
Permitir roaming de dados celulares	Permite o roaming de dados celulares
Permitir Cortana	Permite o assistente de voz Cortana
Permitir que a pesquisa utilize a localização	Permite que a pesquisa utilize a localização
Permitir a adição de uma conta de e-mail que não seja da Microsoft	Especifica se o utilizador está autorizado a adicionar contas de correio eletrónico não MSA.
Permite a ligação da conta Microsoft	Especifica se é permitido utilizar a conta MSA para autenticação e serviços de ligação não relacionados com o correio eletrónico.
Permitir sincronizar as minhas definições	Permite a sincronização de definições em todo o dispositivo
Nomes de domínio protegidos para empresas	Especifica os nomes de domínio da empresa separados por ";".
Permite ao utilizador desativar a Restauração do sistema	Permite ao utilizador desativar a Restauração do sistema. **ATENÇÃO!** Esta funcionalidade só deve ser utilizada em dispositivos pertencentes ou fornecidos pela empresa ou organização, ou num dispositivo pertencente ao utilizador, se este permitir que o dispositivo seja totalmente gerido pela empresa. Se desactivares esta definição de política, o Restauro do Sistema é

	desativado e não é possível aceder ao Assistente de Restauro do Sistema. A opção de configurar a Restauração do sistema ou criar um ponto de restauração através da Proteção do sistema também está desativada.
Permitir o cancelamento da inscrição do utilizador	Permite que o utilizador remova a parte corporativa do dispositivo e, assim, se desligue dos Servidores AppTec360. Se isso acontecer, deixa de ser possível gerir o aparelho **ATENÇÃO!** Esta funcionalidade só deve ser utilizada em dispositivos pertencentes ou fornecidos pela empresa ou organização, ou num dispositivo pertencente ao utilizador, se este permitir que o dispositivo seja totalmente gerido pela empresa. Se desactivares esta definição de política, os utilizadores não poderão remover as inscrições na MDM. Especifica se o utilizador está autorizado a eliminar a conta do local de trabalho através do painel de controlo do local de trabalho. O servidor MDM pode sempre apagar remotamente a conta.

BitLocker

Configuração do BitLocker

Definições gerais	
Exige a encriptação do dispositivo	Solicita aos utilizadores que activem a encriptação do dispositivo. Dependendo da edição do Windows e da configuração do sistema, pode ser solicitado aos utilizadores: - Para confirmar que a encriptação de outro fornecedor não está activada. - Para desativar a Encriptação da Unidade de Disco BitLocker e voltar a ativar o BitLocker.
Métodos de encriptação	
Método de encriptação para unidades do sistema operativo	
Método de encriptação para unidades de dados fixas	
Método de encriptação para unidades de dados amovíveis	
Desativar o aviso sobre encriptação de disco de terceiros	Desactiva o aviso de aviso sobre um serviço de encriptação de disco de terceiros que está a ser utilizado no dispositivo. A partir do Windows 10, versão 1803, esta definição só é suportada para dispositivos associados ao Azure Active Directory.
Permite executar a encriptação enquanto o utilizador não administrador tem sessão iniciada	Suportado apenas para dispositivos associados ao Azure Active Directory

Extensões AppTec360	
Encriptação silenciosa	Se for selecionado juntamente com "Require device encryption" (Exigir encriptação do dispositivo), o AppTec360 Management Service executará a encriptação silenciosa automática das unidades do dispositivo.
Gera automaticamente credenciais de utilizador	A unidade do SO encriptada será protegida com credenciais de utilizador geradas automaticamente. Ou um PIN TPM, quando um TPM está disponível, ou uma palavra-passe textual de 6 dígitos. As credenciais geradas são enviadas para o endereço de correio eletrónico registado para o dispositivo em causa. Se esta opção estiver desactivada, a única proteção possível para a encriptação silenciosa é a utilização do TPM. Nesse caso, para dispositivos sem um TPM, a encriptação silenciosa falhará.
Encripta unidades fixas	Todas as unidades de dados fixas disponíveis serão também encriptadas e protegidas com "Desbloqueio automático" utilizando uma chave armazenada na unidade do SO.

Definições da unidade do SO

Exige autenticação adicional no arranque	Esta definição permite-te configurar se o BitLocker requer uma autenticação sempre que o computador é iniciado. Esta definição é aplicada durante a configuração do BitLocker. Se activares esta definição, os utilizadores podem configurar opções de arranque avançadas no assistente de configuração do BitLocker.
Bloqueia o BitLocker sem um TPM compatível	
Apenas TPM	
TPM e PIN	
TPM e chave	
TPM, chave e PIN	Se pretenderes exigir a utilização de um PIN e de uma unidade flash USB (chave), o utilizador deve configurar o BitLocker utilizando a ferramenta de linha de comandos "manage-bde" em vez do assistente de configuração da Encriptação de Unidade de Disco BitLocker.

Exige o comprimento mínimo do PIN

	Caracteres mínimos

Configura a mensagem e o URL da recuperação antes do arranque	Configura toda a mensagem de recuperação ou substitui o URL existente que é apresentado no ecrã de recuperação da chave de pré-inicialização quando a unidade do SO está bloqueada. Nota: Nem todos os caracteres e línguas são suportados no pré-arranque. Recomenda-se vivamente que verifiques se os caracteres que utilizas aparecem corretamente no ecrã de recuperação antes do arranque.
	Opção de mensagem de recuperação antes do arranque
	Mensagem de recuperação personalizada
	URL de recuperação personalizado

Opções de recuperação da unidade do SO		Esta definição permite-te controlar a forma como as unidades do sistema operativo protegidas pelo BitLocker são recuperadas na ausência das credenciais necessárias. Esta definição é aplicada durante a configuração do BitLocker. Por predefinição, é permitido um agente de recuperação de dados com base em certificados, as opções de recuperação podem ser especificadas pelo utilizador, incluindo a palavra-passe de recuperação e a chave de recuperação, e as informações de recuperação não são copiadas para o AD DS.
	Agente de recuperação de dados baseado em certificados de bloco	Especifica se um agente de recuperação de dados pode ser utilizado com unidades do sistema operativo protegidas pelo BitLocker. Antes de um agente de recuperação de dados poder ser utilizado, tem de ser adicionado a partir do item Políticas de Chave Pública na Consola de Gestão de Políticas de Grupo ou no Editor de Políticas de Grupo Local. Consulta o Guia de Implementação da Encriptação de Unidade de Disco BitLocker no Microsoft TechNet para obteres mais informações sobre como adicionar agentes de recuperação de dados.
	Definições da palavra-passe de recuperação do BitLocker	
	Definições da chave de recuperação BitLocker	
	Guarda as informações de recuperação do BitLocker nos Serviços de Domínio do Active Directory	
	Configuração do armazenamento de recuperação do BitLocker do AD DS	O armazenamento do pacote de chaves suporta a recuperação de dados de uma unidade que tenha sido fisicamente corrompida.
	Exige o armazenamento de dados de recuperação no AD DS	Impedir que os utilizadores activem o BitLocker, a menos que o computador esteja ligado ao domínio e

Definições de acionamento fixas	
Opções de recuperação de unidades fixas	Esta definição permite-te controlar a forma como as unidades fixas protegidas pelo BitLocker são recuperadas na ausência das credenciais necessárias. Esta definição é aplicada durante a configuração do BitLocker. Por predefinição, é permitido um agente de recuperação de dados com base em certificados, as opções de recuperação podem ser especificadas pelo utilizador, incluindo a palavra-passe de recuperação e a chave de recuperação, e as informações de recuperação não são copiadas para o AD DS.
Agente de recuperação de dados baseado em certificados de bloco	
Definições da palavra-passe de recuperação do BitLocker	
Definições da chave de recuperação BitLocker	
Guarda as informações de recuperação do BitLocker nos Serviços de Domínio do Active Directory	
Configuração do armazenamento de recuperação do BitLocker do AD DS	O armazenamento do pacote de chaves suporta a recuperação de dados de uma unidade que tenha sido fisicamente corrompida.
Requer o armazenamento de dados de recuperação no AD DS	Impede que os utilizadores activem o BitLocker, a menos que o computador esteja ligado ao domínio e que a cópia de segurança das informações de recuperação do BitLocker para o AD DS seja bem sucedida. Nota: A palavra-passe de recuperação é gerada automaticamente.
Recusa o acesso de escrita a unidades fixas desprotegidas	

Definições da unidade amovível	
Recusa o acesso de escrita a unidades amovíveis desprotegidas	Nega o acesso de escrita a unidades de dados amovíveis que não estejam protegidas pelo Bitlocker. Nota: Se "Discos amovíveis: Negar acesso de escrita" estiver activada na política de grupo, esta definição de política será ignorada.
Nega o acesso de escrita a dispositivos configurados noutra organização	Apenas as unidades com campos de identificação correspondentes aos campos de identificação do computador terão acesso de escrita. Estes campos são definidos pela definição de política de grupo "Fornecer os identificadores únicos para a tua organização".

Estado do BitLocker

Aqui podes ver o estado atual das unidades encriptadas BitLocker

C [OS Drive]
Estado da encriptação
Criptografado (%)
Estado de proteção
Método de encriptação
Protectores de chaves
Recuperar palavra-passe

Com um clique no botão "Rodar a palavra-passe de recuperação", podes rodar a palavra-passe de recuperação do BitLocker.

Gestão de certificados

Lista de certificados

Aqui tens uma lista de certificados que estão instalados no dispositivo que está a ser apresentado.

Configuração do certificado

Aqui podes configurar os certificados e a forma como serão instalados no dispositivo.

Certificado fiável	
Descrição	Descrição do certificado
Âmbito de aplicação	Âmbito de implementação do certificado: Utilizador atual vs Dispositivo
Armazenamento de certificados	A opção "Certificados não confiáveis" só está disponível a partir do Windows 10, versão 1803
Ficheiro de certificado	Carrega um ficheiro PKCS#1

Certificado de identidade			
Descrição	Descrição do certificado		
Âmbito de aplicação	Âmbito de implementação do certificado: Utilizador atual vs Dispositivo		
Localização chave	O fornecedor de armazenamento de chaves para instalar a chave privada.		
		TPM. Falha se não houver TPM presente	
	TPM. Se não houver TPM presente, recorre ao Software KSP		
	Fornecedor de armazenamento de chaves de software		Marca a chave privada como exportável
	Windows Hello para Empresas	Nome do contentor	Especifica o nome do contentor do Windows Hello para Empresas (anteriormente conhecido como Microsoft Passport for Work).
		Texto do PIN	Especifica o texto personalizado a ser exibido no prompt do PIN do Windows Hello para Empresas durante o registro do certificado.
Credencial	Carrega um ficheiro PKCS#12		

SCEP

Descrição	Descrição do servidor SCEP		
Âmbito de aplicação	Âmbito de implementação do certificado: Dispositivo atual vs Utilizador		
URLs do servidor SCEP	Um ou mais servidores que emitem certificados através do SCEP		
Assunto	Representação de um nome X.500. Por exemplo, "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Nomes alternativos de temas	Tipo	Endereço de correio eletrónico	
		DNS	
		URI	
		Nome principal do utilizador (UPN)	
Impressão digital CA	A impressão digital SHA1 do certificado da Autoridade de Certificação. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Unidades do período de validade	Dias, meses ou anos		
Período de validade			
Desafio	Utilizado como segredo pré-partilhado para inscrição automática		
Tentativas	O número de vezes que o dispositivo deve tentar novamente se o servidor enviar uma resposta PENDING. O valor predefinido é 5. O valor máximo é 30.		
Atraso de repetição	Número de minutos a aguardar antes de tentar de novo. O valor predefinido é 5. O valor mínimo é 1.		
Tamanho da chave	Tamanho da chave em bits		
Algoritmo de hash	Família de algoritmos de hash		
Utilização das chaves	A extensão de utilização da chave define o objetivo (por exemplo, cifragem, assinatura) da chave contida no certificado. Pelo menos uma das opções "Assinatura digital" ou "Cifragem de chaves" tem de ser selecionada.		

Utilização alargada da chave	Especifica as utilizações de chaves alargadas, sujeitas à configuração do servidor SCEP. Especifica a lista de OIDs correspondentes, por exemplo, 1.3.6.1.5.5.7.3.2 (Autenticação de cliente)		
Localização chave	O fornecedor de armazenamento de chaves para instalar a chave privada.		
		TPM. Falha se não houver TPM presente	
	TPM. Se não houver TPM presente, recorre ao Software KSP		
	Fornecedor de armazenamento de chaves de software		
	Windows Hello para Empresas	Nome do contentor	Especifica o nome do contentor do Windows Hello para Empresas (anteriormente conhecido como Microsoft Passport for Work).
		Texto do PIN	Especifica o texto personalizado a ser exibido no prompt do PIN do Windows Hello para Empresas durante o registro do certificado.

Gestão de ligações

Wifi

Nesta definição, efectua a pré-configuração dos dispositivos do utilizador final para acesso aos pontos de acesso internos

Identificador do conjunto de serviços (SSID)	SSID para a rede, para a qual a ligação será estabelecida
Auto Join	Ativar a adesão automática à rede
Rede oculta	Ativar, no caso de o AP não transmitir o SSID

Tipo de segurança

Estabelece o tipo de segurança AP

Sistema aberto WEP	
Palavra-passe	Palavra-passe para o PA

WPA PSK	
Palavra-passe	Palavra-passe para o PA

WPA EAP	
Tipo de autenticação	Tipo de autenticação, apenas possível com "PEAP-MSCAHPv2"
Ligação rápida	Os dispositivos podem alternar entre pontos de acesso, sem terem de se autenticar novamente
Acesso para convidados	O utilizador não tem uma conta e, por isso, deve registar-se como convidado
Verificações de quarentena	O cliente deve efetuar verificações NAP (Network Access Protection) e partilhar os resultados com o sistema, que decide então se o cliente pode ligar-se
Exige ligação criptográfica	A autenticação só é possível através da ligação criptográfica
Validação do servidor	O cliente verifica se o certificado do servidor é válido. Se for esse o caso, estabelece uma ligação
Solicita certificados	Permite que o utilizador aceite certificados não fidedignos
Nomes de servidores	Oferece a opção de mostrar o nome do servidor RADIUS, que oferece a autenticação e autorização de rede

WPA2-PSK	
Palavra-passe	Palavra-passe AP

WPA2 EAP	
Tipo de autenticação	Tipo de autenticação, apenas possível com "PEAP-MSCAHPv2"
Ligação rápida	
Acesso para convidados	
Verificações de quarentena	Ativa a proteção de acesso à rede NAP
Exige ligação criptográfica	A autenticação só é possível através da ligação criptográfica
Validação do servidor	
Solicita certificados	Solicita um certificado de servidor validado, um nome ou uma autenticação de certificado raiz (CA)
Nomes de servidores	Listagem dos servidores em que os dispositivos devem confiar
Não tens	Não há segurança estabelecida
Utiliza o servidor proxy	Utilização de um servidor proxy
Endereço do servidor	Endereço do servidor proxy
Porta do servidor	Porta do servidor do servidor proxy

Utiliza o servidor proxy

Ativa a utilização do servidor proxy.

Endereço do servidor	Endereço do servidor proxy utilizado por esta rede.
Porta do servidor	Porta do servidor proxy utilizada por esta rede.

Restrições de Wifi

Aqui podes definir várias restrições Wifi.

Permitir WiFi	Permitir/negar WiFi
Permitir a partilha da Internet	Permitir a utilização de um Hotspot
Permite a ligação automática a pontos de acesso WiFi Sense	Permite a ligação automática a pontos de acesso WiFi Sense
Permite a configuração manual do WiFi	Permite ao utilizador ligar-se a redes WiFi que não tenham sido definidas pela AppTec
Frequência de varrimento WLAN	Estabelece o intervalo do WLAN-Scan. Aqui, um valor mais elevado aumenta a capacidade de reconhecer redes WIFI.

VPN

Efectua as definições apropriadas aqui, para configurar as ligações VPN

Nome da ligação	Nome da ligação indicada		
Tipo de VPN	Uma ligação VPN por aplicação é utilizada para proteger o tráfego de determinadas aplicações.		
	VPN	Sempre ligado	Isto ligará automaticamente a VPN no início da sessão e permanecerá ligado até que o utilizador desligue manualmente.
	VPN por aplicação	Aplicações VPN	Define as aplicações que utilizam esta ligação VPN
		Bloqueio por aplicação	O bloqueio por aplicação faz com que as aplicações seleccionadas só tenham conetividade através desta ligação VPN. Esta funcionalidade depende da Firewall do Windows Defender.
	Perfil WIP	Domínio WIP para esta ligação	Enterprise ID, que é necessário para ligar este perfil VPN a uma política de Proteção de Informação do Windows (WIP)

Tipo de ligação

AppTec360 VPN	
Para o "AppTec360 VPN", é necessário que o carregamento lateral de aplicações seja permitido. Ativa a opção "Permitir carregamento lateral de aplicações" em "Gestão de segurança" → "Definições de restrições" → "Funcionalidade do dispositivo".	
Configuração da porta de entrada	Para configurar uma ligação VPN com lista negra, selecciona uma configuração VPN com um servidor DNS especificado. Podes definir uma configuração VPN em "Definições gerais" → "Universal Gateway" → "Definições VPN".

IKEv2		
Servidores	Lista de servidores VPN	
Túnel do dispositivo	Ativa a ligação antes do início de sessão do utilizador.	
Método de autenticação	PAA	EAP XML
	Certificados de máquinas	
Algoritmo de encriptação		
Algoritmo de verificação da integridade		
Grupo Diffie-Hellman		
Algoritmo de transformação de cifra		
Algoritmo de transformação de autenticação		
Grupo de sigilo de encaminhamento perfeito (PFS)		

PPTP		
Servidores	Lista de servidores VPN	
Método de autenticação	PAA	EAP XML

L2TP		
Servidores	Lista de servidores VPN	
Método de autenticação	PAA	EAP XML
Algoritmo de encriptação		
Algoritmo de verificação da integridade		
Grupo Diffie-Hellman		
Algoritmo de transformação de cifra		
Algoritmo de transformação de autenticação		
Grupo de sigilo de encaminhamento perfeito (PFS)		

Automático		
Servidores	Lista de servidores VPN	
Método de autenticação	PAA	EAP XML

Configurações genéricas de VPN

Lembra-te das credenciais em cada início de sessão	
Registar endereços IP no DNS interno	
Regras de filtragem de tráfego de rede	Limita a ligação VPN ao conjunto de regras definido.
Lista de pesquisa de sufixos DNS	Sufixos DNS a adicionar à lista de pesquisa DNS para encaminhar nomes curtos.
Regras da tabela de políticas de resolução de nomes (NRPT)	As regras da tabela de Política de Resolução de Nomes (NRPT) definem como o DNS resolve nomes quando ligado à VPN.
Deteção de redes fiáveis	Lista de sufixos DNS para identificar uma rede de confiança.
Separa o túnel	O túnel dividido significa que o tráfego pode passar por qualquer interface, conforme determinado pela pilha de rede.
Rotas de tunelamento divididas	Lista de rotas a adicionar à tabela de encaminhamento para a interface VPN.
Configuração do proxy	Configura o Proxy utilizado com esta rede
Endereço de proxy	Endereço do servidor proxy como um nome de anfitrião totalmente qualificado ou um endereço IP.
Porto	Porta do servidor proxy.
URL de configuração automática do proxy	URL para recuperar automaticamente as definições de proxy.

Restrições VPN

Aqui podes definir várias restrições VPN.

Permitir definições VPN	Esta orientação permite/proíbe o utilizador de desativar e alterar as definições da VPN
Permitir VPN através de telemóvel	Permite/obriga o dispositivo a estabelecer uma ligação VPN, se o dispositivo estiver a utilizar dados móveis
Permitir Roaming VPN através do telemóvel	Permite/obriga o dispositivo a estabelecer uma ligação VPN, se o dispositivo estiver em roaming

Bluetooth

Aqui podes determinar se o Bluetooth deve ser permitido ou proibido.

Permitir Bluetooth	Ativar/desativar o Bluetooth

Gestão PIM

Exchange Active Sync

Configura a conta ActiveSync no dispositivo do utilizador final

Nome da conta	Nome da conta de correio eletrónico
Nome do anfitrião do servidor	Endereço do servidor/FQDN
Nome de domínio	Domínio do servidor
Endereço de e-mail	Endereço de correio eletrónico
Nome do utilizador	Nome do utilizador
Palavra-passe do utilizador	Opcionalmente, já podes anexar uma palavra-passe ao utilizador aqui
Utiliza SSL	Utiliza a ligação SSL
Intervalo de sincronização	Aqui podes estabelecer o intervalo de sincronização Sincronização manual = O utilizador tem de transferir os seus e-mails e efetuar uma sincronização manual
Filtro de idade do correio	Quantidade de tempo, até que os e-mails sejam sincronizados Sem filtro = ilimitado
Nível de registo	Estabelecimento dos níveis de registo para o tráfego ActiveSync
Sincronizar e-mail	Ativado = os e-mails são sincronizados
Sincronizar contactos	Ativado = os contactos são sincronizados
Sincroniza o calendário	Ativado = o calendário está sincronizado
Sincronizar tarefas	Ativado = as tarefas são sincronizadas

eMail

Estabelecimento de contas POP3/IMAP4 no dispositivo do utilizador final.

Descrição da conta	Nome da conta de correio eletrónico
Nome do remetente	Nome do remetente apresentado
Nome de domínio	Nome de domínio da conta de correio eletrónico
Endereço de e-mail	Endereço de correio eletrónico do utilizador
Nome do utilizador	Nome do utilizador
Palavra-passe do utilizador	Opcionalmente, já podes anexar uma palavra-passe ao utilizador aqui
Credenciais alternativas do servidor de saída	Aqui podes definir se são necessárias outras credenciais para o servidor de saída
Nome de domínio de saída	Nome de domínio de saída
Nome de utilizador do servidor de saída	Nome do utilizador do servidor de saída
Palavra-passe do servidor de saída	Palavra-passe do servidor de saída
Protocolo de correio eletrónico	POP3 ou IMAP4, pode ser utilizado como um protocolo
Nome do anfitrião do servidor de correio de entrada	Nome do anfitrião do servidor de correio de entrada
Utiliza SSL para mensagens recebidas	Utiliza SSL para e-mails recebidos
Nome do anfitrião do servidor de correio de saída	Nome do anfitrião do servidor de correio de saída
Utiliza SSL para os e-mails enviados	Utiliza SSL para e-mails de saída
Autenticação do servidor de saída	É necessária uma autenticação do servidor de saída
Intervalo de sincronização	Aqui podes estabelecer o intervalo de sincronização Sincronização manual = O utilizador tem de transferir os seus e-mails e efetuar uma sincronização manual
Filtro de idade do correio	Quantidade de tempo, até que os e-mails sejam sincronizados Sem filtro = ilimitado

Gestão de aplicações

Gestor de aplicações empresariais

Aplicações instaladas

Aqui tens uma lista das aplicações que estão atualmente instaladas no dispositivo que está a ser apresentado.

Aplicações obrigatórias

Aqui podes configurar uma lista de aplicações que são obrigatórias no dispositivo.

Esta lista será verificada sempre que o dispositivo se ligar à MDM e instala todas as aplicações desta lista que não estejam instaladas no dispositivo, independentemente de a aplicação ter sido desinstalada ou nunca ter sido instalada anteriormente.

Podes carregar aplicações internas do Windows 10 e depois adicioná-las a esta lista ou podes adicionar configurações do Microsoft Office que têm de ser configuradas previamente em "Definições gerais" > "Gestão de aplicações" > "Microsoft Office".

Restrições da aplicação de sistema

Aplicações da caixa de entrada
Permite alarmes e relógio
Permitir calculadora
Permitir câmara
Permitir o contacto com o suporte
Permitir Cortana
Permitir o Explorador de Ficheiros
Permitir começar
Permite a música Groove
Permitir mapas
Permite o envio de mensagens
Permitir o Microsoft Edge
Permite filmes e TV
Permitir dinheiro
Permitir notícias
Permitir OneDrive
Permite o OneNote
Permitir o calendário e o correio do Outlook
Permitir que as pessoas
Permitir telefone
Permitir fotografias
Permite o Powerpoint
Permitir definições
Permite o Skype
Permitir desportos
Permitir armazenar
Permite o Gravador de Voz
Permitir carteira
Permite o tempo

Permite o Hub de Feedback do Windows
Permitir palavra
Permite à Xbox

Definir páginas
Permitir contas no local de trabalho
Permitir informações avançadas
Permitir canto das aplicações
Permite bloquear e filtrar
Permitir perfil de cor
Permite o modo de condução
Permitir e-mail e contas
Permite o Equalizador
Permitir teclado
Permitir barra de navegação
Permitir o modo de avião da rede
Permitir a partilha de Internet na rede
Permitir serviços de rede
Permitir rede Wi-Fi
Permite o Bluetooth do sistema do PC
Permitir Avaliar o teu dispositivo
Permitir a atualização do restauro
Permitir a partilha
Permitir início
Permitir tempo Língua
Permitir tempo Região
Permitir o ecrã de bloqueio predefinido do Windows
Permitir conta de trabalho ou escola

Lista negra e lista branca

Em "Black- & Whitelisting", podes escolher entre o modo "Whitelist" e o modo "Blacklist".

Lista branca	Apenas as aplicações e os serviços adicionados à lista podem ser instalados no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão activados e definidos, para que o utilizador os possa executar.
	Todas as outras aplicações que não sejam adicionadas à lista não podem ser instaladas no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão desactivados e definidos, para que o utilizador não os possa executar.
Lista negra	As aplicações e os serviços que são adicionados à lista não podem ser instalados no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão desactivados e definidos, para que o utilizador não os possa executar.
	Todas as outras aplicações que não são adicionadas à lista podem ser instaladas no dispositivo do utilizador final. Se estes já estiverem pré-instalados no dispositivo do utilizador final, serão activados e definidos, para que o utilizador os possa executar.

Através da tecla , adiciona mais aplicações ou serviços à lista atualmente utilizada.

Através do botão , adiciona mais aplicações ou serviços à lista atualmente inativa.

Podes adicionar uma aplicação da "Windows App Store" ou introduzir diretamente um "Identificador de aplicação" para adicionar à lista negra ou branca.

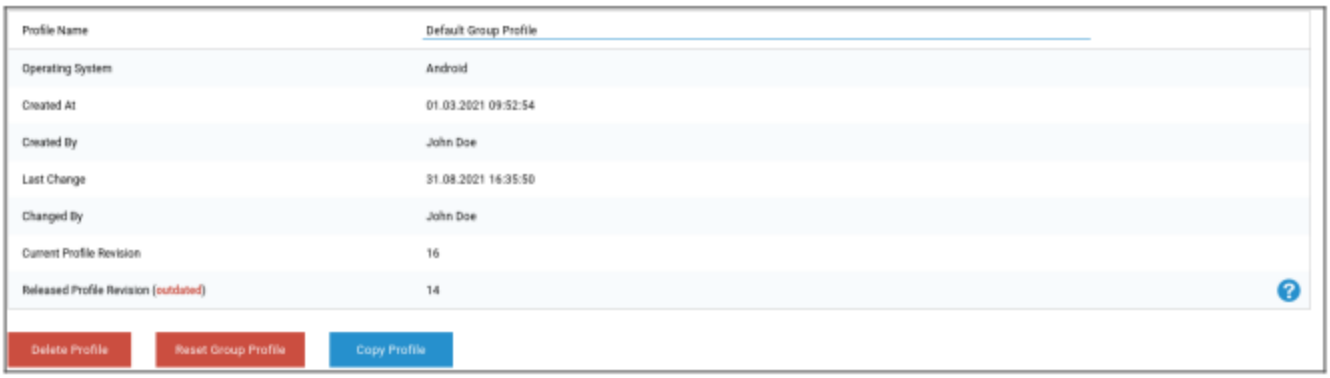
Configuração do MacOS

Dependendo de teres selecionado um perfil ou um dispositivo, o ecrã e os seus subpontos são diferentes - presta muita atenção a isto!

Geral

Síntese do perfil do grupo (apenas a nível do grupo)

Ao abrires um perfil de grupo, terás uma visão geral rápida do perfil.



Nome do perfil	Nome do perfil (pode ser alterado aqui)
Sistema operativo	Sistema operativo para o qual o perfil se destina
Criado em	Tempo de criação
Criado por	O criador do perfil
Última alteração	Hora da última modificação do perfil
Alterado por	Conta que efectuou as últimas alterações
Revisão do perfil atual	Revisão do estado do perfil guardado
Revisão do perfil lançado	Revisão do perfil atribuído ("Atribuir agora"). Se a etiqueta apresentar " (desatualizado)" por trás do texto, significa que guardaste o perfil mas ainda não o atribuíste, pelo que os dispositivos continuarão a receber uma versão mais antiga.

Síntese do dispositivo (apenas ao nível do dispositivo)

Apresenta uma visão geral resumida do aparelho.

Nome do dispositivo	Nome do dispositivo
Modelo	Modelo
Sistema operativo	Sistema operativo
Número de série	Número de série do aparelho
Propriedade do dispositivo	O tipo de propriedade configurado
Tipo de dispositivo	O tipo do dispositivo
Conformidade	Mostra se o dispositivo é compatível
Endereço IP	O endereço IP a partir do qual o dispositivo está ligado ao servidor
Visto pela última vez	Hora da última ligação do dispositivo
Último empurrão	Hora do último envio para o dispositivo
Atribuição	Aqui podes mover o dispositivo para outro utilizador ou grupo

Config Revision (apenas a nível do dispositivo)

Aqui tens uma visão geral do perfil de grupo que está atribuído ao aparelho.

Se clicares no perfil de grupo, acederás diretamente ao perfil e poderás efetuar definições.

Com o símbolo, podes reverter as aplicações atribuídas para as definições do perfil de grupo.

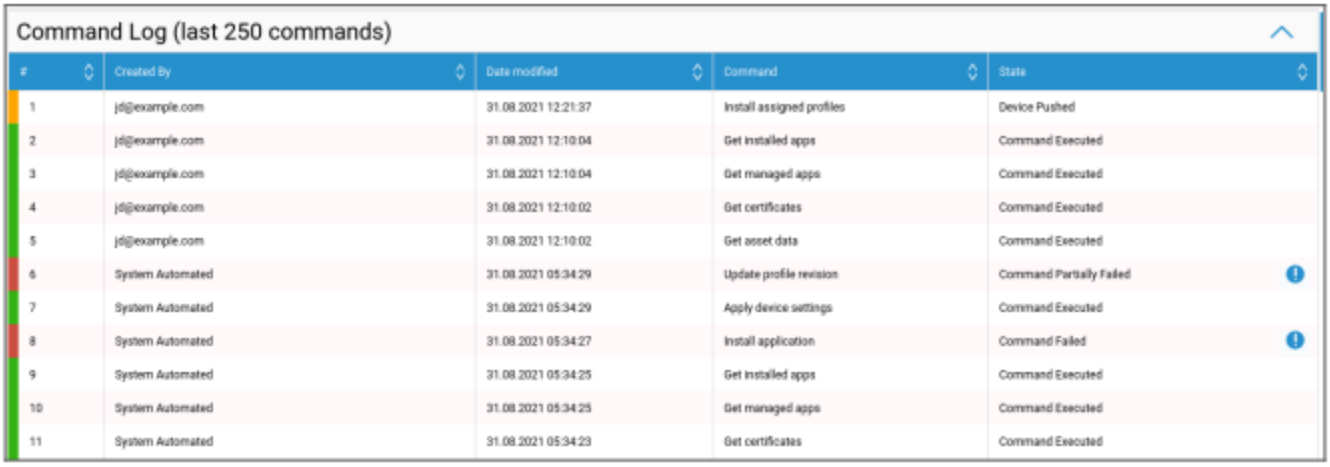
Com o símbolo, podes repor o perfil do dispositivo para que não tenha quaisquer definições.

"Newer Revision available" indica que o perfil de grupo foi alterado e guardado, mas não atribuído. O perfil de grupo tem de ser atribuído com "Atribuir agora" ao nível do grupo para aplicar as alterações aos dispositivos.

Registo do dispositivo (apenas ao nível do dispositivo)

Registo de comandos

Aqui podes ver quais os comandos que foram emitidos para o dispositivo e qual o seu estado.



Os comandos criados por "Sistema automatizado" são automaticamente criados pelo sistema.

Status de comando possíveis

Dispositivo empurrado	Foi enviado um pedido push para o serviço push (por exemplo, APNS) para dizer ao dispositivo para se ligar novamente ao servidor EMM.
Comando criado	O comando foi criado no sistema.
Comando enviado	O comando foi enviado para o dispositivo depois de este se ter ligado ao servidor.
Comando Executado	O comando foi executado com sucesso.
Falha no comando	O comando falhou. *
Comando parcialmente falhado	Dependendo do sistema operativo do dispositivo, alguns comandos podem ser agrupados. Neste caso, algumas partes deste grupo de comandos falharam. *
Comando executado, eventualmente falhou	O comando foi executado, mas talvez não o tenha sido.
Comando repuxado	O comando foi reenviado por um utilizador.
Descartado	O comando foi rejeitado. Por exemplo, porque foi substituído por outro comando ou porque o dispositivo foi registado novamente e os comandos antigos foram removidos

*Se houver um ponto de exclamação por trás da mensagem, podes obter mais informações passando o cursor sobre o ícone.

Gestão de activos (apenas a nível do dispositivo)

Informações sobre o dispositivo

Número do modelo	Número do modelo
Nome do anfitrião	Nome do anfitrião
Nome de anfitrião local	Nome de anfitrião local
Sistema operativo	Sistema operativo
Versão do SO	Versão do SO
UDID	UDID
Memória livre / total	Memória livre / total

WiFi

Endereço IP	Endereço IP
WiFi MAC	WiFi MAC

Celular

Número de telefone	Número de telefone
Estado do roaming	Estado do roaming
Roaming (Voz / Dados)	Roaming (Voz / Dados)
Endereço IP	Endereço IP
Operador/Carrier	Operador/Carrier
Rede da operadora SIM	Rede de operadoras
Versão para transportadora	Versão para transportadora
ICCID	ICCID
Atual MCC/MNC	Atual MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Gestão de actualizações (apenas ao nível do dispositivo)

Atualizar informações

Este separador mostra informações sobre as definições de atualização do sistema no dispositivo.

Autocheck ativado	Se o sistema estiver a verificar a atualização automaticamente.
Atualização automática de aplicações activada	Se o sistema instalar automaticamente actualizações de aplicações.
Actualizações automáticas do SO activadas	Se o sistema instala automaticamente as actualizações do sistema operativo.
Actualizações de segurança automáticas activadas	Se o sistema instalar automaticamente as actualizações de segurança.
Atualização da aplicação Descarregamento em segundo plano ativado	Se o sistema descarregar actualizações de aplicações em segundo plano.
URL do catálogo	O URL do catálogo de atualização de software que o cliente está a utilizar.
É o catálogo predefinido	Se "sim", Catalog é o catálogo predefinido.
Efectua um controlo periódico	Se "sim", inicia uma nova verificação.
Data do exame anterior	A data da última verificação de atualização de software.
Resultado do exame anterior	O código de resultado da última verificação de atualização de software.

Gestão da segurança

Antirroubo

Limpa e bloqueia

Limpeza total	Envia um comando para repor as predefinições do dispositivo
Limpeza da empresa	Remove a MDM do dispositivo e remove todos os dados da MDM (por exemplo, contas, aplicações)
Bloqueio do ecrã	Faz com que o dispositivo regresse ao ecrã de bloqueio

Configuração de segurança

Código de acesso

Desativação do código permitida	Determina se o utilizador é obrigado a definir um PIN. A simples definição deste valor (e não de outros) obriga o utilizador a introduzir um código de acesso, sem impor um comprimento ou qualidade.
Permite um valor simples	Permitir que o utilizador utilize as mesmas sequências de números, escalonadas e reduzidas (ex. 1234, 1111)
Exige um valor alfanumérico	As palavras-passe devem conter pelo menos uma letra
Comprimento mínimo do código de acesso	Comprimento mínimo da palavra-passe
Número mínimo de caracteres complexos	Número mínimo de símbolos alfanuméricos na palavra-passe
Idade máxima do código de acesso	Número de dias, após os quais a palavra-passe deve ser alterada
Bloqueio automático máximo	Tempo máximo após o qual o dispositivo é bloqueado
Período máximo de tolerância para o bloqueio do dispositivo	Tempo durante o qual o dispositivo pode ser bloqueado sem pedir o código de acesso no desbloqueio
Idade máxima da palavra-passe (1-730 dias, ou nenhuma)	Dias após os quais o código de acesso deve ser alterado
Histórico de códigos de acesso (1-50 códigos de acesso, ou nenhum)	Número de códigos de acesso únicos antes da reutilização

Certificado

PKCS#1	
Descrição	Introduz uma descrição para o certificado
Credencial	Carrega um ficheiro pkcs1

PKCS#12	
Descrição	Introduz uma descrição para o certificado
Credencial	Carrega um ficheiro pkcs12

Definições de restrições

Funcionalidade do dispositivo

Permitir câmara	Permite a utilização da câmara
Permite o Game Center	Quando falso, o Game Center é desativado e o seu ícone é removido do ecrã inicial.
Permite jogos multijogador	Quando falso, proíbe os jogos multijogador.
Permite adicionar amigos do Game Center	Quando falso, proíbe a adição de amigos ao Game Center.
Permitir a Fototeca iCloud	Se definido como falso, desactiva a Fototeca do iCloud. As fotografias que não forem totalmente transferidas da Fototeca em iCloud para o dispositivo serão removidas do armazenamento local.
Permitir Touch ID	Se for falso, impede o Touch ID de desbloquear um dispositivo.

iCloud

Bloqueia determinadas funcionalidades durante o emparelhamento do iCloud

Permite a sincronização de documentos	Permite a sincronização de documentos
Permitir a sincronização das chaves do iCloud	Permitir a sincronização das chaves do iCloud
Permitir notas do iCloud	Quando falso, não permite os serviços do MacOS iCloud Notes
Permitir iCloud BTMM	Quando falso, não permite o serviço iCloud do MacOS Back to My Mac.
Permitir o iCloud FMM	Quando falso, desativa o serviço iCloud do MacOS Find My Mac.
Permitir favoritos do iCloud	Quando falso, não permite a sincronização dos Marcadores do iCloud do MacOS.
Permitir o Mail do iCloud	Quando falso, não permite os serviços iCloud do MacOS Mail.
Permitir o Calendário iCloud	Quando falso, não permite os serviços iCloud da MacOS Cloud.
Permitir lembretes do iCloud	Quando falso, desativa os serviços do Lembrete do iCloud.

Permitir a agenda de endereços do iCloud	Quando falso, não permite os serviços do Catálogo de Endereços do iCloud do MacOS.

Gestão dos meios de comunicação social

Ejetar ao terminar a sessão	Ejecta todos os suportes de dados amovíveis ao terminar a sessão
Permitir rede	Permite o acesso a suportes de rede
Permitir disco interno	Permite o acesso ao disco interno.
Exige autenticação	Exige autenticação para a utilização deste meio de comunicação
Apenas para leitura	O Utilizador só pode ler dados do suporte
Permitir disco externo	Permite o acesso ao disco externo.
Exige autenticação	Exige autenticação para a utilização deste meio de comunicação
Apenas para leitura	O Utilizador só pode ler dados do suporte
Permite a utilização de imagens de disco	Permite o acesso a imagens.
Exige autenticação	Exige autenticação para a utilização deste meio de comunicação
Apenas para leitura	O Utilizador só pode ler dados do suporte
Permite a utilização de DVD-RAMs	Permite o acesso ao disco DVD-RAM.
Exige autenticação	Exige autenticação para a utilização deste meio de comunicação
Apenas para leitura	O utilizador só pode ler dados do suporte
Permite a utilização de DVD	Permite o acesso ao disco DVD.
Exige autenticação	Exige autenticação para a utilização deste meio de comunicação
Permite a utilização de CDs	Permite o acesso ao disco CD.
Exige autenticação	Exige autenticação para a utilização deste meio de comunicação

Gestão de ligações

Wi-Fi

Aqui podes adicionar e configurar ligações Wi-Fi

Identificador do conjunto de serviços (SSID)	SSID da rede, para a qual a ligação será estabelecida
Auto Join	Ativar a adesão automática à rede
Rede oculta	Ativa, no caso de o AP não transmitir o SSID
Configuração de proxy	Configuração de um Proxy para cada ponto de acesso
Não tens	Não utilizes um servidor proxy
Manual	Estabelece um proxy manual
URL do servidor proxy	Endereço para aceder às definições de proxy
Porto	Estabelece a porta para o Proxy
Autenticação	Nome de utilizador para a autenticação no Proxy
Palavra-passe	Palavra-passe para a autenticação no Proxy
Automático	Estabelece um Proxy automaticamente
URL do servidor proxy	URL do ficheiro de definições do proxy
Tipo de segurança	Estabelece o tipo de segurança para o PA
WEP	
Palavra-passe	Palavra-passe para o PA
WPA/WPA2	
Palavra-passe	Palavra-passe para o PA
WEP Enterprise - WPA / WPA2 Enterprise / Qualquer empresa	Ver tabela Erro: Fonte de referência não encontrada abaixo
Não tens	Não estabelece nenhuma segurança
Desativar a aleatoriedade do endereço MAC	Desactiva a aleatoriedade do endereço MAC para essa rede Wi-Fi enquanto estiver associada à rede. Mostra também um aviso de privacidade nas Definições, indicando que a rede reduziu as protecções de privacidade.

Configuração de Wi-Fi empresarial

Nota: Só está disponível quando "Tipo de segurança" está definido para um tipo de empresa.

Protocolos	Protocolo de autenticação suportado na rede de destino
TLS	Ativar / desativar a utilização
TTLS	Ativar / desativar a utilização
Autenticações internas	Protocolo de autenticação que deve ser utilizado: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Ativar / desativar a utilização
PEAP	Ativar / desativar a utilização
EAP-FAST	Ativar / desativar a utilização
EAP-SIM	Ativar / desativar a utilização
Utiliza o PAC	Utilização do PAC (Controlo de Acesso Protegido)
Provisão PAC	Configuração do PAC de provisão
Provisiona a PAC de forma anónima	Fornecimento anónimo de CAP
Autenticação	
Nome de utilizador	Nome de utilizador de autenticação
Não utilizes Por ligação Palavra-passe	Não utilizes a palavra-passe por ligação
Palavra-passe	A palavra-passe a utilizar
Certificado de identidade	Carrega/selecciona o certificado de autenticação
Identidade exterior	Identidade que pode ser vista externamente
Confia	
Certificado de confiança 1	Carrega o primeiro certificado de confiança
Certificado de confiança 2	Carrega o segundo certificado de confiança
Certificado de confiança 3	Carrega o terceiro certificado de confiança
Servidor de confiança Nomes de certificados	Os nomes dos certificados de servidor esperados (numa lista separada por vírgulas)

VPN

Dependendo do tipo de ligação selecionado, podem estar visíveis campos diferentes.

Nome da ligação	Nome do perfil VPN
Tipo de VPN	
VPN	Todo o tráfego de rede do dispositivo será encaminhado através de uma ligação VPN.
Tipo de ligação	Estabelece o tipo de ligação VPN
IPsec (cisco)	Protocolo IPsec da cisco
L2TP	Protocolo L2TP
SSL personalizado	Ligação através de SSL personalizado
IKEv2	Protocolo IKEv2
Configuração de proxy	Configuração de um Proxy para a ligação VPN
Não tens	Não estabelecer um proxy
Manual	Estabelece manualmente um Proxy
URL do servidor proxy	Endereço para aceder às definições de proxy
Porto	Estabelece a porta para o Proxy
Autenticação	Nome de utilizador para a autenticação no Proxy
Palavra-passe	Palavra-passe para a autenticação no Proxy
Automático	Estabelece um Proxy automaticamente
URL do servidor proxy	URL para aceder às definições de Proxy

Proxy HTTP

Tipo de proxy	
Manual	Estabelece um Proxy manualmente
URL do servidor proxy	Endereço de acesso às definições de proxy
Porto	Estabelece a porta proxy
Autenticação	Nome de utilizador para a autenticação no Proxy
Palavra-passe	Palavra-passe para a autenticação no Proxy
Automático	Estabelece um Proxy automaticamente
URL do PAC de proxy	URL do PAC de proxy
Permite a ligação direta se o PAC não estiver acessível	Permite a ligação direta (sem VPN), se o PAC não estiver acessível
Permite contornar o proxy para aceder a redes cativas	Permite contornar o proxy para aceder a redes internas cativas

AirPrint

Endereço IP	Endereço IP da impressora
Caminho de recursos	Caminho definido para o dispositivo AirPrint

AirPlay

Nome do dispositivo	Nome do dispositivo
Palavra-passe	Palavra-passe de emparelhamento
Lista branca	Define uma lista de dispositivos, com os quais o dispositivo pode emparelhar-se exclusivamente

Gestão PIM

Exchange Active Sync

Nome da conta	Nome da conta.
Endereço de correio eletrónico	O endereço da conta (por exemplo, max@company.com)
Nome de anfitrião do servidor	Nome de anfitrião interno
Nome de utilizador	Os campos "Domain" e "Login Name" devem estar em branco para que o aparelho solicite o utilizador.
Domínio	Os campos "Domain" e "Login Name" devem estar em branco para que o aparelho solicite o utilizador. Se uma ACL Gateway Configuration estiver activada e o campo Domain não estiver vazio, o AppTec360 Universal Gateway autenticará o dispositivo com o seguinte nome "Domain\Login Name"
Palavra-passe	A palavra-passe da conta (por exemplo, secretUserPassword)
Dias anteriores do Mail to Sync	O número de dias anteriores de correio a sincronizar
Utiliza SSL	Utiliza SSL para o anfitrião interno do Exchange
Opção avançada	Mostrar opções avançadas
Porta do servidor	Porta interna
Caminho do servidor	Caminho interno
Nome de anfitrião externo	Anfitrião externo
Porta externa	Porta externa
Caminho externo	Caminho externo
Utiliza SSL para o exterior Anfitrião de intercâmbio	Utiliza SSL para o anfitrião externo do Exchange

eMail

Configuração de contas POP3 / IMAP no dispositivo do utilizador final

Descrição da conta	Nome das contas de e-mail
Tipo de conta	
IMAP	
Prefixo do caminho	O prefixo do caminho para pastas especiais
POP	
Nome de exibição do utilizador	Nome de apresentação do utilizador
Endereço de e-mail	Endereço de correio eletrónico do utilizador

Correio de entrada	Definições do servidor de entrada
Endereço do servidor de correio eletrónico	Endereço do servidor de correio eletrónico
Porta do servidor de correio	Porta do servidor de correio
Nome do utilizador	Nome do utilizador correspondente
Tipo de autenticação	Tipo de autenticação
Não tens	Não Tipo de autenticação
Palavra-passe (apenas ao nível do aparelho)	Solicitação da palavra-passe
Desafio-Resposta MDM	
NTLM	NTLM-Autenticação
HTTP MD5 Digest	
Utiliza SSL	Utiliza SSL, se necessário

Correio de saída	Definições do servidor de saída
Endereço do servidor de correio eletrónico	Endereço do servidor de correio eletrónico
Porta do servidor de correio	Porta do servidor de correio
Nome do utilizador	Nome do utilizador correspondente
Tipo de autenticação	
Não tens	Nenhum método de autenticação
Palavra-passe (apenas ao nível do aparelho)	Solicitação da palavra-passe
Desafio-Resposta MDM	
NTLM	NTLM-Autenticação
HTTP MD5 Digest	
Utiliza SSL	Utiliza SSL, se necessário
Senha de saída igual à de entrada	Senha de saída igual à de entrada
Utiliza apenas no correio	Ativar, se todas as mensagens de correio eletrónico de saída tiverem de ser enviadas através da aplicação de correio eletrónico

CalDav

Configura a instalação e a distribuição de uma conta CalDav

Descrição da conta	Nome de exibição da conta
Nome do anfitrião	Nome do anfitrião e/ou endereço IP
Porto	Porta da conta CalDav
URL principal	URL principal da conta
Nome de utilizador	Nome de utilizador CalDav correspondente
Palavra-passe (apenas ao nível do aparelho)	Respectiva palavra-passe CalDav
Utiliza SSL	Utiliza SSL, se necessário

CardDav

Configura a criação e distribuição de uma conta CardDav

Descrição da conta	Nome de exibição da conta
Nome do anfitrião	Nome do anfitrião e/ou endereço IP
Porto	Porta da conta CardDav
URL principal	URL principal da conta
Nome de utilizador	Nome de utilizador do respetivo CardDav
Palavra-passe (apenas ao nível do aparelho)	Respectiva palavra-passe CardDav
Utiliza SSL	Utiliza SSL, se necessário

LDAP

Nesta área, configura uma ligação LDAP, de modo a permitir uma troca dinâmica de certificados entre o dispositivo do utilizador final e o Active Directory.

Tem em atenção que o utilizador selecionado necessita da respectiva permissão de leitura.

Descrição da conta	Descrição da conta
Nome de utilizador da conta	Utilizador para acesso LDAP
Palavra-passe da conta	Palavra-passe para o acesso LDAP
Nome de anfitrião da conta	Nome de anfitrião/endereço IP do servidor LDAP
Utiliza SSL	Utiliza SSL, se necessário

Na segunda parte, podes definir filtros individuais para pesquisar no registo LDAP.

Descrição	Âmbito de aplicação	Pesquisa na base
Descrição do filtro	Nível de pesquisa no registo LDAP	Define o filtro individual

Painel de controlo e relatórios

Definições do painel de controlo

Aqui podes ver quais os painéis existentes, editá-los ou criar novos painéis. Cada Dashboard tem o seu próprio conjunto de dados para mostrar e configuração de gráficos.

Controlo das definições do painel de controlo

Público	Define o Painel como público, para que outros utilizadores possam ver o Painel. É claro que os utilizadores têm de poder iniciar sessão e ver os Dashboards. Se "Público" não estiver ativado, só o criador o pode ver.
Predefinição	Define o Dashboard como predefinido para que seja aberto automaticamente da próxima vez que acederes à Vista do Dashboard.
	Mostra o Dashboard e os seus gráficos
	Eliminar o painel de controlo
	Editar o nome do painel e as definições
	Faz uma cópia do Dashboard
	Adiciona um painel de controlo completamente novo

Vista do painel de controlo

Mostra os dados e os gráficos do painel selecionado e também permite que os alteres.

Controlo do painel de controlo

	Permite-te definir os dados que são mostrados no Dashboard, a quantidade de dados a mostrar e o tamanho em que esses dados devem ser mostrados
	Leva-te de volta à Visão Geral do Painel
	Repõe a predefinição do Painel atualmente aberto
	Guarda todas as alterações que fizeste ao Painel atualmente aberto (por exemplo, quais os dados a mostrar)
	Altera o tipo de gráfico para gráfico de pilares
	Altera o tipo de gráfico para gráfico de pizza
	Altera o tipo de gráfico para gráfico de rosca
	Altera o tipo de gráfico para gráfico de área polar
	Altera a ordem de ordenação

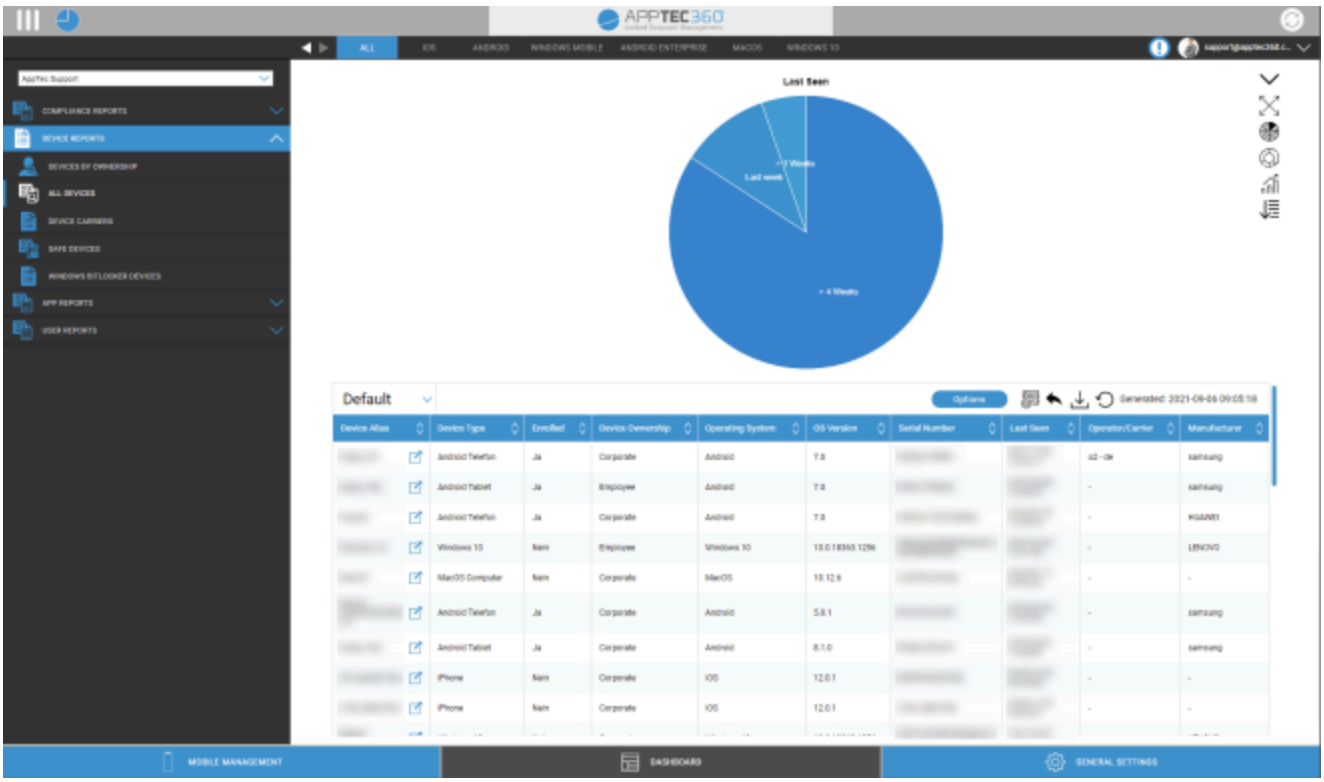
Relatórios alargados

O "Relatório alargado" oferece visões gerais e gráficos detalhados sobre as informações do dispositivo e do utilizador.

Existem alguns relatórios predefinidos, mas todos eles podem ser alterados manualmente para adicionar ou remover dados a mostrar.

Tem em atenção que só podes alterar manualmente os dados que são mostrados. A categoria de relatório selecionada define os dados em que se baseia. Por exemplo, nunca poderás ver dispositivos Android no relatório iOS em Relatórios de dispositivos Todos os dispositivos iOS

No canto superior esquerdo, podes limitar os dados do relatório a um determinado grupo (e a todos os seus subgrupos). Por predefinição, esta opção está definida para o teu nó raiz, pelo que tem em conta TODOS os dispositivos e utilizadores.



Controlo alargado de relatórios

Em cada síntese, é possível utilizar as seguintes funções para modificar o relatório da forma que se desejar:

	Esconde o gráfico (se o gráfico for apresentado)
	Mostra o gráfico (se o gráfico estiver oculto)
	Expande o gráfico (se o gráfico estiver recolhido)
	Recolhe o gráfico (se o gráfico estiver expandido)
	Altera o tipo de gráfico para gráfico de pilares
	Altera o tipo de gráfico para gráfico de pizza
	Altera o tipo de gráfico para gráfico de rosca
	Altera o tipo de gráfico para gráfico de área polar
	Altera a ordem de ordenação
	Modifica as seguintes partes da síntese exibida: • Adicionar/Remover colunas • Especifica a ordem pela qual as colunas são mostradas • Mostra/esconde o gráfico por cima da tabela • Selecciona a coluna que é utilizada para o gráfico • Filtra os dados da tua tabela
	Abre o gestor de configuração para guardar e carregar diferentes relatórios
	Repõe a predefinição do Relatório atualmente aberto
	Exportar o relatório atual como um ficheiro .csv
	Gera novamente os dados e recarrega o relatório atual

Podes encontrar uma lista de todos os relatórios predefinidos nas páginas seguintes.

Relatórios de conformidade

Dispositivos enraizados

Vê os dispositivos que foram enraizados/ jailbroken.

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Sistema operativo
Número de telefone
Visto pela última vez
Fabricante

Dispositivos em roaming

Visão geral de todos os dispositivos que estão em roaming

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Tipo de dispositivo
Sistema operativo
Número de telefone
Visto pela última vez

Dispositivos habilitados para roaming

Visão geral de todos os dispositivos que activaram o roaming, mas que não estão necessariamente em roaming.

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Tipo de dispositivo
Sistema operativo
Número de telefone
Visto pela última vez

Dispositivos supervisionados

Visão geral de todos os dispositivos que são supervisionados no modo supervisionado (apenas iOS)

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Tipo de dispositivo
Visto pela última vez

Dispositivos inactivos

Visão geral de todos os dispositivos que não se ligaram ao servidor nos últimos 7 dias

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Tipo de dispositivo
Sistema operativo
Visto pela última vez

Relatórios de dispositivos

Dispositivos por propriedade

Aqui podes ver quantos dispositivos foram atualmente implementados como dispositivos empresariais (dispositivos empresariais) e dispositivos de funcionários (dispositivos privados).

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
Tipo de dispositivo
Propriedade do dispositivo
Sistema operativo

Todos os dispositivos

Aqui podes ver uma visão geral de todos os dispositivos com as informações mais importantes.

Colunas predefinidas deste relatório:

Apelido do dispositivo
Tipo de dispositivo
Inscrito
Propriedade do dispositivo
Sistema operativo
Versão do SO
Número de série
Visto pela última vez
Operador/Carrier
Fabricante

Suportes de dispositivos

Aqui podes ver uma visão geral sobre o operador (fornecedor de telemóveis).

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Sistema operativo
Versão do SO
Operador/Carrier

Dispositivos SAFE

Aqui podes ver uma visão geral dos dispositivos que utilizam a versão SAFE.

Uma vez que a vista geral e/ou o SAFE só está disponível para dispositivos Samsung, não verás os separadores habituais neste ponto.

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail
Tipo de dispositivo
Visto pela última vez
Versão SAFE

Dispositivos Windows BitLocker

Aqui podes ver uma visão geral dos dispositivos Windows que utilizam o BitLocker.

Colunas predefinidas deste relatório:

Apelido do dispositivo
Proprietário do dispositivo
E-Mail

Estado do BitLocker

Relatórios de aplicações

Aqui tens uma variedade de visões gerais sobre as aplicações. Em todos estes relatórios, podes clicar numa entrada para ver que versões estão instaladas nos dispositivos e com que frequência. Nesta vista, podes clicar novamente numa versão específica para veres quais os dispositivos que têm essa versão específica instalada.

Nota: Pode demorar algum tempo até o sistema obter informações actualizadas do dispositivo. Além disso, os relatórios não são actualizados a cada minuto. Poderás ter de ser paciente para ver o estado atual se acabaste de atribuir uma nova aplicação ou versão. O recarregamento manual do relatório forçará o relatório a mostrar os dados mais actualizados disponíveis

Aplicações instaladas

Aqui tens uma visão geral de todas as aplicações instaladas.

Colunas predefinidas deste relatório:

Nome	Nome da respectiva aplicação e/ou serviço
Identificador	ID definida da aplicação/serviço
Contagem total	Com que frequência esta aplicação/serviço foi instalada nos dispositivos dos utilizadores finais

Aplicações mais instaladas

Aqui tens uma visão geral das aplicações que foram mais instaladas.

Colunas predefinidas deste relatório:

Nome	Nome da respectiva aplicação e/ou serviço
Identificador	ID definida da aplicação/serviço
Contagem total	Com que frequência esta aplicação/serviço foi instalada nos dispositivos dos utilizadores finais

Aplicações obrigatórias

Aqui tens uma visão geral das aplicações obrigatórias (obrigatórias compulsivas).

Colunas predefinidas deste relatório:

Nome	Nome da respectiva aplicação e/ou serviço
Identificador	ID definida da aplicação/serviço
Fonte da aplicação	Qual é a AppStore envolvida: • Google PlayStore (Android) • iTunes AppStore (iOS)
SO	Sistema operativo

Aplicações na lista negra

Aqui tens uma visão geral de todas as aplicações definidas na lista negra.

Colunas predefinidas deste relatório:

Nome	Nome da respectiva aplicação e/ou serviço
Identificador	ID definida da aplicação/serviço
Fonte da aplicação	Qual é a AppStore envolvida: • Google PlayStore (Android) • iTunes AppStore (iOS)
SO	Sistema operativo

Relatórios de utilizadores

Tarifa

Aqui tens uma visão geral das tarifas telefónicas e dos cartões SIM dos teus utilizadores.

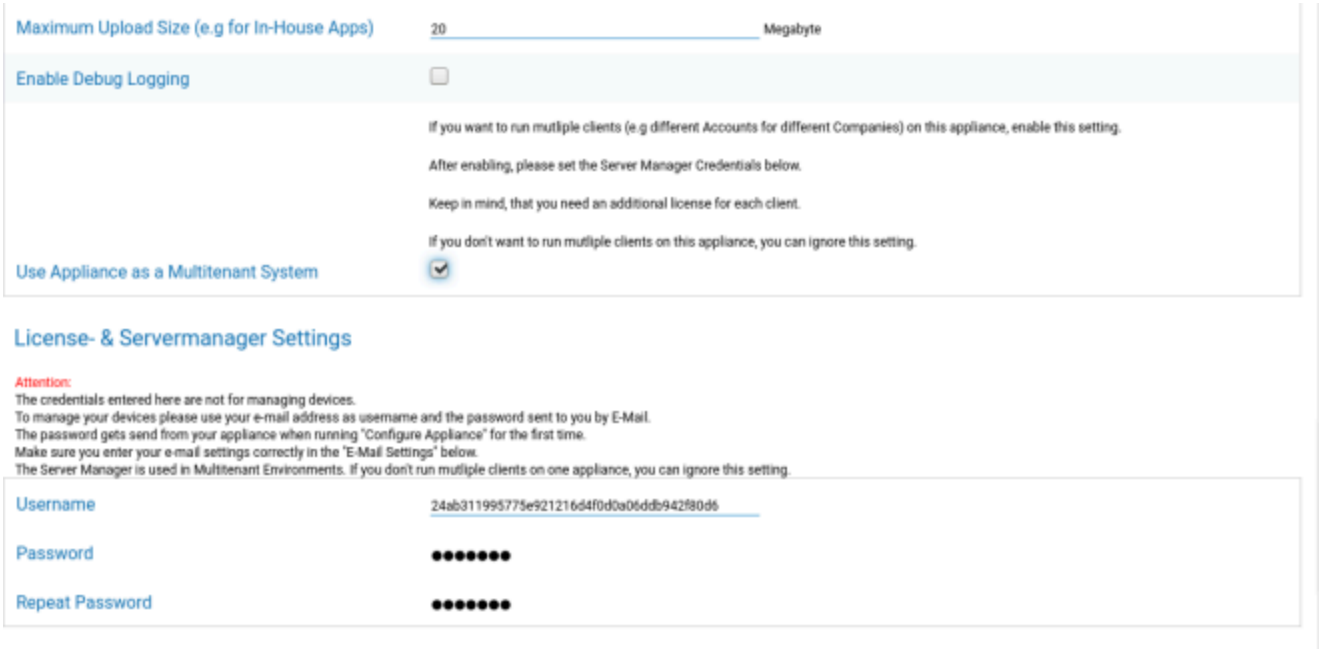
Colunas predefinidas deste relatório:

E-Mail
Nome
número de telefone
transportadora
tarifa
opção
preço
contratoCancelado
início do contrato
duranteTempo
mobileAndData
dadosVolume
multiSIM
tipo
simCardSerial1
simCardSerial2
simCardSerial3
pino1
pino2
puk1
puk2
nota

Gestão de multilocatários

O AppTec360 EMM é capaz de alojar vários inquilinos separados, cada um com os seus próprios utilizadores e grupos, permissões e definições globais.

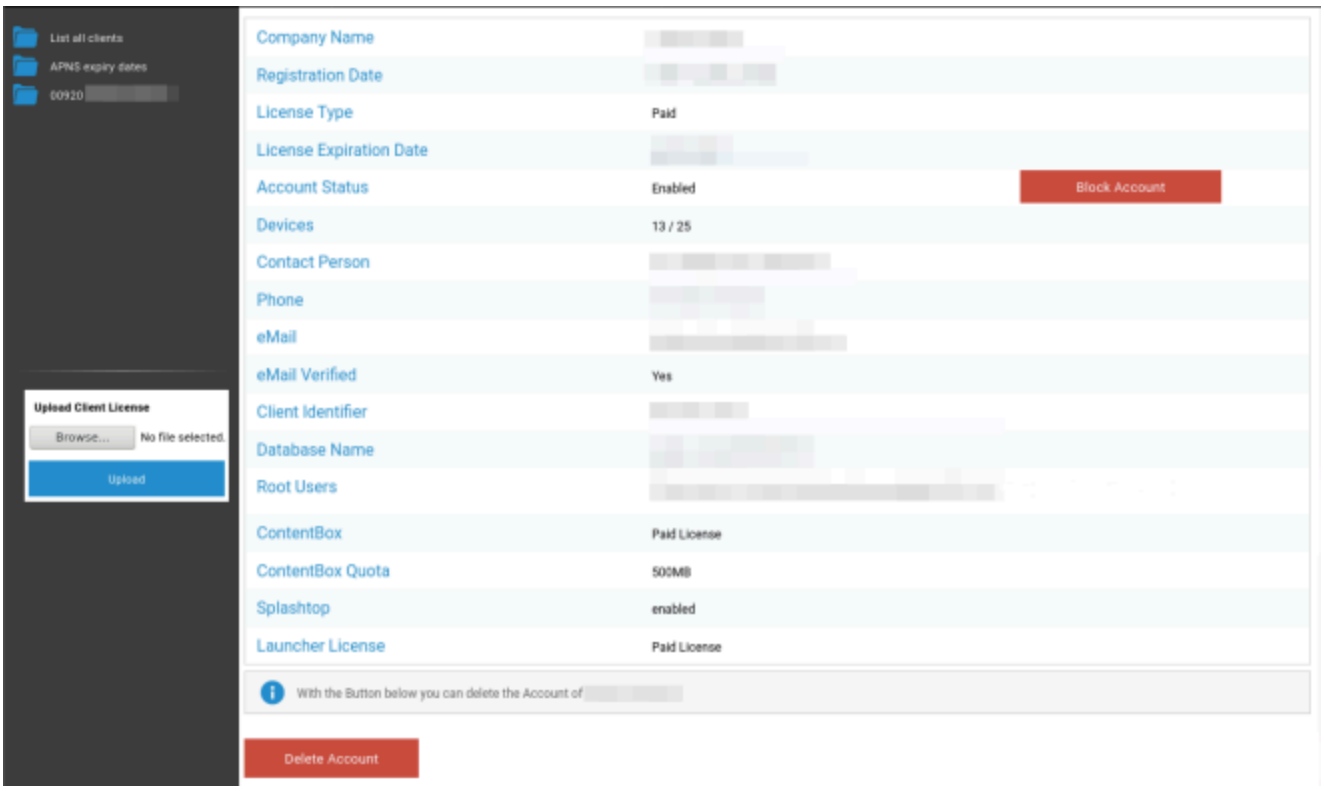
Para ativar as capacidades Multitenant, tens de as ativar na interface de configuração da Appliance no "Passo Três - Definições do Servidor".



No novo menu, define um nome de utilizador e uma palavra-passe para o Gestor de servidor. Guarda as definições e executa "Configurar aparelho" no "Passo 5 - Contrato de licença" para aplicar a definição.

Quando a configuração estiver concluída, podes iniciar sessão com as credenciais definidas através da interface normal do Mobile Management.

Depois de iniciares sessão, podes ver a seguinte vista.



À esquerda, podes ver todos os inquilinos (neste caso, apenas um com o ID 920) e, à direita, as informações sobre este cliente. Também tens a opção de bloquear o acesso à conta, bem como de eliminar o cliente (ATENÇÃO: isto irá remover todos os dados relacionados com esse cliente).

À esquerda, podes carregar uma nova licença de cliente, que pode ser uma atualização de licença para um cliente existente ou uma nova licença que cria automaticamente um novo cliente. Quando é criado um novo cliente, é enviado automaticamente um e-mail com a palavra-passe de início de sessão para o endereço de e-mail para o qual a licença foi emitida.

Para obter uma licença de cliente nova ou actualizada (por exemplo, se precisar de mais licenças de dispositivos), contacta o teu representante de vendas.

Vistas adicionais

Lista todos os clientes

Mostra uma visão geral sobre todos os clientes no sistema.

ID do cliente	ID do cliente
Identificador	Identificador de cliente
Base de dados	Base de dados
Nome da empresa	Nome da empresa
eMail	Pessoa de contacto eMail
Verificado	Se o eMail da pessoa de contacto é verificado ou não
País	País
Dispositivos	Número de dispositivos registados
Data de registo	Ponto no tempo da atribuição de licença
Último login	Último login na conta de administrador
Licença	Mostra o tipo de licença (Gratuita|Paga)
Licença CB	Tipo de licença da ContentBox (Gratuita|Paga)
Estado	Estado atual do AppTec-Client
Expirado	Mostra, se a licença tiver expirado
iOS	Número de dispositivos iOS
Android	Número de dispositivos Android
Windows Mobile	Número de dispositivos Windows Mobile
MacOS	Número de dispositivos MacOS
Windows 10	Número de dispositivos Windows 10
Android Enterprise	Número de dispositivos Android para empresas
IOS BYOD (registo de utilizadores)	Número de dispositivos IOS BYOD (registo de utilizadores)
IoT	Número de dispositivos IoT

Datas de validade do APNS

Mostra uma visão geral das datas de expiração de todos os certificados APNS de todos os clientes.

ID do cliente	ID do cliente
Nome da empresa	Nome da empresa
Data de expiração	Data de expiração do certificado APNS da Apple
Informação	Informações sobre a expiração

Contacto

Tens mais perguntas? Contacta-nos através de:

Para questões técnicas gerais

support@apptec360.com

+41 61 511 3210

Para questões relacionadas com a instalação de um aparelho virtual

consulting@apptec360.com

+41 61 511 3214

Isenção de responsabilidade