AppTec360 Enterprise Mobile Manager e ContentBox

Manuale di amministrazione | Versione 5.0 (202110)

Sommario

- Sicurezza SecurePIM
- Browser SecurePIM
- Scambio

Gestione delle connessioni

- Wi-Fi
  - Configurazione del proxy
  - Tipo di sicurezza
- VPN
  - Tipo di VPN
    - VPN
    - VPN per app
  - Configurazione del proxy
- APN
- Cellulare
- Proxy HTTP
- AirPrint
- AirPlay

Gestione del PIM

- Sincronizzazione attiva di Exchange
- eMail
  - Posta in arrivo
  - Posta in uscita
- CalDav
- Calendari sottoscritti
- LDAP

Gestione del web

- Webclips
- Filtro dei contenuti web

Gestione delle app

- Enterprise App Manager
  - Applicazioni installate (solo a livello di dispositivo)
  - Applicazioni obbligatorie
    - Opzioni di installazione
  - Applicazioni web

- Restrizioni e impostazioni
  - Applicazioni nella lista nera/bianca
  - Restrizioni della SysApp
  - App-VPN
  - Impostazioni dell’app
- App Store aziendale
  - Applicazioni iTunes
  - In-house
- Modalità chiosco
  - Tipo di applicazione
    - Pacchetto
    - URL
  - Impostazioni della modalità Kiosk

Android Enterprise – Configurazione dei dispositivi completamente gestita

Generale

- Panoramica del profilo del gruppo (solo a livello di gruppo)
- Panoramica del dispositivo (solo a livello di dispositivo)
- Revisione della configurazione (solo a livello di dispositivo)
- Registro del dispositivo (solo a livello di dispositivo)
  - Registro dei comandi
  - Possibili stati del comando
- Impostazioni del dispositivo
  - Configurazione del cliente
  - Carta da parati

Gestione delle risorse (solo a livello di dispositivo)

- Info sul dispositivo
  - Wi-Fi
- Cellulare
- Bluetooth

Gestione della sicurezza

- Antifurto (solo a livello di dispositivo)
  - Informazioni GPS (solo a livello di dispositivo)
  - Pulisci e blocca (solo a livello di dispositivo)

- Pulisci e blocca (solo a livello di dispositivo)
- Messaggio (solo a livello di dispositivo)
- Configurazione della sicurezza
  - Codice di accesso
  - Crittografia
  - AntiVirus
- Fine vita (solo a livello di dispositivo)
  - Pulisci (solo a livello di dispositivo)
- Impostazioni di restrizione
  - Restrizioni
  - Proprietario del dispositivo AE

Contenitore BYOD

- Android Enterprise
  - Android Enterprise
  - Scambio Gmail
  - Applicazioni del sistema AE
  - Codice di accesso al contenitore
- Samsung KNOX
  - Attivazione
  - Codice di accesso Knox
  - Knox Security
  - Scambio Knox
  - Knox eMail
  - Applicazioni Knox

Gestione delle connessioni

- Wifi
  - Tipo di sicurezza
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Restrizioni
- APN
- Bluetooth

Gestione del PIM

- Scambio
- eMail
- AE Gmail Exchange

Gestione delle app

- Enterprise App Manager
  - Applicazioni installate (solo a livello di dispositivo)
  - App di sistema (solo a livello di dispositivo)
  - Applicazioni obbligatorie
  - Applicazioni del sistema AE
- Restrizioni e impostazioni
  - Black- e Whitelisting
  - Restrizioni delle applicazioni di sistema
    - Applicazioni Samsung
    - Applicazioni Huawei
  - Impostazioni di gestione delle app
- App Store aziendale
  - Playstore
  - In-house
- Play Store aziendale
- Modalità chiosco e launcher
  - Modalità chiosco
  - AppTec360 Launcher
  - Impostazioni di AppTec360

Telecomando

- Splashtop
- Teamviewer

Gestione dei contenuti

- Contentbox
- Browser sicuro

Configurazione PC Windows 10

Generale

- Panoramica del profilo del gruppo (solo a livello di gruppo)
- Panoramica del dispositivo (solo a livello di dispositivo)
- Impostazioni

Panoramica generale

Introduzione ad AppTec360

La soluzione Enterprise-Mobile-Management di AppTec offre la possibilità di gestire e configurare tutti i dispositivi mobili con la sua intuitiva console di gestione. In questo scenario, il server EMM può essere eseguito nel tuo ambiente oppure puoi utilizzare la nostra soluzione basata sul cloud.

Anche per quanto riguarda l'installazione centralizzata delle applicazioni aziendali sugli smartphone, sei nel posto giusto. Con Enterprise Mobile Manager puoi distribuire applicazioni e documenti aziendali sui dispositivi in pochi secondi o bloccare le applicazioni indesiderate con white/blacklist.

L'utilizzo di dispositivi privati nelle aziende rappresenta una nuova sfida per la sicurezza di smartphone e tablet. Dato che i dipendenti vogliono utilizzare sempre più spesso i loro smartphone, gli amministratori IT devono proteggere un gran numero di dispositivi di vario tipo. Ti aiuteremo a proteggere tutti i dispositivi e i dati sensibili che vi sono memorizzati e a gestirli da una console intuitiva.

Sistemi operativi dei dispositivi supportati

AppTec360 offre supporto per dispositivi iOS, Android e Windows. Tieni presente che le capacità funzionali delle piattaforme citate possono essere diverse da un sistema operativo all'altro.

- Apple iOS 11.0 o superiore*
- Apple macOS 10.11 o superiore
- Google Android 4.4 o superiore** sulla versione Cloud
- Google Android 4.1 o superiore** sulla versione OnPrem
- MS Windows 10 o superiore*** (computer desktop, notebook e tablet)

**Si prega di notare che i dispositivi con iOS 10 o precedenti non possono essere registrati a causa delle drastiche modifiche apportate da Apple al processo di registrazione.*

***I dispositivi possono essere collegati e configurati anche se utilizzano una versione non più supportata dal produttore. Tieni presente che potrebbero esserci delle funzioni che richiedono una determinata versione di Android. Nei casi di assistenza, seguiamo il supporto ufficiale del produttore. In caso di problemi o bug causati da una versione obsoleta e non più supportata dal produttore, ci riserviamo il diritto di offrire un'assistenza limitata.*

****La versione Home di Windows non è supportata a causa delle limitazioni del sistema operativo. Ti consigliamo di utilizzare una versione del sistema operativo ancora supportata dal produttore. Non solo per la compatibilità, ma anche per motivi di sicurezza. Per questo motivo consigliamo iOS 12 o superiore e Android 9 o superiore.*

Directory LDAP supportate

- Microsoft Active Directory
- Aprire LDAP

Informazioni aggiornate sui "Sistemi operativi dei dispositivi supportati" e sulle "Directory LDAP supportate" sono disponibili qui:

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

Spiegazione della “modalità supervisionata” sui dispositivi Apple

La modalità supervisionata rappresenta un'interfaccia ampliata per i dispositivi iOS.

Sul dispositivo rispettivamente configurato, possono essere applicate ulteriori limitazioni relative alla funzionalità del dispositivo dell'utente finale. Questi sono contenuti anche nel manuale dell'amministrazione e sono contrassegnati da un banner.

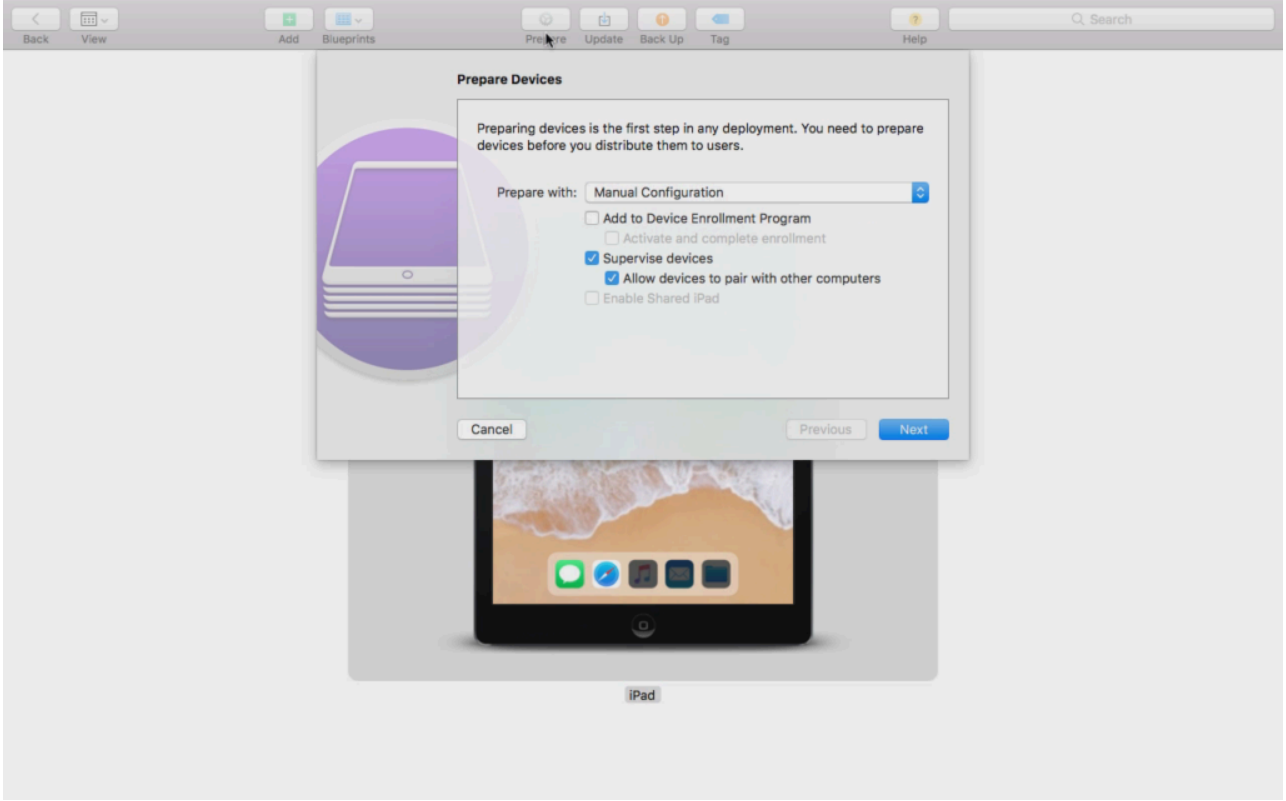
Disponibile in modalità supervisionata

La "modalità supervisionata" può essere attivata con il programma "Apple Configurator". Il Configuratore Apple può impostare le impostazioni predefinite dei nuovi dispositivi iOS come strumento di configurazione (tramite l'interfaccia USB).

Lo strumento non solo può installare profili di configurazione, ma anche applicazioni. È gratuito, ma richiede un computer Mac.

Attiva la modalità supervisionata

1. Apri il Configuratore Apple



2. Clicca sul dispositivo e scegli "Prepara".
3. Scegli "Configurazione manuale" e "Supervisione dei dispositivi".
4. Clicca su "Avanti".
5. (Opzionale) Ora puoi aggiungere un server MDM dove il dispositivo verrà iscritto. Il link si trova in "Impostazioni generali - Configurazione iOS - Configuratore e URL" Scegli la tua Organizzazione o creane una nuova
6. Scegli la tua Organizzazione o creane una nuova
7. Scegli quali sono i passaggi da saltare nella configurazione iniziale e clicca su "Avanti" (ATTENZIONE: se procedi, il tuo dispositivo verrà cancellato).

Ora il tuo dispositivo verrà messo in modalità supervisionata. Questa operazione può richiedere alcuni minuti. Al termine, il dispositivo si riavvierà.

Ora il tuo dispositivo è supervisionato!

Aggiungere un dispositivo al DEP

Puoi anche aggiungere i dispositivi al DEP (Device Enrollment Programm) utilizzando il Configuratore Apple, se i tuoi dispositivi sono su iOS 11 o superiore.

Ulteriori informazioni su DEP: https://www.apple.com/business/dep/

Segui la stessa procedura che segui per supervisionare un dispositivo e in più seleziona "Aggiungi al programma di registrazione del dispositivo". Ti verranno richiesti i dati di accesso al DEP se non hai mai effettuato l'accesso al DEP con il Configuratore Apple.

Al termine del processo, il dispositivo può essere trovato nel Server DEP "Dispositivi aggiunti da Apple Configurator 2". Ora puoi utilizzare questo server e collegarlo alla console di gestione o trasferire il dispositivo a un server già esistente.

Hai aggiunto con successo un dispositivo al DEP!

Spiegazione di Android Enterprise

Che cos'è Android Enterprise?

Android Enterprise offre un migliore controllo dei dispositivi di lavoro gestiti con un MDM. Questo permette agli amministratori di avere il pieno controllo sui dispositivi Android o di separare i dati aziendali da quelli privati sui dispositivi container. Inoltre, Android Enterprise consente una più semplice registrazione dei dispositivi e una facile distribuzione delle app.

Quali sono i requisiti per utilizzare Android Enterprise?

Android Enterprise può essere utilizzato gratuitamente da tutti. Per abilitare tutte le funzioni di Android Enterprise è sufficiente collegare un account Google all'MDM. Per saperne di più, consulta la sezione Android Enterprise.

Android Enterprise può essere utilizzato su dispositivi con Android 5.1 o superiore, ad eccezione di Enhanced Work Profile (vedi sotto). Raccomandiamo almeno Android 7 o superiore per facilitare l'iscrizione o Android 11 per utilizzare tutte le funzioni disponibili.

Quali sono le modalità disponibili con Android Enterprise?

Ci sono 3 diverse modalità da utilizzare quando si usa Android Enterprise.

Dispositivo AE completamente gestito (gestito per lavoro): Un dispositivo completamente gestito che viene utilizzato solo per lavoro. In questo modo l'amministratore ha il pieno controllo del dispositivo. Questo non consente un uso privato del dispositivo. Per iscrivere i dispositivi in questa modalità, è necessario resettare i dispositivi e iscriverli con un QR Code (vedi Iscrizione AE) o iscriverli tramite Knox Enrollment o Zero Touch.

Contenitore BYOD AE: Il contenitore BYOD (bring your own device) consente agli utenti di accedere ai dati aziendali sul proprio telefono privato in un contenitore separato. In questa modalità, le app private non possono vedere i dati e le app aziendali e viceversa. Per registrare i dispositivi in questa modalità, è necessario scaricare l'applicazione AppTec e scansionare un codice QR. Crea un dispositivo nella console e seleziona come tipo di dispositivo "Contenitore AE (BYOD & Profilo di lavoro Enahnced)". Clicca sul codice QR del nuovo dispositivo generato per ottenere il codice QR e imposta il primo interruttore su "Legacy & BYOD".

AE Enhanced Work Profile: (richiede Android 11 o superiore) Mentre il contenitore BYOD di cui sopra porta i dati aziendali su un dispositivo privato, l'Enhanced Work Profile fa lo stesso ma per un dispositivo di proprietà dell'azienda. Crea lo stesso contenitore, ma dà all'amministratore un po' più di controllo sul dispositivo, per cui l'utente non può semplicemente rimuovere l'MDM dal dispositivo. Crea un dispositivo nella console e seleziona come tipo di dispositivo "Contenitore AE (BYOD & Profilo di

lavoro Enahnced)". Clicca sul codice QR del nuovo dispositivo generato per ottenere il codice QR e imposta il primo interruttore su "Profilo di lavoro avanzato". Questo codice QR può essere scansionato dopo aver resettato il dispositivo e aver toccato 6 volte lo schermo come spiegato nel Metodo 1 in Iscrizione AE.

Come posso assegnare le app ai dispositivi Android Enterprise?

Per prima cosa devi approvare le app che vuoi utilizzare in Impostazioni generali → Gestione app → AE Play Store → Play Store Apps. Dopo aver approvato un'app puoi assegnarla all'elenco delle app obbligatorie → del tuo profilo cliccando sul "+" e selezionando l'app dalla scheda "AE Play Store". In questo modo l'applicazione verrà scaricata e installata automaticamente. Non è richiesto alcun account google sul dispositivo e l'utente non deve confermare o autorizzare questa operazione.

Carica le tue applicazioni sul Google Play Store

È possibile caricare le tue applicazioni interne sul Google Play Store. In questo modo potrai beneficiare di diversi vantaggi come il meccanismo di aggiornamento del Play Store.

Per farlo, hai bisogno di un account Google Developer. Accedi utilizzando Google Play Console(https://play.google.com/apps/publish)

Clicca su "Crea applicazione". Scegli la lingua predefinita e il titolo dell'applicazione.

Create application

Default language *

English (United Kingdom) – en-GB ▾

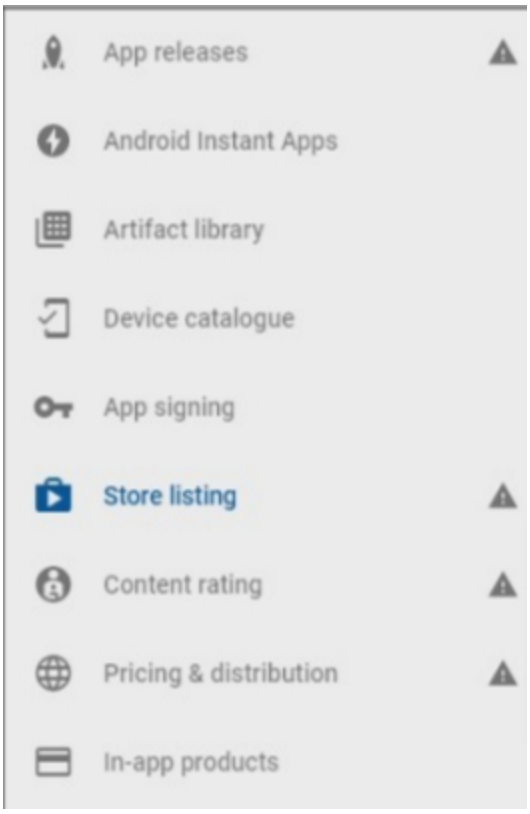
Title *

AppTec Demo App

15/50

CANCEL CREATE

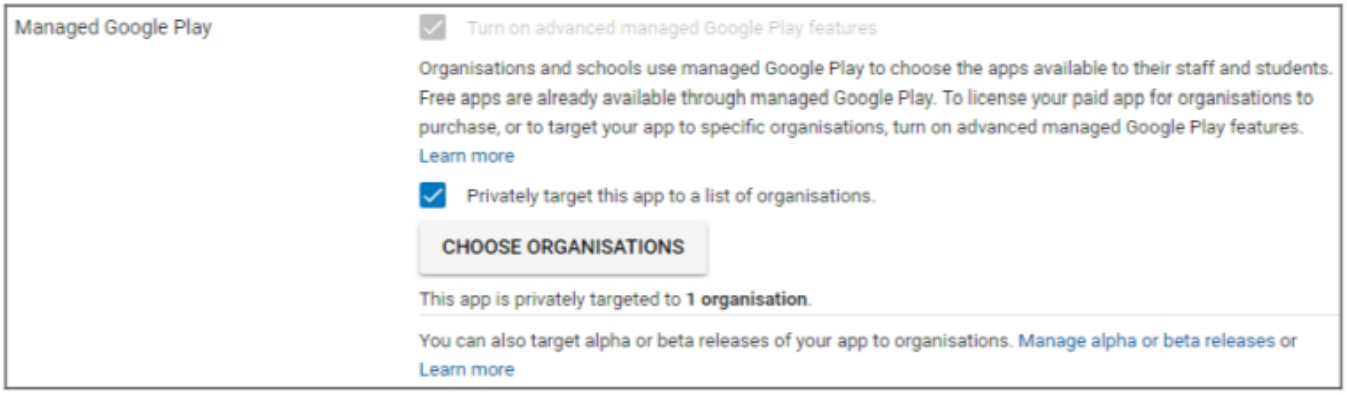
Nella pagina successiva ti verrà chiesto di inserire diversi dettagli sulla tua applicazione.



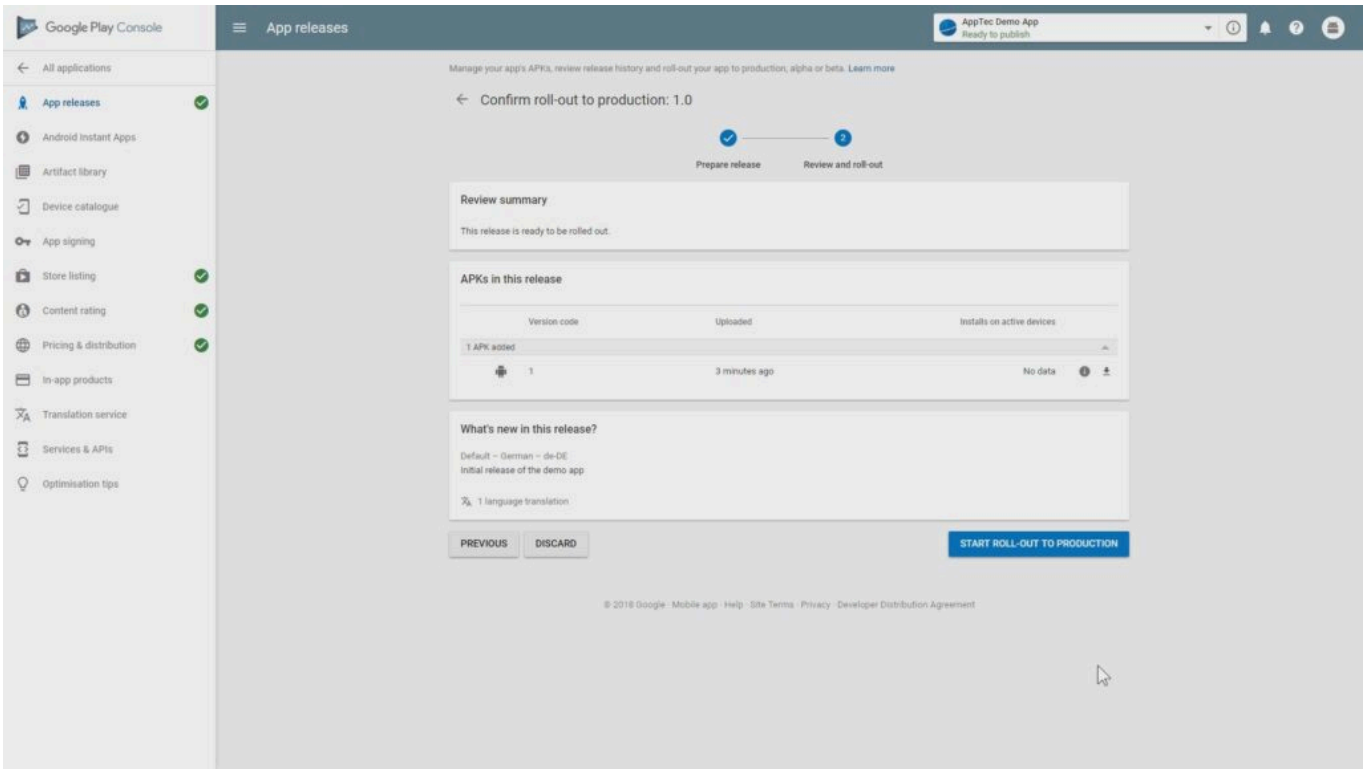
Dopo aver inserito tutti i dettagli, vedrai diversi simboli di suggerimento sul lato sinistro.

Passa il mouse su di essi per vedere quali passi sono rimasti e seguili nell'ordine che preferisci.

Nota: assicurati di selezionare le due caselle di controllo in "Managed Google Play" sotto "Pricing & Distribution". In caso contrario, l'app sarà pubblica e accessibile a tutti. Assicurati anche di scegliere la contea di distribuzione.



Dopo aver completato tutti i passaggi, puoi andare su "Rilascio dell'app". Clicca su "Review" e "Start Roll-Out to Production" per finalizzare la tua bozza e pubblicare l'app.



Ci vorrà un po' di tempo prima che l'applicazione sia disponibile sul Play Store. Al termine del processo, potrai cercare la tua app nello store Play for Work e approvarla. Dopodiché potrai semplicemente assegnare l'app ai dispositivi utilizzando la console EMM, proprio come fai con le altre app.

Requisiti e installazione

Requisiti

Requisiti di sistema

Il dispositivo virtuale è disponibile nel formato di virtualizzazione aperto (VMWare, VirtualBox, Citrix Xen Server) e come file compresso .vhdx (Hyper-V)*.

*Nota: la macchina deve essere creata con la Generazione 1 quando si utilizza Hyper-V.

Il disco virtuale ha una dimensione target di 20 GB e la macchina richiede 4 GB di RAM.

L'apparecchiatura è basata su Debian 9 64bit

Aggiorna la macchina importata alla compatibilità più recente (ad esempio in VMWare) e assicurati che il tipo di sistema operativo della macchina sia impostato correttamente nell'hypervisor.

Chiave di licenza

Per attivare e installare correttamente il server, è necessario disporre di un file di licenza valido. Puoi ottenerne uno direttamente da AppTec360 e/o dal tuo rivenditore di fiducia.

Risoluzione di indirizzi IP e DNS

L'appliance AppTec360 deve essere raggiungibile dal dispositivo utilizzando l'hostname per cui è stata rilasciata la licenza.

Per iscrivere i dispositivi Windows 10 devi anche impostare un sottodominio aggiuntivo sotto forma di "enterpriseenrollment.", che punta all'appliance.

Certificato SSL

Poiché tutte le connessioni da e verso i dispositivi devono essere protette tramite SSL, è necessario un certificato valido per il nome dell'host emesso da un'autorità di certificazione di cui il dispositivo si fida. La chiave privata del certificato deve essere caricata senza password. Nella maggior parte dei casi è necessario un certificato intermedio per la CA affinché i dispositivi riconoscano il certificato del server.

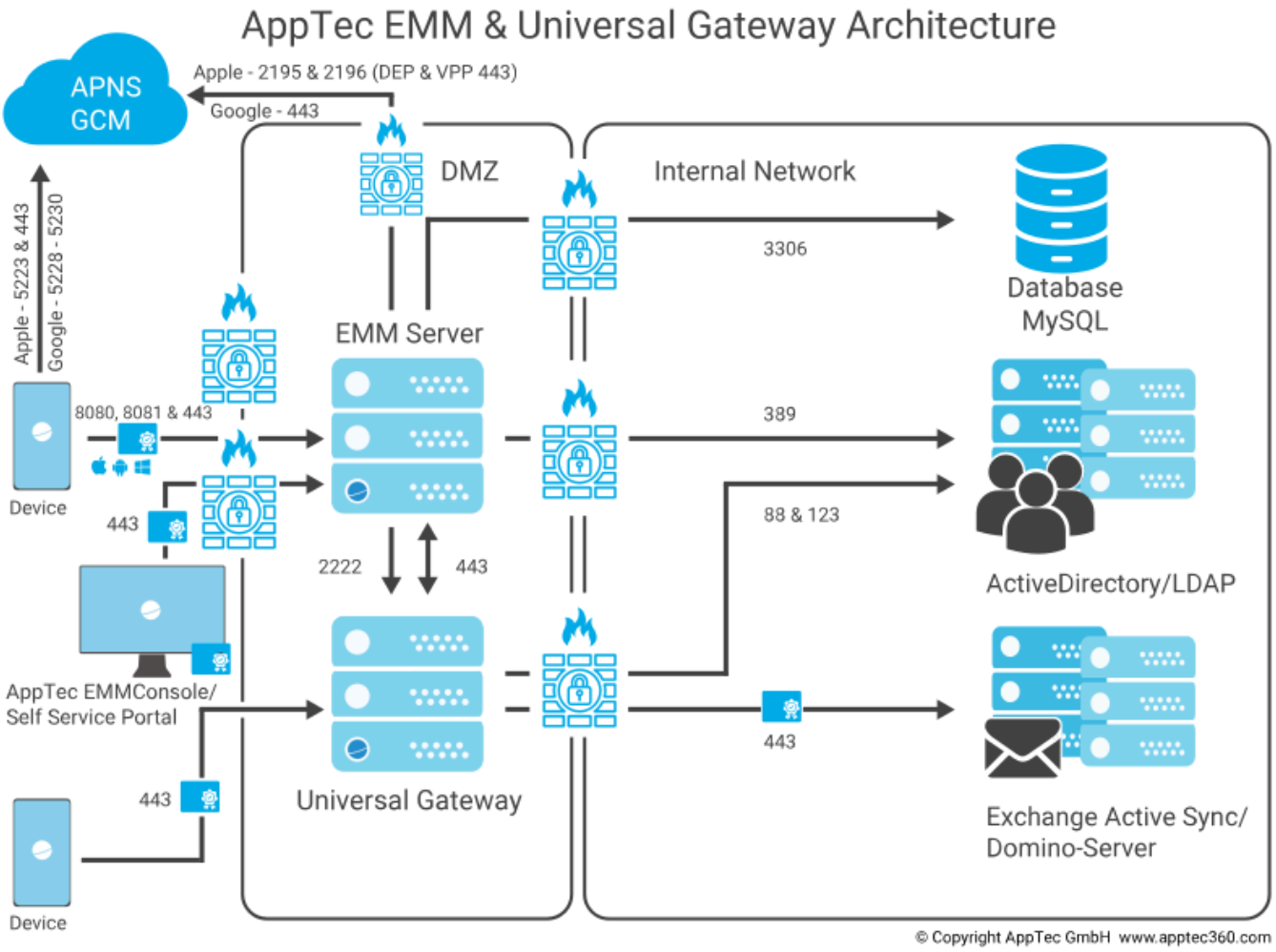
I dispositivi Windows 10 richiedono un certificato specifico per il sottodominio di iscrizione all'azienda.

A partire dalla versione 202104 dell'appliance puoi anche utilizzare i certificati Let's Encrypt, che vengono generati automaticamente (come descritto nel Passo 2 - Certificato SSL).

Server SMTP

È necessario un server di posta elettronica e/o un email-relay per consentire all'AppTec360 EMM di inviare e-mail (ad esempio per la registrazione del dispositivo e la convalida dell'account).

Regole del firewall



Questo diagramma mostra quale connessione è necessaria a seconda dei servizi che vuoi utilizzare.

Per una descrizione più dettagliata, consulta la tabella alla pagina successiva.

Qualsiasi (esterno/dispositivi)	→	**AppTec360 Appliance / emmconsole.com**
Porti	443	Gestione, AppStore aziendale e comunicazione con Windows Phone
	8080	Comunicazione Android e iOS
	80	Prima configurazione di Let's Encrypt. In seguito utilizza il 443.
Qualsiasi (Dispositivi)	→	**Qualsiasi (esterno)**
Porti	5223, 443	Apple Push Service, deve essere raggiungibile senza proxy, 443 come Fallback, vedi https://support.apple.com/en-us/HT203609
	5228-5230	Il servizio push di Android (FCM) deve essere raggiungibile senza proxy.
Apparecchio AppTec360	→	**Controllore di dominio**
Porti	389, (LDAPS 636)	Sincronizzazione degli utenti con LDAP
Apparecchio AppTec360	→	**Qualsiasi**
Porto	443	Utilizzato per il servizio push di Android (GCM) Ricerca su AppStore / Play Store
Apparecchio AppTec360	→	**emmconsole.com**
Porti	443	Aggiornamenti delle appliance AppTec360, generazione di certificati APNS
Apparecchio AppTec360	→	**Rete Apple (17.0.0.0/8)**
Porti	2195, 2196	Servizio Push di Apple e Servizio Feedback
	443	DEP E VPP

Aggiornamenti sulla sicurezza

Il sistema operativo Debian deve essere aggiornato regolarmente per ottenere le ultime correzioni di sicurezza. Tuttavia, assicurati di non aggiornare manualmente a una versione principale più recente di Debian. Quando AppTec360 EMM sarà compatibile con una versione principale più recente, aggiungeremo un modo per effettuare l'upgrade in un aggiornamento dell'appliance.

Password predefinite della Virtual Appliance

Utente di accesso (il login di root è disabilitato. Usa "sudo" per le attività di amministrazione)

apptec

Password di accesso

apptec

Utente root di MySQL

radice

Password di root di MySQL

apptec

Utente predefinito di MySQL

AppTec

Password utente predefinita di MySQL

AppTec

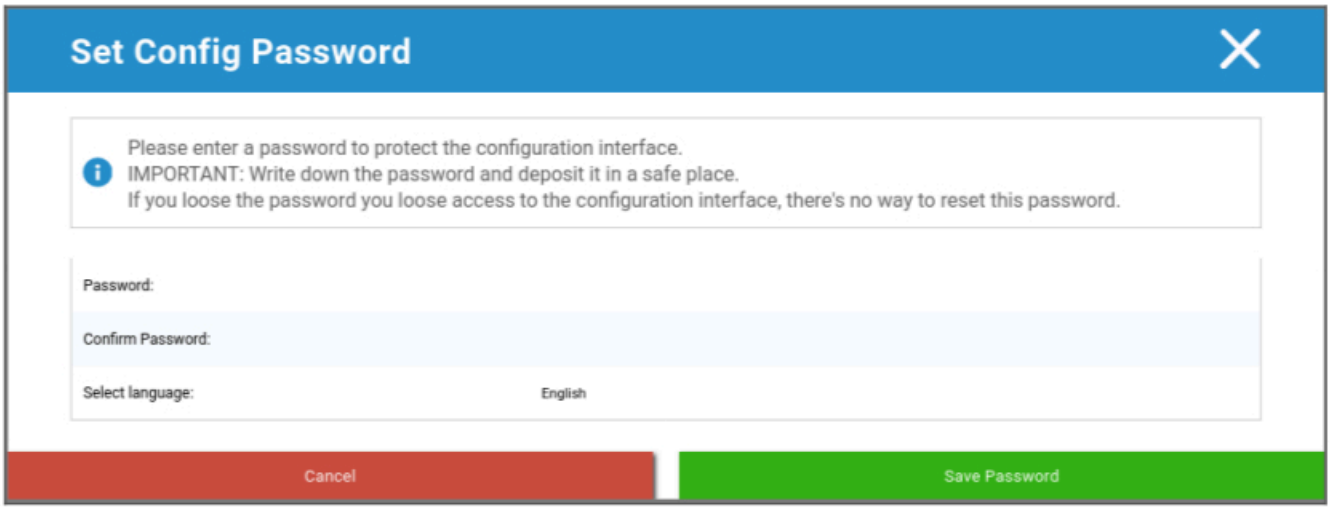
Configurazione della periferica virtuale

Importante: prima di iniziare la configurazione della Virtual Appliance, la risoluzione del display deve essere impostata ad almeno 1280 x 800 pixel.

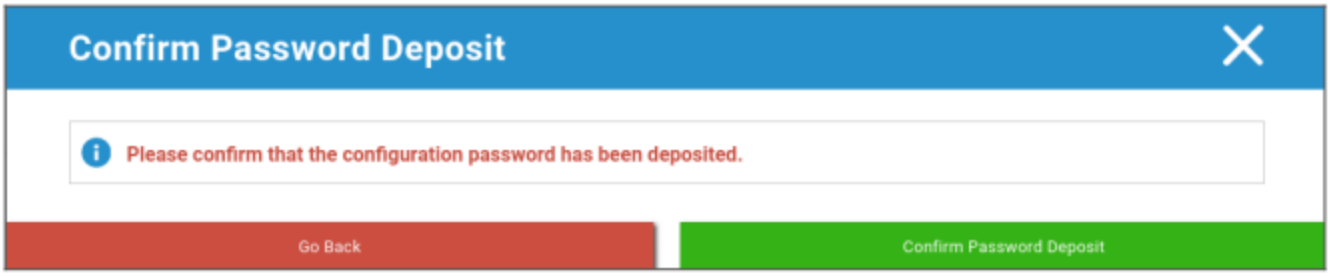
Dopo aver effettuato l'accesso all'appliance, Firefox dovrebbe avviarsi automaticamente e visualizzare l'interfaccia di configurazione.

Preparazione

Per prima cosa devi fornire una password per l'interfaccia di configurazione. Questa password viene utilizzata per criptare tutte le informazioni e i file inseriti nell'interfaccia di configurazione. Qui puoi anche impostare la lingua in cui deve essere visualizzata l'interfaccia (può essere modificata in seguito).

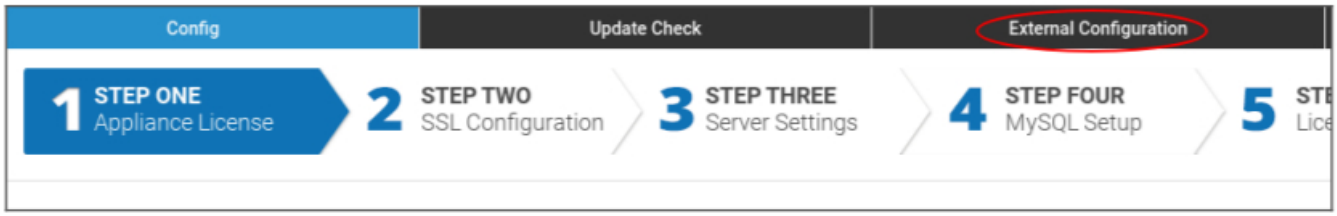


La password può essere reimpostata solo dal Supporto AppTec360, quindi assicurati di depositarla in un luogo sicuro e di confermare l'imminente popup.



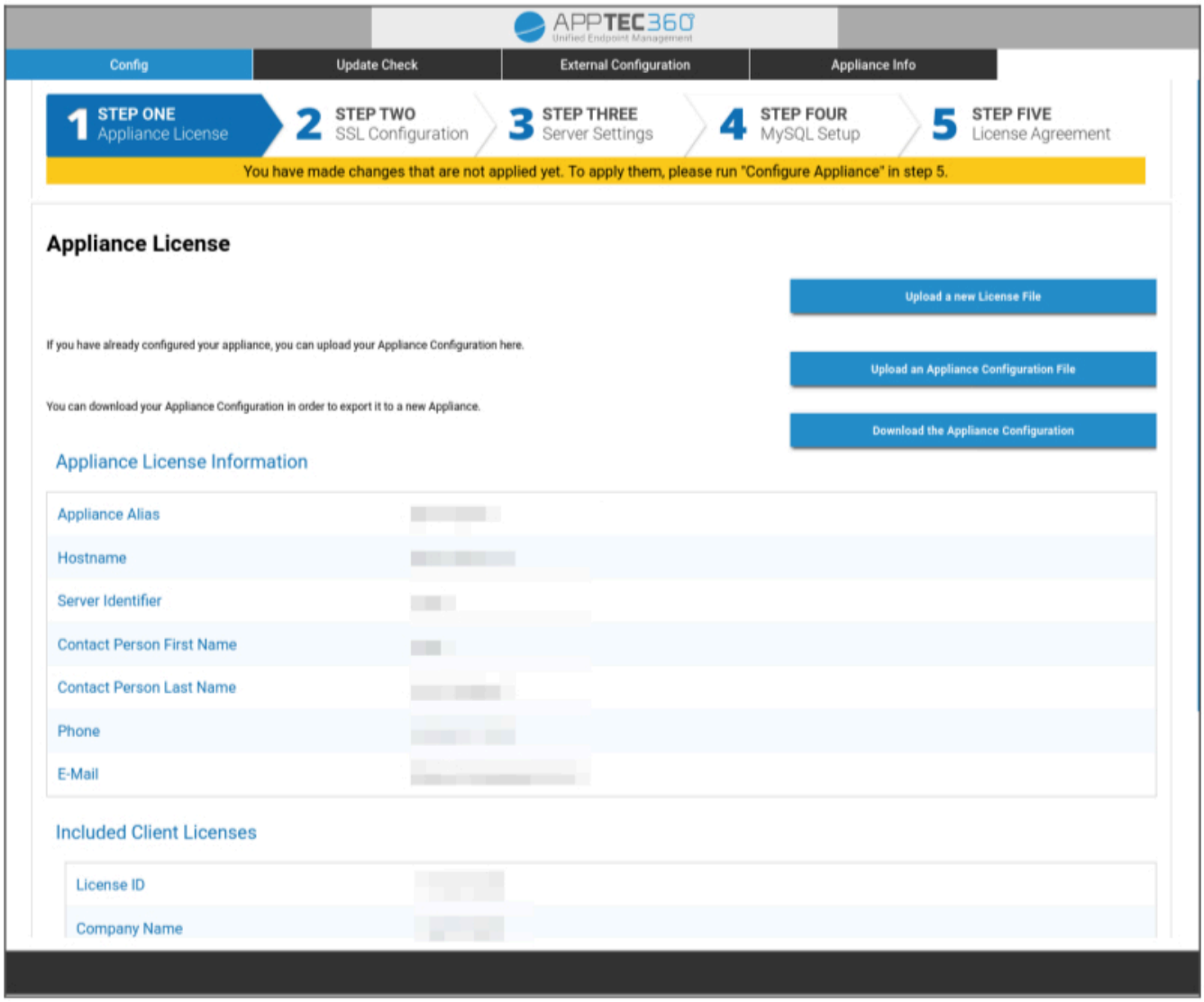
Configura da un host esterno

Per facilitare il processo di configurazione, puoi rendere la pagina di configurazione accessibile da remoto. Per farlo, segui la procedura descritta in "Configurazione da host esterno".



Primo passo – Licenza dell’apparecchio

1. Carica il file della licenza che hai ricevuto da AppTec.
2. Se il file di licenza è stato caricato correttamente, potrai vedere le informazioni sulla licenza dell'appliance come nella schermata seguente.



Secondo passo – Certificato SSL

Puoi utilizzare l'impostazione automatica dei certificati utilizzando Let's Encrypt oppure fornire tu stesso i certificati (per maggiori informazioni, vedi Certificato SSL).

Automatico

Il certificato verrà generato automaticamente utilizzando il servizio Let's Encrypt.

AppTec360 EMM utilizza la sfida HTTP-01 per la convalida del dominio, il che significa che la porta HTTP deve essere aperta da internet per la prima richiesta di un certificato. Le richieste di rinnovo successive possono essere convalidate tramite HTTPS.

Cambia i pulsanti di opzione in "Automatico (Let's Encrypt)" e premi "SALVA VALORI". Il certificato verrà richiesto automaticamente quando si applica la configurazione nel Passo 5 - Contratto di licenza. Il certificato verrà rinnovato automaticamente se necessario e riceverai un'e-mail se il certificato sta per scadere (il che implica che il rinnovo potrebbe essere fallito).

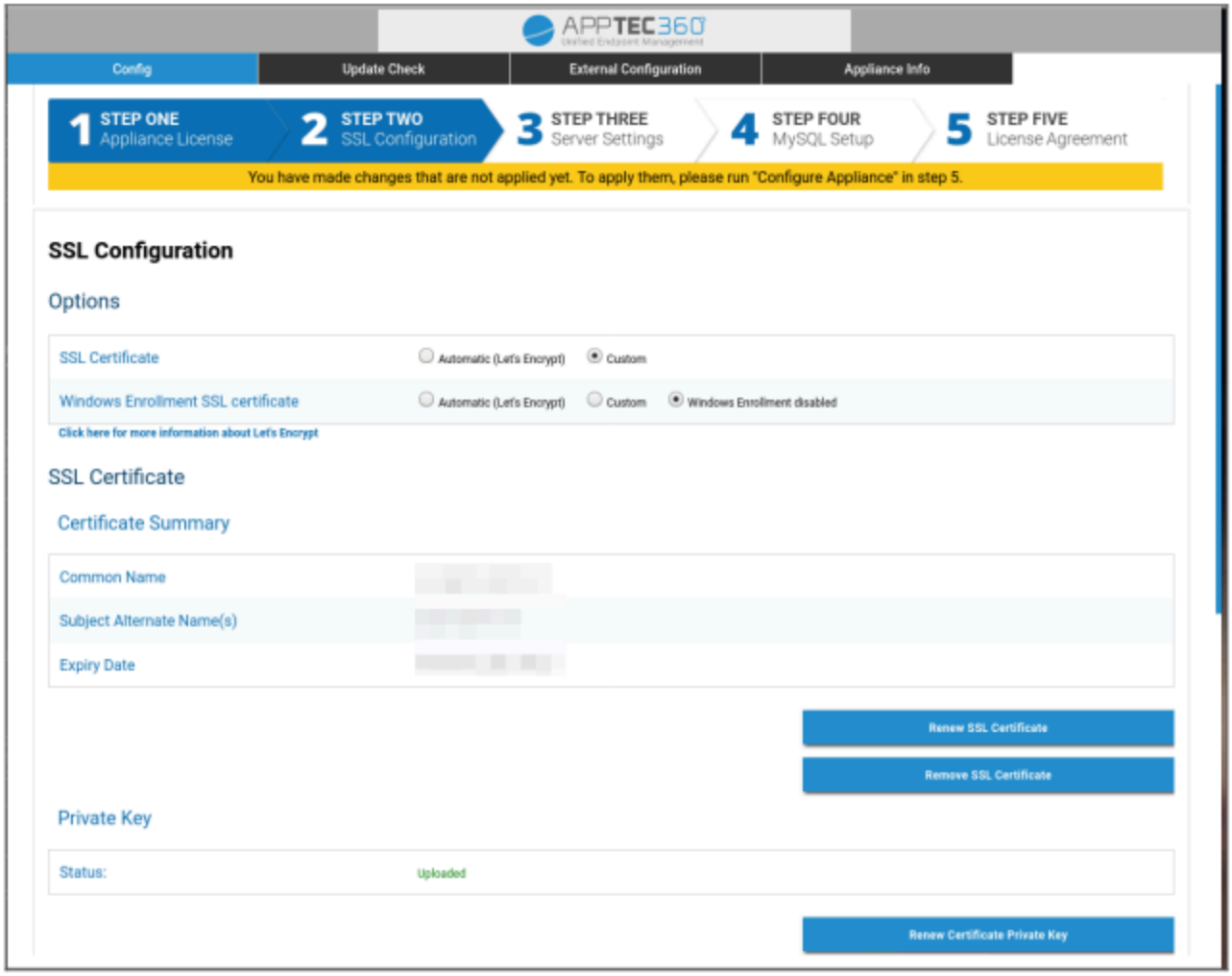
Personalizzato

1. Carica il certificato SSL per il tuo hostname con licenza. Puoi vedere il nome dell'host nel Passo 1 - Licenza della periferica.

2. Carica anche la chiave privata del certificato e, se necessario, il certificato intermedio.

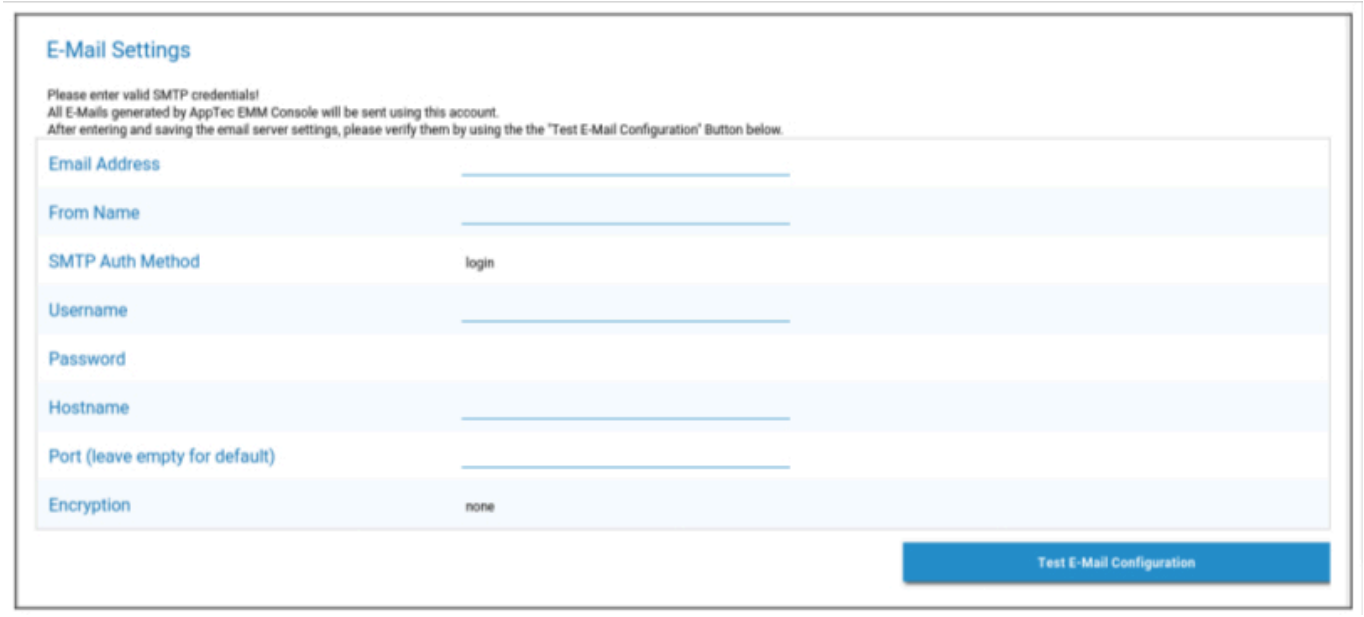
Importante: la chiave non deve essere protetta da password. Se così fosse, rimuovi la password prima di caricarla.

Suggerimento: se vuoi utilizzare anche i dispositivi Windows 10, devi abilitare il "Certificato SSL di Windows Enrollment" e caricare il certificato, la chiave privata e il certificato intermedio per il tuo sottodominio (come descritto nel caricamento di Indirizzo IP e Risoluzione DNS) in fondo alla pagina.



Terzo passo – Impostazioni del server

1. Inserisci un indirizzo e-mail di assistenza globale. Questo indirizzo verrà utilizzato nelle e-mail inviate ai tuoi utenti in modo che sappiano chi contattare in caso di problemi con il loro dispositivo.
2. Fornisci le impostazioni di posta elettronica che il sistema utilizzerà per inviare le e-mail. Le impostazioni verranno utilizzate per inviare e-mail all'utente e anche per inviare segnalazioni di bug e richieste di funzionalità a"support@apptec360.com". Dopo aver salvato le impostazioni di posta elettronica, devi verificarle cliccando su "Test E-Mail Configuration" e seguendo le istruzioni.



Quarto passo – Configurazione di MySQL

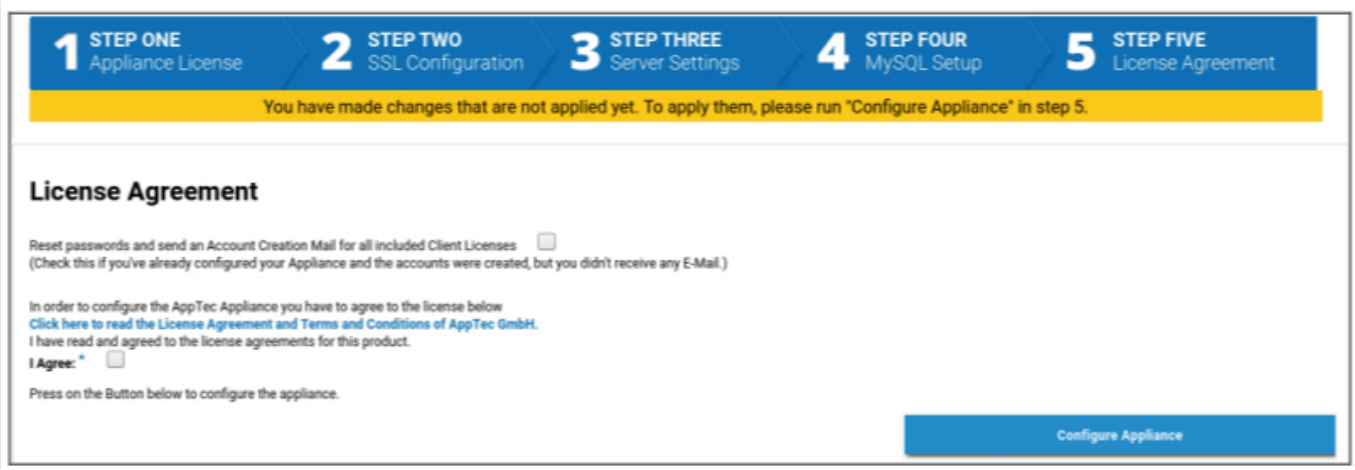
1. Se vuoi utilizzare il database interno puoi saltare questo passaggio. Altrimenti puoi inserire le informazioni di connessione del tuo server di database esterno.


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 – Contratto di licenza

1. Ti invitiamo a leggere il contratto di licenza.
2. Seleziona "Accetto" e premi il pulsante "Configura apparecchio" per applicare le impostazioni.

Suggerimento: dovrai eseguire "Configura apparecchiatura" ogni volta che modifichi le impostazioni nei 5 passi per applicarle.



Congratulazioni!

Hai terminato la configurazione del dispositivo virtuale.

Un'e-mail contenente la tua password è stata inviata all'indirizzo che hai fornito per la licenza (visibile in "Licenze client incluse" nella Fase Uno - Licenza dell'appliance).

Ora puoi accedere alla console utilizzando questa password e l'indirizzo e-mail che hai ricevuto.

Per accedere alla console, inserisci il nome dell'host della console nella barra degli indirizzi del tuo browser.

Puoi trovare il nome dell'host della tua appliance nel Passo 1 - Licenza dell'appliance.

Risoluzione dei problemi

1. Non hai ricevuto un'e-mail quando hai configurato l'appliance nella fase cinque - Contratto di licenza:

Assicurati che le impostazioni della tua posta elettronica nella Fase Tre - Impostazioni del server siano corrette. Per inviare nuovamente la password, seleziona "Reimposta le password e invia una mail di creazione dell'account per tutte le licenze client incluse" nel Passo 5 - Contratto di licenza prima di eseguire nuovamente "Configura l'appliance".

2. Hai ricevuto un errore relativo a Let's Encrypt durante la configurazione nel Passo 5 - Contratto di licenza:

Assicurati che l'appliance sia raggiungibile con il suo nome di dominio sulla porta 80. Let's encrypt scrive anche un log in "/var/log/letsencrypt" che può essere utile per la risoluzione di ulteriori problemi.

Raccomandazioni sulla sicurezza

Si consiglia di eseguire i seguenti passaggi per proteggere l'appliance AppTec360.

Non si tratta di una serie completa di istruzioni, ma solo di una raccomandazione per una configurazione di base.

- Cambia la password dell'utente di AppTec360
- Cambia la password degli utenti MySQL "root" e "AppTec" e aggiorna di conseguenza il Passo 4 - Configurazione di MySQL.
- Cambia la porta predefinita del server SSH
- Blocca la porta 80 nella tua console e disattiva il traffico HTTP in entrata, utilizzando solo HTTPS. Una volta configurato, è possibile anche una configurazione esterna tramite HTTPS.
- Limita l'accesso all'interfaccia di gestione solo a determinati Ip in fondo alla Fase Tre - Impostazioni del server.
- Configurare il firewall

Impostazioni generali

Panoramica dell’account

Informazioni sull’account

Panoramica

Qui puoi vedere una panoramica del tuo account AppTec360.

Nome dell'azienda	Il nome della tua azienda
Data di creazione	Data di creazione del tuo account
Tipo di licenza	Pagato = licenza a pagamento Gratuito = licenza non retribuita Nota: gli account di una periferica OnPremise saranno sempre indicati come pagati per motivi tecnici.
Identificatore del cliente	Identificativo del tuo conto (NON è il tuo codice cliente)
Data di scadenza della licenza	Data di scadenza della tua licenza AppTec360
Licenza ContentBox	Free = licenza gratuita per 25 dispositivi Pagato = licenza a pagamento per x dispositivi
Lanciatore	Mostra se è possibile utilizzare o meno il launcher personalizzato per Android.
Dispositivi	Numero di licenze attualmente utilizzate / totale
Persona di contatto	Persona di contatto fornita
Telefono	Numero di telefono fornito
eMail*	Indirizzo e-mail fornito
Utente principale	Utenti Root che possono accedere
Versione software	Versione attuale del software

**Nota: l'indirizzo e-mail indicato è quello inserito per la registrazione dell'Account. In base a ciò verrà creato un utente nell'albero degli utenti/dispositivi e potrà essere modificato. La modifica di questo utente cambierà l'indirizzo e-mail che dovrai usare per accedere, ma non le informazioni nella panoramica dell'account.*.

Segnalazione di bug

Un bug report può essere inviato direttamente all'assistenza per segnalare problemi o bug e include informazioni e registri sul tuo account e sulla tua configurazione.

Oggetto	L'oggetto della segnalazione di bug. Includi un numero di ticket se vuoi aggiungerlo a un ticket di assistenza esistente.
Comportamento previsto	Descrivi dettagliatamente cosa hai fatto e cosa ti aspettavi che accadesse.
Comportamento effettivo	Descrivi nel dettaglio cosa è successo esattamente. Cita i messaggi di errore ESATTAMENTE. È utile anche aggiungere degli screenshot all'allegato.
A che ora si è verificato il problema?	Indica il momento preciso in cui hai ricevuto un messaggio di errore/problema specifico. Nel migliore dei casi includi anche i secondi, ad es. 18:55:27
Il problema può essere replicato? Se sì, come (in dettaglio)?	Descrivi dettagliatamente come puoi riprodurre il problema.
Questa funzione ha funzionato in precedenza come ti aspettavi? Se sì, fino a quando?	Lascia vuoto se non lo sai.
Sono state apportate modifiche specifiche al sistema prima della comparsa di questo problema? Se sì, quali sono i cambiamenti (in dettaglio)?	Cita sempre l'ultima modifica o azione effettuata prima della comparsa del problema, anche se pensi che sia irrilevante.
Se applicabile: Quali sono i modelli di dispositivi e le versioni del sistema operativo interessati?	Indica sempre la versione esatta del sistema operativo (ad esempio, iOS 14.7.1 o Android 11).
Se applicabile: Qual è l'indirizzo IP pubblico e/o il numero di serie del dispositivo?	Nominane almeno uno, anche se tutti i dispositivi sono interessati.
Includi i file di log	Seleziona questa opzione per inviare il file di log con il bugreport. Si consiglia di farlo.
Recupera lo stato attuale del VPP da Apple e includilo nel bugreport	Include informazioni sulle assegnazioni di licenze VPP. Attivalo solo se ti viene richiesto dall'assistenza o se il tuo problema riguarda il VPP.

Allegato	Allega qualsiasi file che possa essere utile (ad esempio, screenshot di un messaggio di errore).

Richiesta di funzionalità

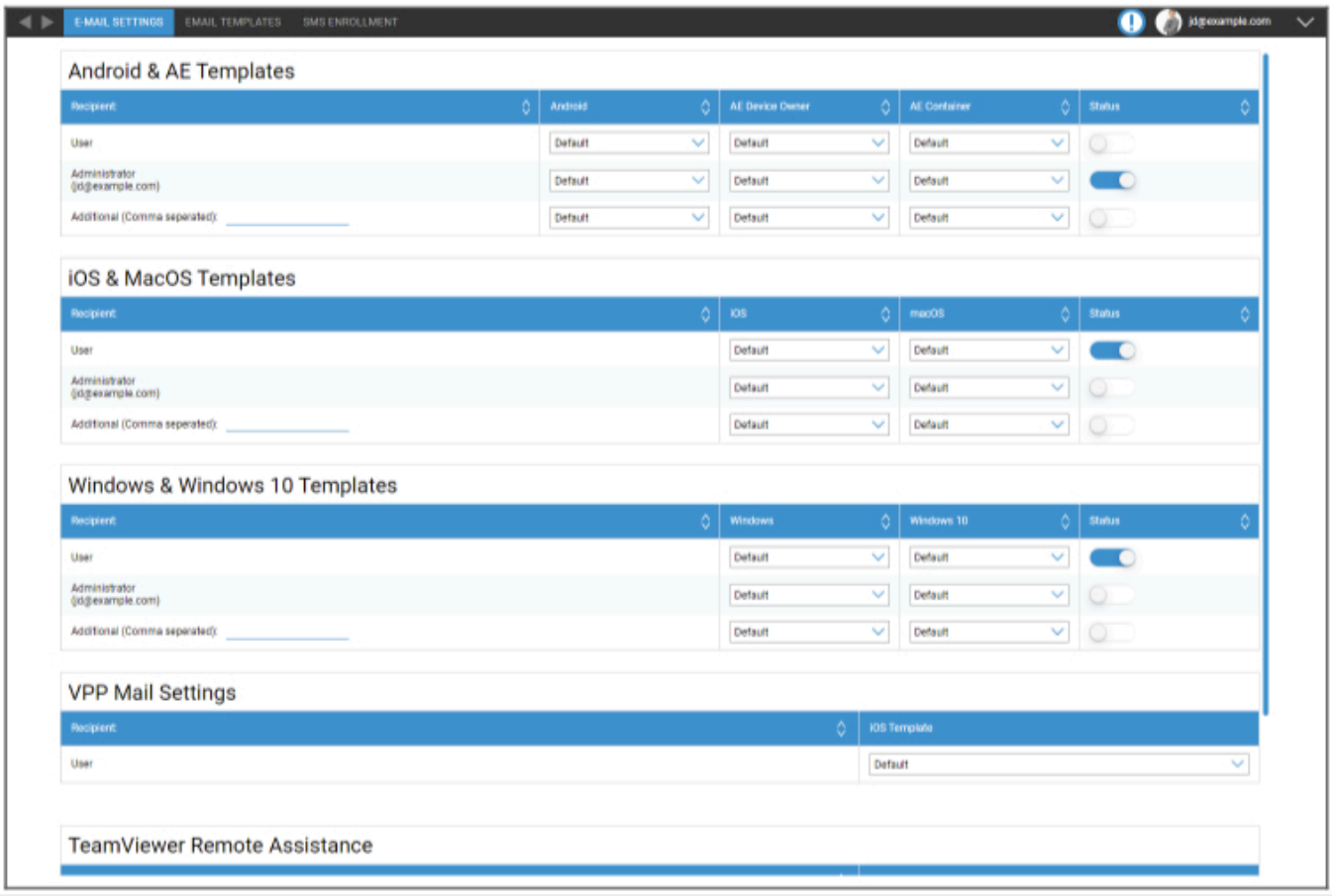
Una richiesta di funzionalità può essere inviata direttamente all'assistenza. Può contenere la richiesta di una caratteristica specifica o di un miglioramento per

Sommario	Una breve sinossi del tuo problema
Descrizione	Una descrizione dettagliata del tuo problema, che sia il più specifica possibile
Allegato	Allega dei file alla segnalazione di un bug

Configurazione globale

Impostazioni eMail

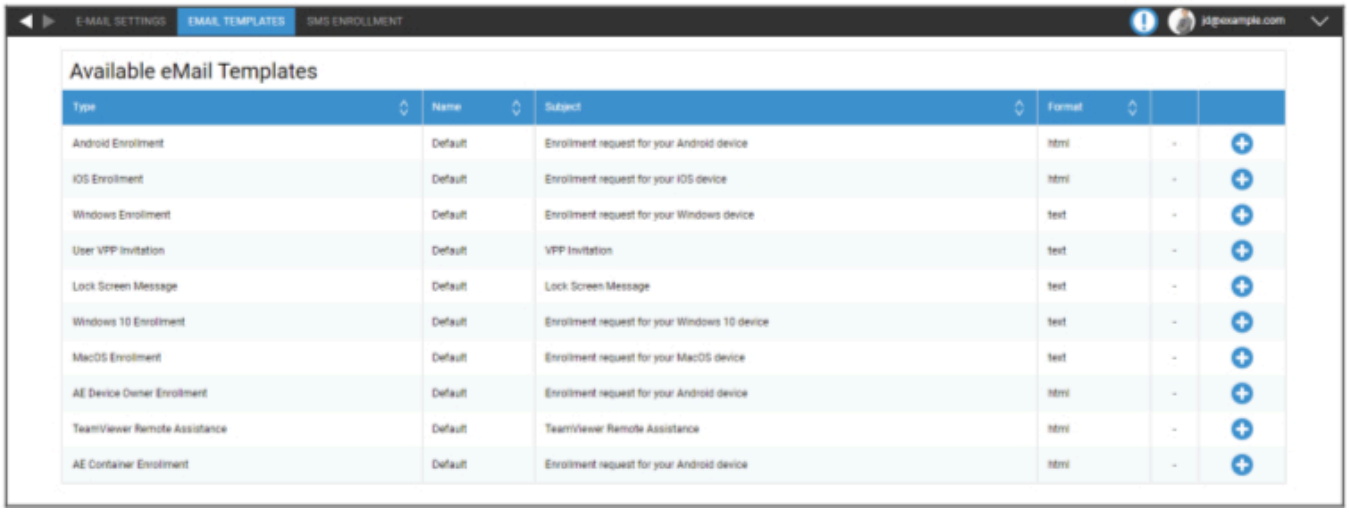
Qui puoi definire chi riceve una mail quando viene generata una richiesta di iscrizione e quale modello di testo viene utilizzato per quella mail.



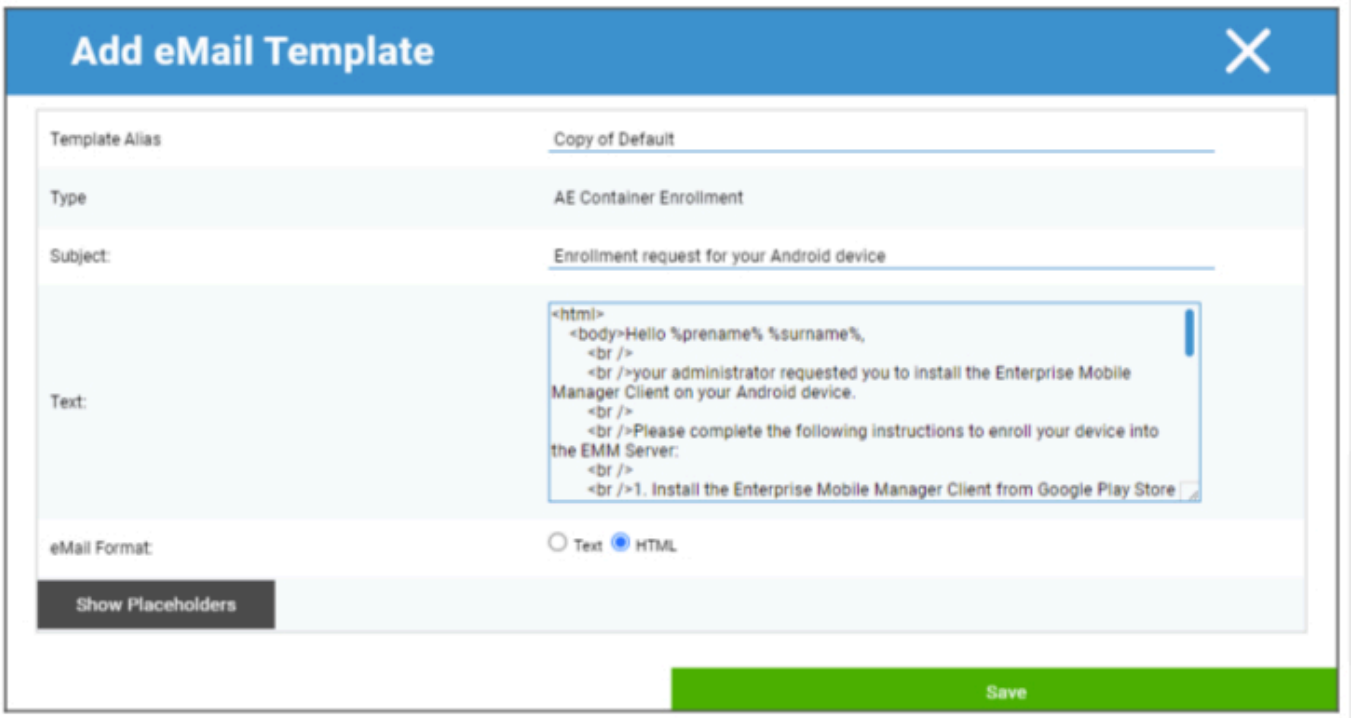
Modelli di eMail

Qui puoi generare e modificare i tuoi modelli per diversi scenari. Questi possono essere in forma di testo normale o in HTML. Con l'HTML puoi controllare meglio la formattazione del testo.

I modelli predefiniti non possono essere modificati o cancellati.



Puoi anche utilizzare dei segnaposto come variabili che verranno sostituite automaticamente. Clicca su "Mostra segnaposto" durante la modifica per vedere i segnaposto disponibili. Categorie diverse hanno segnaposti diversi.



Iscrizione via SMS

Qui puoi attivare il processo di iscrizione via SMS.

(Predefinito: disattivato)

Vedrai anche un display che indica quanti crediti SMS sono ancora disponibili.

I crediti SMS devono essere acquistati separatamente.

Privacy

Accesso GPS

Qui puoi proteggere la Vista GPS per ogni dispositivo con 1 o 2 password (principio dei quattro occhi). Ti verrà richiesto di inserire la password ogni volta che cercherai di accedere alla posizione di un dispositivo.

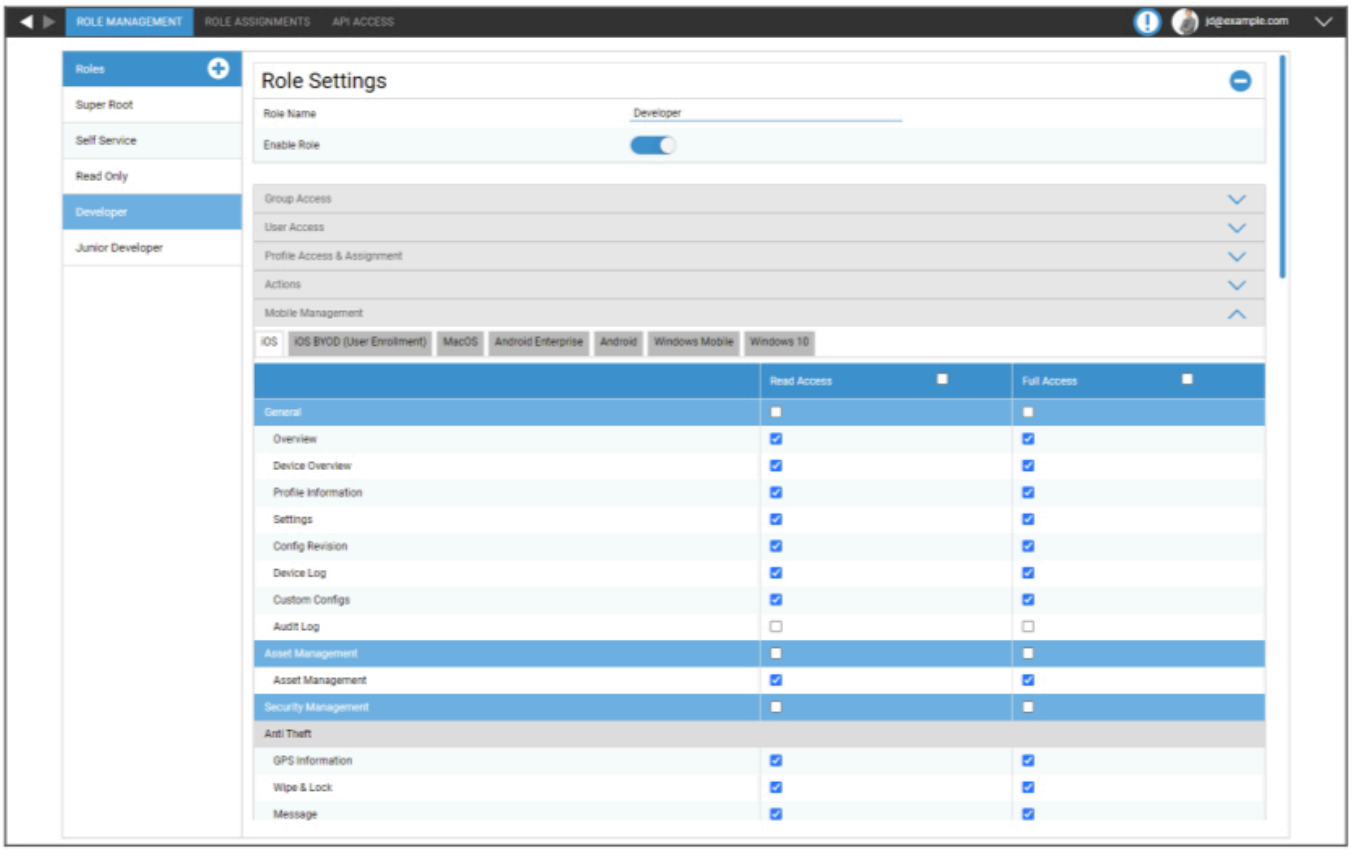
Limita l'accesso alle impostazioni del GPS	Off = la funzione è disattivata e non è richiesta alcuna password per la localizzazione.
	On = la funzione è attiva e viene richiesta una password per la localizzazione.
Metodo di protezione	Usa una sola password = usa una sola password per la localizzazione
	Usa due password = usa due password per la localizzazione
Inserisci la password (1)	Inserisci la password scelta
Ripeti la password (1)	Reinserisci la password scelta
opzionale: Inserisci la password 2	Inserisci la seconda password scelta
opzionale: Ripeti la password 2	Reinserisci la seconda password scelta

Nota: dopo aver impostato il codice di accesso, dovrai inserirlo ancora una volta prima che sia completamente abilitato.

Accesso basato sui ruoli

Gestione dei ruoli

I ruoli definiscono ciò che un utente può vedere e fare quando accede alla console di gestione. Questo ti permette di creare utenti che possono accedere ma con funzionalità limitate.



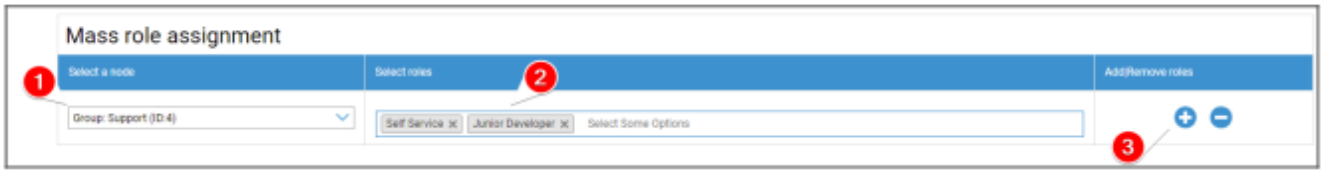
Il ruolo Super Root è un ruolo predefinito che è sempre in grado di vedere e modificare tutto. Non può essere modificato o cancellato. Il ruolo Self Service è in grado di vedere solo i propri utenti e i propri dispositivi. Puoi combinare il Self Service e un ruolo personalizzato per consentire agli utenti, ad esempio, di accedere e registrare i dispositivi da soli e solo per il proprio utente.

I ruoli personalizzati possono essere attivati o disattivati manualmente. I nuovi ruoli sono disabilitati per impostazione predefinita. Gli utenti con un ruolo disabilitato lavorano come se non avessero il ruolo. Questo ti permette, ad esempio, di limitare temporaneamente le azioni di un determinato ruolo.

Tutti i permessi sono suddivisi tra "Accesso in lettura" e "Accesso completo". Dare a un ruolo l'accesso in lettura gli permette di vedere una parte specifica della console. L'accesso completo consente al ruolo di vedere e modificare la parte specifica della console.

Assegnazione dei ruoli

Qui puoi avere una panoramica di tutti gli utenti che hanno un ruolo e vedere quale hanno. Qui puoi anche assegnare un ruolo agli utenti o a interi gruppi:

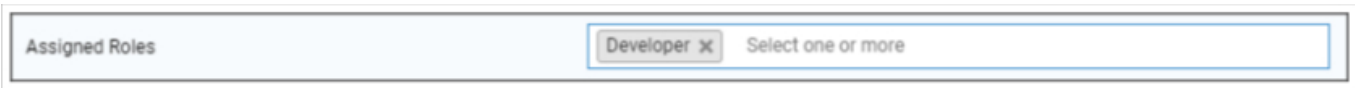


1. Seleziona per quale gruppo o utente vuoi aggiungere o rimuovere i ruoli. Puoi selezionare un singolo utente o un gruppo. Quando si seleziona un gruppo, la modifica avrà effetto su tutti gli utenti di quel gruppo e su tutti gli utenti dei sottogruppi del gruppo selezionato.
2. Seleziona il ruolo che vuoi aggiungere o rimuovere. Puoi selezionare uno o più ruoli.
3. . Seleziona l'operazione che vuoi eseguire. Cliccando sul "+" si aggiungono i ruoli selezionati se l'utente o gli utenti non li hanno già. Cliccando su "-" si rimuovono i ruoli selezionati dagli utenti. Se aggiungi dei ruoli a un utente che non ha ancora alcun ruolo, verrà automaticamente attivata la funzione "Può accedere" per l'utente.
4. Salva per terminare il processo. Gli utenti che in precedenza non avevano alcun ruolo e la voce "Può accedere" era disabilitata, riceveranno automaticamente una mail con un link per impostare una password.

Sotto l'assegnazione del ruolo di massa puoi trovare la panoramica dei ruoli assegnati. Puoi anche modificare manualmente i ruoli per determinati utenti.

Assegnazione di un ruolo

Per assegnare un ruolo a un utente, devi andare in Gestione cellulare, dove trovi la struttura dei tuoi gruppi, utenti e dispositivi. Modifica l'utente per assegnargli un ruolo. In alternativa, puoi utilizzare il metodo sopra descritto anche per i soli utenti singoli.



Accesso API

Accedi all'API REST di AppTec360

L'API REST di AppTec360 richiede un token di autenticazione (chiave API) e una chiave privata che devono essere generati nella Managment Console.

Per farlo, accedi ad AppTec360 EMM e vai su

Impostazioni generali → Accesso basato sui ruoli → Accesso API e aggiungi una nuova chiave.

Devi selezionare un utente i cui permessi saranno applicati alla chiave API.

La chiave privata può essere scaricata solo una volta. Dopo l'avvio del download, la chiave verrà cancellata e il pulsante "Download" scomparirà.

Se perdi la tua chiave privata, devi generare una nuova chiave API.

Regole generali

- L'API REST è disponibile sotto l'URL di base:

/public/external/api

- Tutte le richieste devono essere inviate tramite POST.
- L'API REST supporta solo le richieste via HTTPS.
- Le richieste devono contenere le seguenti intestazioni:

Nome dell'intestazione	Valore dell'intestazione	Descrizione
Tipo di contenuto	applicazione/json	fisso
auth	123...xyz	Chiave API dalla scheda "Accesso API
firma	Firma codificata in base64	Firma del payload generato con il metodo chiave privata dalla scheda "Accesso API

- Il corpo della richiesta deve essere un oggetto codificato json che deve contenere i seguenti valori:

Campo	Campo Esempio Valore	Descrizione
api	v2/dispositivo/elenco dispositivi	Nome dell'API
tempo	1529662725	Timestamp Unix (UTC) del computer client. La differenza di tempo massima consentita tra il client e il server è di 30 minuti.

- In caso di successo, l'API restituisce i dati richiesti (vedi le Query di seguito) e un codice di stato HTTP 200.
- Se si verifica un errore, il codice di stato HTTP sarà compreso tra 4xx e 5xx a seconda dell'errore e l'oggetto risposta conterrà un array con la chiave "errors", che contiene un elenco di messaggi di errore leggibili dall'uomo.
- Se non ci sono dati corrispondenti per un dispositivo, verrà restituito un array vuoto.
- Se l'Id di un dispositivo non esiste, i dati restituiti saranno nulli.

Esempio di richiesta

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]}}

Domande

Elenco di tutti i dispositivi

Funzionalità: Restituisce un elenco di tutti i dispositivi contenenti l'ID del dispositivo, l'IMEI e il numero di serie.
URI API: v2/device/listdevices
Parametri obbligatori: nessuno
Parametri opzionali: nessuno

Esempio di corpo della richiesta

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

Esempio di corpo della risposta

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

Ottieni un elenco di posizioni (GPS)

Funzionalità: Restituisce un elenco di tutte le voci del registro delle posizioni memorizzate per gli id dei dispositivi
URI API: v2/device/listposition
Parametri obbligatori: "ids" - Array di ID del dispositivo
Parametri opzionali: nessuno

Esempio di corpo della richiesta


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


Esempio di corpo della risposta


```
{
"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":[],
]
}
```

Ottieni la mappa delle risorse

Funzionalità:
Restituisce un elenco di tutti i possibili asset memorizzati da richiedere utilizzando Get any asset data. Per richiedere i dati puoi utilizzare il modulo a lettura umana o l'etichetta dell'asset.
URI API: v2/device/getassetmap
Parametri obbligatori: nessuno
Parametri opzionali: nessuno

Esempio di corpo della richiesta

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

Esempio di corpo della risposta

Questa risposta è stata abbreviata per renderla più leggibile.

{
"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": []
}

Ottieni i dati di qualsiasi asset

Funzionalità: Restituisce un elenco di dati di asset richiesti per gli id dei dispositivi
URI API: v2/device/getassetdata
Parametri obbligatori: "ids" - Array di ID del dispositivo
Parametri opzionali:
"assetkeys" - Chiavi dei dati dell'asset da restituire. Se non viene specificato, tutti i dati degli asset disponibili saranno
restituito. Puoi ottenere un elenco delle chiavi degli asset utilizzando Get asset map.

Esempio di corpo della richiesta


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


Esempio di corpo della risposta


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

Esempio di codice in 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)
```

Configurazione Apple

Certificato APNS

Qui puoi caricare un certificato APNS. È necessario per gestire i dispositivi iOS e MacOS.

Nota: il certificato APNS è valido solo per un anno. Deve essere rinnovato prima della scadenza. Il processo di rinnovo è identico a quello di creazione (vedi sotto) e richiede solo pochi minuti.

Se dimentichi di rinnovarlo in tempo, non potrai apportare modifiche ai dispositivi già registrati. **e dovrai iscrivere nuovamente tutti i dispositivi.** .

Passo 1

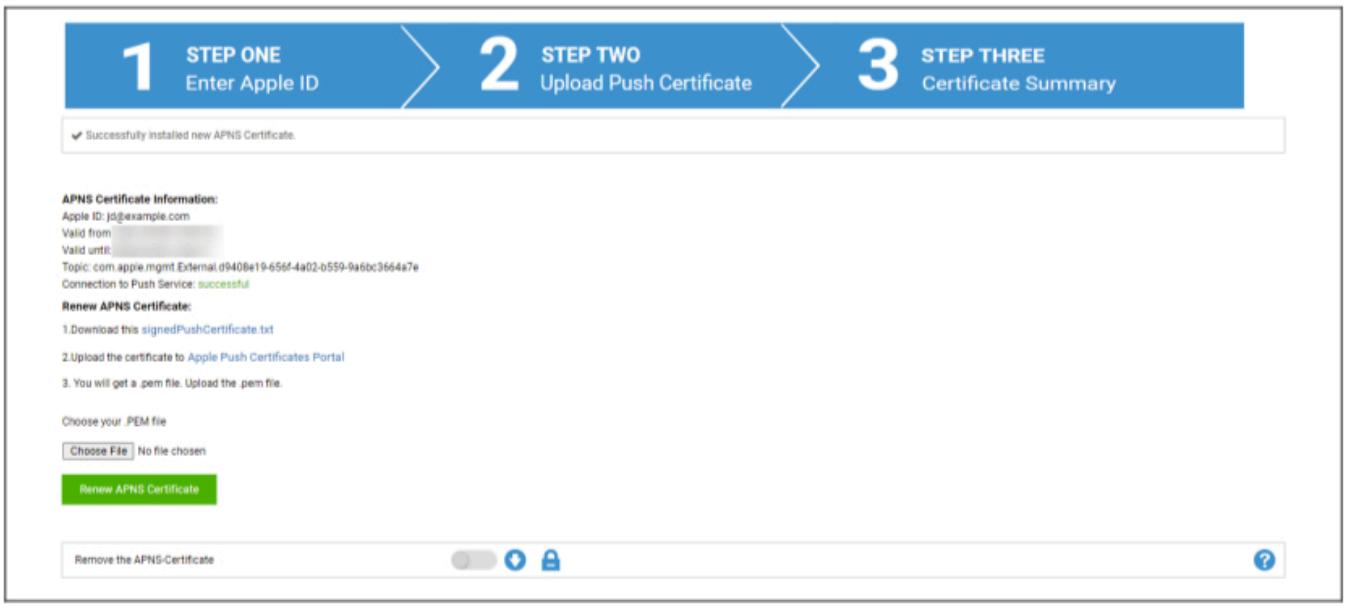
- Per prima cosa, inserisci il tuo ID Apple che vuoi utilizzare per creare il certificato APNS.

Nota: questo ID Apple viene utilizzato solo per la creazione del certificato APNS. Questo ID Apple non ha nulla a che fare con i dispositivi e i dispositivi non sono a conoscenza di questo ID Apple. Inoltre, è necessario accedere a questo ID Apple per rinnovare il certificato APNS. Pertanto si consiglia di utilizzare un ID Apple generico e di documentare i dati di accesso. Un promemoria viene inviato all'indirizzo di posta utilizzato dell'ID Apple prima della scadenza del certificato APNS.

- Clicca su "Prossimo passo" per procedere.
- (facoltativo) Puoi anche recuperare il certificato APNS precedentemente cancellato se l'hai eliminato per sbaglio

Passo 2

- Scarica il file signedPushCertificate.txt
- Vai su https://identity.apple.com/pushcert/ ed effettua il login con l'ID Apple del punto 1.
- Clicca su "Crea un certificato".
- (opzionale) inserisci una Nota. Questo può essere utile se gestisci più inquilini per identificarli facilmente.
- Clicca su "Scegli file" per selezionare il file signedPushCertificate.txt scaricato in precedenza.
- Clicca su "Carica".
- Ora vedrai la conferma della creazione di un certificato APNS.
- Clicca su "Scarica" e salva.
- Torna alla console di gestione.
- Clicca su "Scegli file" e seleziona il certificato APNS che vuoi caricare.
- Clicca su "Carica".



Passo 3

Ora hai configurato con successo il certificato APNS e puoi gestire i dispositivi iOS e MacOS.

Al punto 3 vedrai una panoramica del tuo certificato APNS attualmente utilizzato.

Hai anche la possibilità di rinnovare il certificato APNS seguendo i passi indicati sullo schermo. Ricordati di rinnovarlo prima che scada.

Quando rinnovi il certificato APNS, ricorda di effettuare il login con l'ID Apple indicato nel passaggio 3 e di rinnovare il certificato precedentemente utilizzato e NON crearne uno nuovo. Vedrai l'"argomento" del certificato APNS nel passaggio 3 e quando cliccherai sulla "i" nel portale dei certificati Apple Push. Si tratta dell'ID univoco che identifica il certificato. Questo ti aiuterà a identificare e rinnovare quello corretto.

Quando ottieni "Errore: Il certificato Push ha un argomento diverso!" durante il rinnovo, significa che hai rinnovato un altro certificato o ne hai creato uno nuovo.

Se vuoi caricare un nuovo certificato, ad esempio se non puoi più accedere all'ID Apple precedentemente utilizzato, devi prima eliminare il certificato attualmente caricato.

In ogni caso, l'eliminazione del certificato APNS significa che non potrai più apportare modifiche ai dispositivi attualmente iscritti fino a quando non li iscriverai nuovamente. Assicurati quindi di essere preparato a questa eventualità e rimuovi il Certificato solo se non c'è altro modo.

Accesso gestito

Qui puoi abilitare l'iscrizione dell'utente per i dispositivi iOS e l'iPad condiviso per i dispositivi iOS.

Iscrizione dell’utente

L'opzione 'Iscrizione utente' abilita una modalità speciale per i dispositivi BYOD.

Per ogni utente deve essere creato un Apple-ID gestito nell'Apple Business Portal.

Durante il processo di iscrizione, agli utenti verranno richieste le credenziali dell'ID Apple.

L'iscrizione dell'utente garantisce la massima sicurezza per l'utente in quanto permette di configurare solo un insieme limitato di impostazioni e restrizioni da parte dell'MDM.

Dominio gestito:

Il dominio utilizzato per mappare l'indirizzo e-mail dell'utente al suo Apple-ID gestito (deve essere nel formato: '@appleid.company.com').Ad esempio john.doe@example.com sarà mappato a john.doe@appleid.company.com

Controlla l'Apple Business Manager per vedere il tuo dominio gestito.

iPad condiviso

Un iPad condiviso è un dispositivo DEP configurato con un profilo DEP speciale.

Questo permette a più utenti di accedere al dispositivo utilizzando il proprio ID Apple gestito.

L'Apple-ID gestito deve essere creato nell'Apple Business Portal o nell'Apple School Manager.

Agli utenti che accedono a un iPad condiviso vengono richieste le credenziali dell'ID Apple gestito.

Dominio gestito:

Il dominio utilizzato per mappare l'indirizzo e-mail dell'utente al suo Apple-ID gestito (deve essere nel formato: '@appleid.company.com').Ad esempio john.doe@example.com sarà mappato a john.doe@appleid.company.com

Controlla l'Apple Business Manager per vedere il tuo dominio gestito.

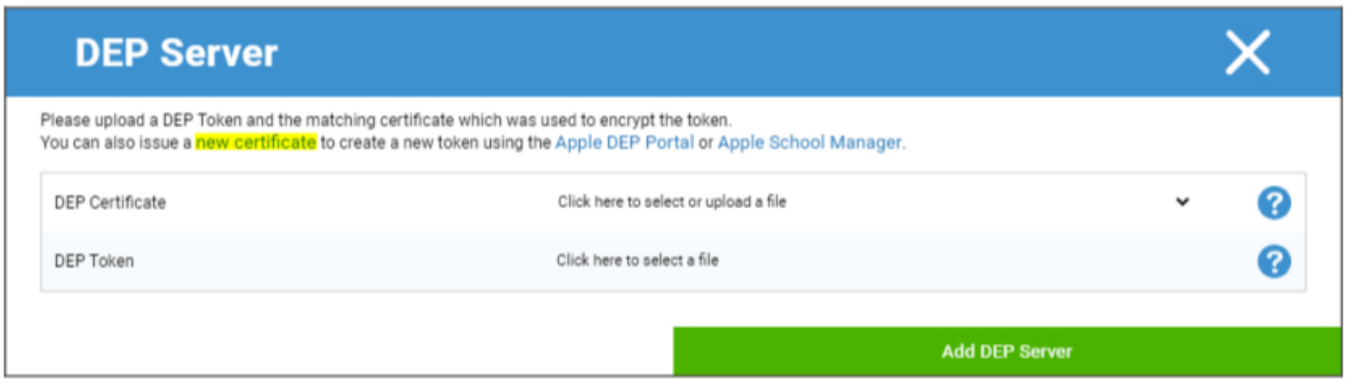
DEP

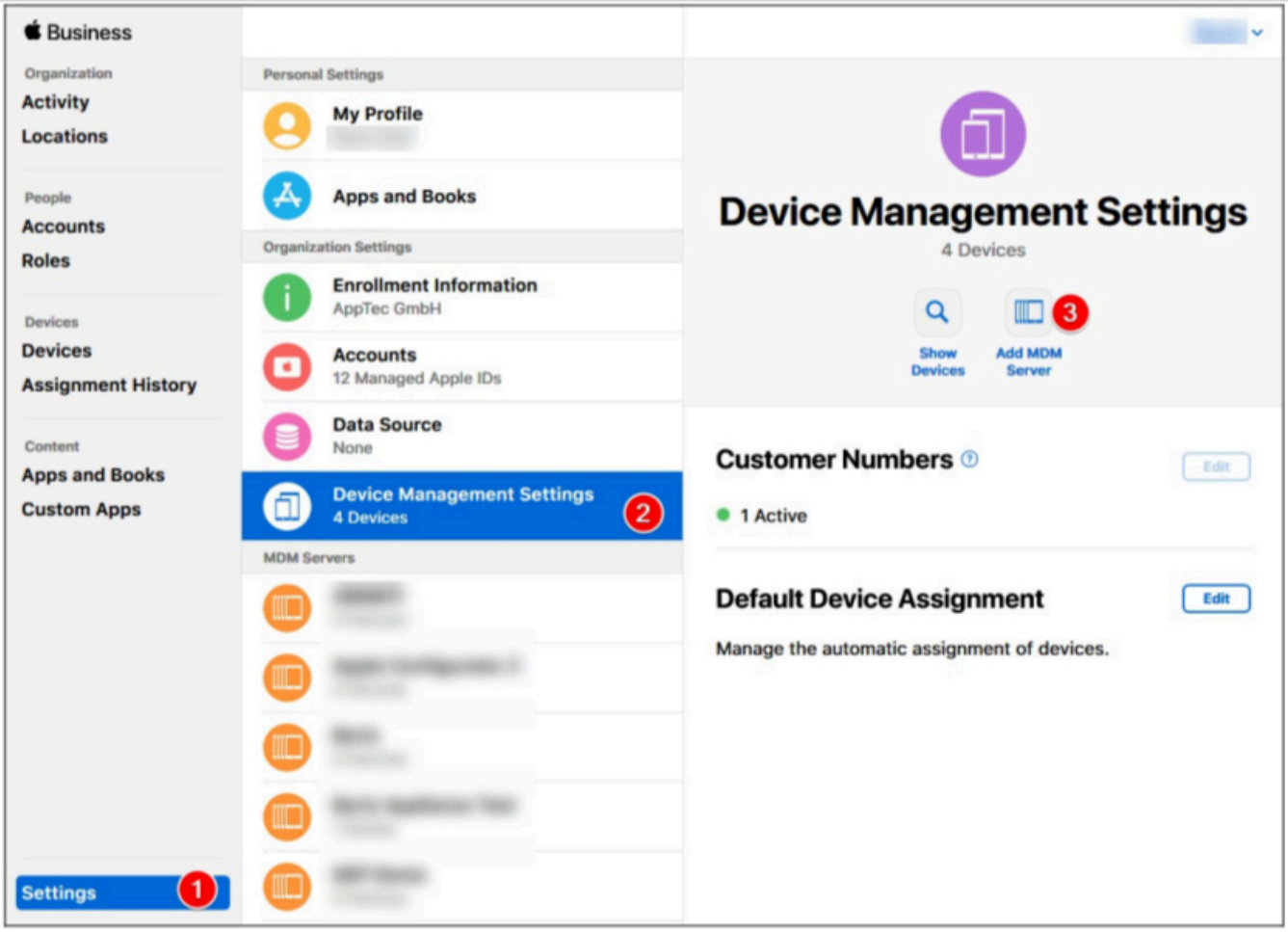
DEP (Device Enrollment Program) ti permette di iscrivere facilmente i dispositivi all'MDM. Quando si utilizza il DEP, i dispositivi vengono collegati automaticamente all'MDM al momento dell'impostazione del dispositivo. Puoi anche saltare quasi tutti i passaggi di configurazione che di solito sono obbligatori su iOS.

Tieni presente che devi acquistare i dispositivi da un rivenditore che supporti il DEP. Per maggiori informazioni, contatta il tuo rivenditore o Apple.

Ulteriori informazioni su DEP: https://www.apple.com/business/dep/

Clicca sul "+" per aggiungere un Token DEP. Nel popup, clicca su "nuovo certificato" nel testo (contrassegnato in giallo nell'immagine sottostante). In questo modo verrà generato e scaricato un certificato DEP. Successivamente accedi all'Apple Business Manager(https://business.apple.com/) o all'Apple School Manager(https://school.apple.com/).

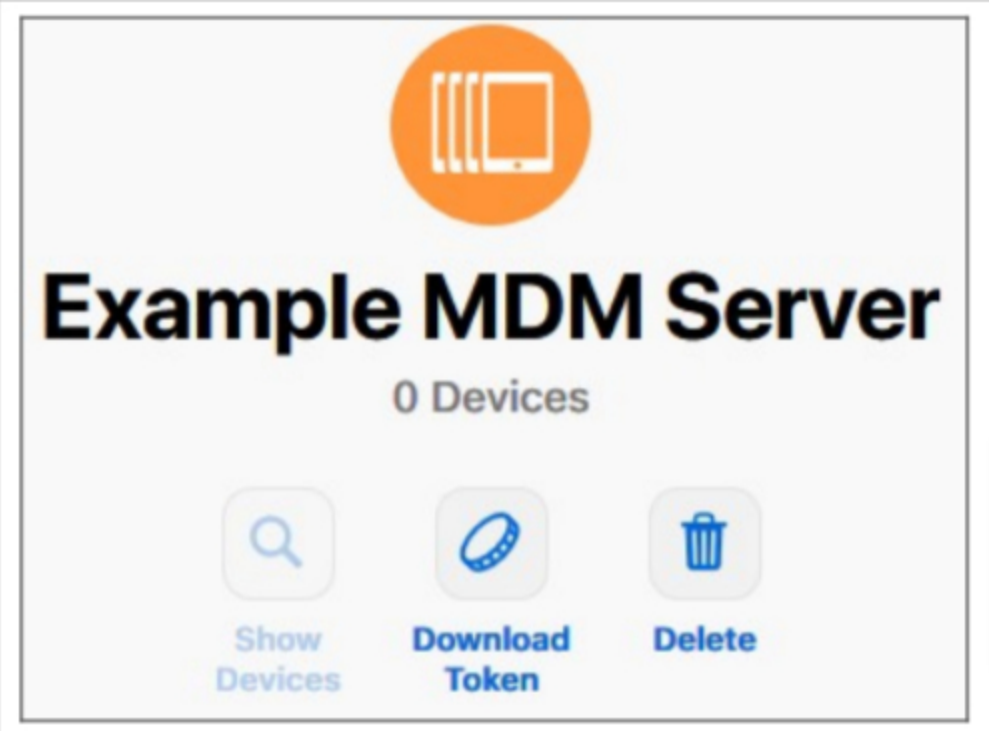




Nell'Apple Business Manager, segui i passi indicati nell'immagine qui sopra. Impostazioni → Impostazioni di gestione dei dispositivi → Aggiungi server MDM.

Dai al server un nome a piacere e carica il certificato DEP scaricato in precedenza in Impostazioni del server MDM → Carica chiave pubblica e clicca su "Salva".

Ora avrai l'opzione "Scarica il token". Clicca su questo e salvalo. Il gettone è valido solo per 1 anno. Ma basta cliccare nuovamente su "Scarica il token" per ottenerne uno nuovo, il che rende il rinnovo del token molto semplice.



Ora puoi tornare all'MDM, dove hai scaricato il certificato DEP. Se non hai chiuso la scheda, il popup per l'aggiunta di un Server DEP dovrebbe essere ancora aperto e il Certificato DEP dovrebbe essere già selezionato. Ora puoi caricare il tuo Token nel campo "DEP Token" e cliccare su DEP Server.

Nella colonna "**Dispositivi**" vedrai il numero di dispositivi assegnati a questo DEP Server. I dispositivi aggiunti a questo server DEP verranno creati automaticamente nel pool DEP di Gestione dispositivi mobili.

Puoi cliccare su questo numero per avere una panoramica di tutti i tuoi dispositivi DEP e del loro stato.

Nota: a seconda del flusso di lavoro o della configurazione del Business Manager, è possibile che tu debba assegnare manualmente questi dispositivi al DEP Server. Puoi anche impostare un DEP Server predefinito nell'Apple Business Manager per i nuovi dispositivi.

Nella colonna "**Profili**" puoi vedere la quantità di profili DEP che hai. Puoi anche cliccare su questo numero per vedere i dettagli dei tuoi Profili DEP e puoi cancellare i profili vecchi/non utilizzati. Al momento non è possibile modificarli. Se vuoi fare un cambiamento, devi crearne uno nuovo.

Nella colonna "**Ultima sincronizzazione**" puoi sincronizzare manualmente il Server DEP (ad esempio se hai appena aggiunto un nuovo dispositivo a DEP) e vedere la data dell'ultima sincronizzazione

andata a buon fine.

Nella colonna "**Profilo automatico**" puoi impostare un profilo DEP come default automatico. Questo profilo verrà assegnato automaticamente ai nuovi dispositivi. Se non imposti un profilo automatico, dovrai assegnare manualmente un profilo ai nuovi dispositivi ogni volta.

Nella colonna "**Aggiungi profilo**" puoi aggiungere un nuovo profilo DEP. Il dispositivo lo riceverà all'inizio della sua configurazione. Il profilo DEP definisce il modo in cui il dispositivo viene configurato e quali fasi di configurazione vengono saltate.

Nota: dopo che un dispositivo è stato registrato, queste impostazioni possono essere modificate solo eseguendo un reset di fabbrica e registrando il dispositivo con un nuovo profilo. Questo è particolarmente importante per le opzioni "**Rimovibile**" e "**Consenti l'accoppiamento**". Nel caso di "**Consenti l'accoppiamento**" si consiglia di attivarlo, poiché può essere disattivato tramite le restrizioni MDM, ma non può essere attivato nuovamente se è stato disattivato nel profilo DEP.

Nella colonna "**Modifica**" puoi caricare un nuovo token, ad esempio quando rinnovi il token.

Configuratore e URL

URL di iscrizione al pool

Qui puoi creare un URL di iscrizione e un QR Code di iscrizione valido per un determinato numero di iscrizioni e fino a una data stabilita. Questo ti permette di iscrivere più dispositivi con un solo link o codice QR.

I dispositivi registrati con questo URL o QR Code saranno presenti nel pool della Gestione dispositivi mobili e dovrai assegnarli manualmente a un gruppo o a un utente.

Nota: questo vale solo per l'iscrizione manuale. Non utilizzare questo URL se iscrivi i dispositivi tramite Apple Configurator.

Profilo MDM – Configuratore Apple

Qui puoi ottenere l'URL necessario per l'iscrizione dei dispositivi tramite Apple Configurator. Mentre prepari i dispositivi con il Configuratore Apple puoi aggiungere i dispositivi all'MDM nello stesso processo. Il configuratore Apple richiede questo URL.

I dispositivi aggiunti tramite Apple Configurator saranno presenti nel Pool di Gestione Cellulari e dovrai assegnarli manualmente a un gruppo o a un utente.

Qui troverai anche un file .mobileconfig che può essere utilizzato per registrare i dispositivi tramite Apple Configurator. In ogni caso è consigliabile utilizzare l'URL.

Configurazione Android

Configurazione Android

Disinstallare la protezione	Se questa funzione è attivata, l'utente non può disattivare l'amministratore del dispositivo senza inserire la password impostata dall'amministratore MDM. La password viene impostata durante l'iscrizione, quindi i dispositivi devono essere nuovamente iscritti per aggiornare la password. Ci sono due opzioni per rimuovere gli amministratori del dispositivo: 1. Manualmente sul dispositivo ◦ Apri l'applicazione EMM sul dispositivo ◦ Passa alla scheda Stato ◦ Tocca "Disinstalla protezione". ◦ Inserisci la password Puoi utilizzare la Revisione per ottenere la password corretta dalla "Cronologia delle password" della console. ◦ Scorri verso il basso e tocca il punto appena aggiunto: "Tocca per disinstallare AppTec360 MDM App" (hai 20 secondi per eseguire questa operazione). ◦ Conferma il messaggio "Disinstalla AppTec360 MDM App" con "ok". In questo modo il dispositivo verrà disiscrivibile dalla console. ◦ Per rimuovere l'applicazione dal dispositivo, conferma la finestra "AppTec360 MDM verrà disinstallata" con "UNINSTALL". 2. l'automatico (Console) ◦ Seleziona il dispositivo nella console ◦ Clicca sull'icona blu dell'ingranaggio e seleziona "Enterprise Wipe". Nota: disponibile solo con Android 4.x e versioni successive o su dispositivi con API KNOX (dispositivi Samsung).

Password di disinstallazione (revisione x)	La password stabilita, con la quale l'utente può rimuovere l'amministratore del dispositivo. Revisione x = contatore, quante volte la password è già stata cambiata È importante quale sia la password di cui l'utente ha bisogno, perché è possibile che il dispositivo non abbia comunicato con il server AppTec360 e quindi la password più recente non sia ancora stata trasmessa.
Storia della password	Cliccando sul pulsante blu ("Mostra la cronologia"), potrai visualizzare le password stabilite in precedenza.
Protezione estesa per la disinstallazione	Questa opzione offre una protezione contro i dispositivi non-SAFE. Finché questa impostazione è attiva, non è possibile disattivare facilmente l'amministratore del dispositivo.
Chiedere all'utente di disinstallare le applicazioni bloccate?	Se possibile, le app bloccate non solo verranno bloccate ma anche disinstallate automaticamente. All'utente verrà richiesto di disinstallare le applicazioni bloccate se non è possibile una disinstallazione automatica.
Blocco delle app del sistema intelligente	Se la funzione Whitelisting è attivata, il client MDM Android blocca tutte le applicazioni installate dagli utenti. Abilita questa impostazione per bloccare tutte le app di sistema avviabili in modalità Whitelisting.

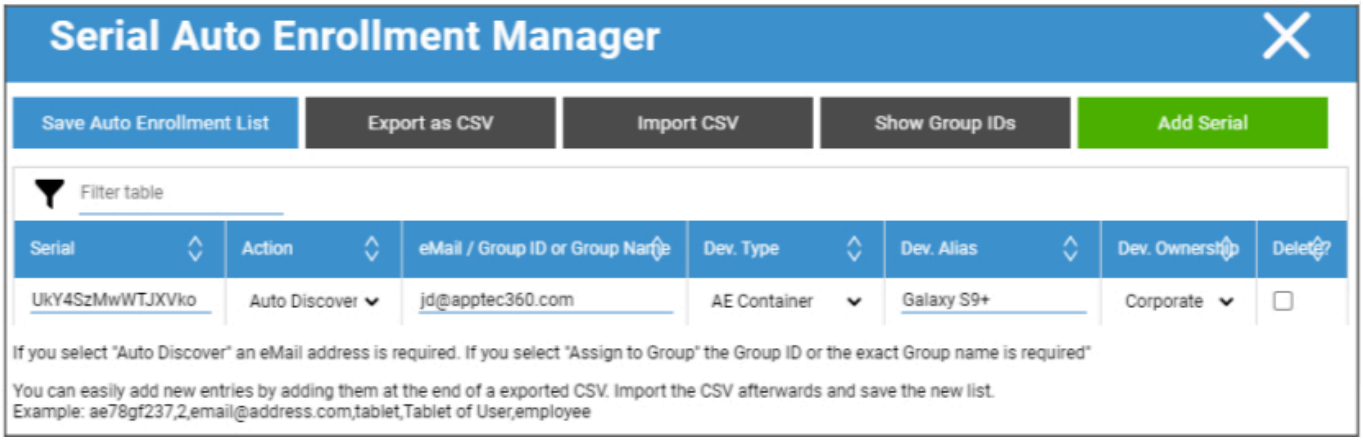
Iscrizione automatica

Qui puoi attivare la funzione di iscrizione automatica per iscrivere automaticamente i tuoi dispositivi quando il client MDM di AppTec360 viene aperto sul dispositivo.

Importante: questo metodo di iscrizione è deprecato e non funziona più su Android 10 o versioni successive. In ogni caso, se utilizzi Android 7 o superiore, dovresti registrare i dispositivi come Android Enterprise completamente gestito. Se vuoi utilizzare il contenitore Android Enterprise BYOD e sei su Android 10 o superiore, devi registrare manualmente il dispositivo tramite credenziali, QR Code o SMS. In ogni caso, l'elenco di iscrizione automatica viene ancora utilizzato per automatizzare il processo di iscrizione, ad esempio per l'iscrizione AE, l'iscrizione Knox, ecc.

In ogni caso, l'elenco di iscrizione automatica viene ancora utilizzato per automatizzare il processo di iscrizione, ad esempio per l'iscrizione AE, l'iscrizione Knox, ecc.

Cliccando su "Serial Manager" o "IMEI Manager" puoi aggiungere rispettivamente il numero di serie o l'IMEI dei tuoi dispositivi. Non è necessario fare entrambe le cose per i tuoi dispositivi, ne basta una sola.



L'**azione** definisce se i dispositivi saranno iscritti al pool, a un utente o a un gruppo.

Puoi anche esportare e importare un file .csv e filtrare le voci per parole chiave.

Android Enterprise

Qui puoi configurare Android Enterprise. Questo è necessario per utilizzare tutte le funzioni di Android Enterprise.

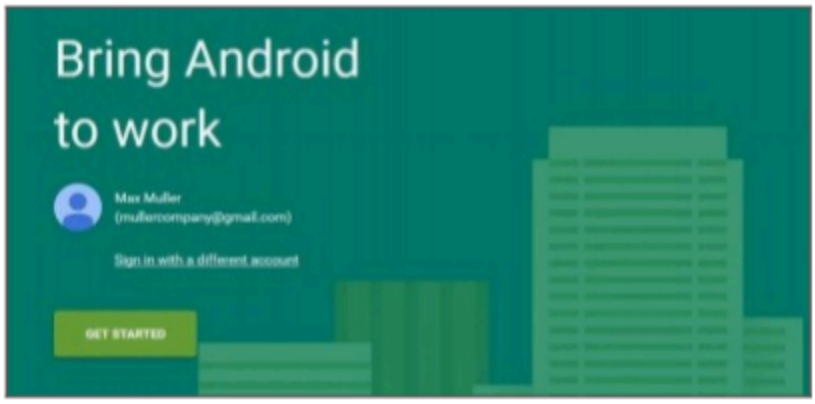
Primo metodo: Account aziendale Android (account Google)

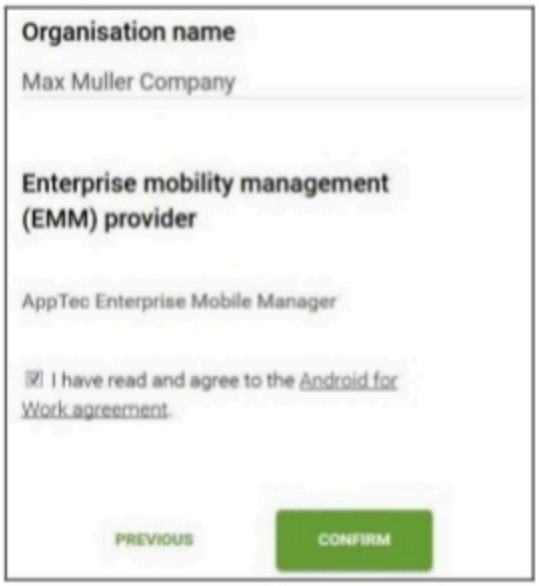
Per prima cosa premi "Prepare Setup", quindi dopo un breve momento dovrebbe comparire il pulsante "Start Setup".

Questo ti porterà alla pagina di configurazione di Android Enterprise di Google.

Effettua il login con l'account Google che vuoi utilizzare, se non sei già loggato, e premi "Inizia".

Ora puoi inserire il nome della tua azienda. Dopo aver fatto ciò, seleziona la casella di controllo e premi "Conferma".





Nell'ultimo passaggio puoi completare la registrazione e tornare alla console. Se tutto funziona, il risultato dovrebbe essere questo:

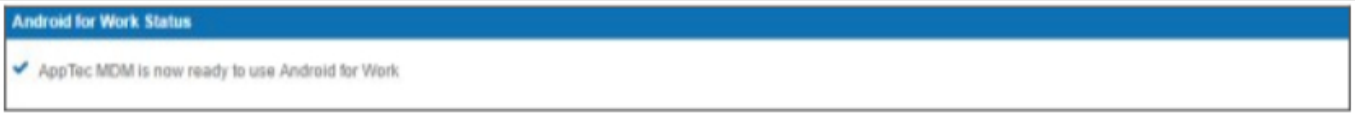
Ora puoi iniziare a configurare il tuo Android Enterprise Container.

Secondo metodo: Account G-Suite

Premi "Usa G-Suite" e accedi al tuo account amministratore Google. Vai su "Sicurezza" -> "Mostra di più" -> "Gestisci il provider EMM per Android" e genera un Token. Nota: se non vedi le impostazioni di Android Enterprise nel tuo account G-Suite, devi andare su "Ottieni altre applicazioni e servizi" e aggiungere la gestione dei dispositivi Android. Ora inserisci il token e il tuo dominio primario nella nostra console e clicca su "Salva le modifiche". Al termine, clicca su "Usa l'account Android Enterprise".

Ora dovresti vedere il pulsante "Crea un account di servizio". Clicca su di esso. Questo processo può richiedere qualche istante.

Se tutto ha funzionato, dovrebbe apparire così:



Ora puoi iniziare a configurare il tuo Android Enterprise Container.

Protezione dal reset di fabbrica

Con la protezione per il ripristino di fabbrica puoi associare il tuo dispositivo a un account google di tua scelta, che sovrascrive anche qualsiasi vincolo esistente con un account google. Per utilizzare la Protezione ripristino dati di fabbrica, devi prima impostarla qui e poi attivarla nei tuoi profili.

Per impostare la protezione dal ripristino di fabbrica, clicca su "FRP Setup" e segui le istruzioni sullo schermo.

NOTA: leggi attentamente ed esegui i passaggi. Ti consigliamo di farlo in una nuova finestra del browser in incognito per evitare di accedere automaticamente all'account Google sbagliato. Puoi bloccarti completamente dal dispositivo, se dovessi inserire un ID sbagliato o perdere l'accesso all'account Google utilizzato!

Iscrizione AE

Qui puoi attivare l'Android Enterprise Ernollment. Utilizzando questo metodo, i tuoi dispositivi entreranno nella modalità Proprietario del dispositivo Android Enterprise. In questa modalità avrai il pieno controllo del dispositivo.

Abilita l'iscrizione all'AE	Attiva l'iscrizione AE Attenzione: Se disattivi l'iscrizione AE, i QR Code esistenti e i dispositivi programmatori NFC già configurati smetteranno di funzionare. Se attivi nuovamente l'iscrizione AE, dovrai inviare nuovamente le configurazioni push NFC / generare nuovi codici QR.
Abilita la scoperta automatica	Quando un dispositivo si iscrive tramite "Iscrizione AE", il sistema cercherà di assegnarlo a un utente in base alle informazioni impostate nella Whitelist Seriale/IMEI ("Impostazioni generali" > "Configurazione Android" > "Iscrizione automatica").
Blocca i dispositivi sconosciuti	Solo i dispositivi che sono stati inseriti nella Whitelist Seriale/IMEI ("Impostazioni generali" > "Configurazione Android" > "Iscrizione automatica") possono iscriversi.

Nota sui metodi 1 e 2: la "schermata di benvenuto" si riferisce alla prima schermata che vedi dopo il reset di fabbrica. L'aspetto può variare a seconda della versione di Android e/o del modello di dispositivo che stai utilizzando.

Metodo 1: Iscrizione con codice QR

(richiede Android 7.0 o superiore) Ti consigliamo di utilizzare sempre questo metodo se utilizzi Android 7 o versioni successive.

1. Ripristino delle impostazioni di fabbrica del dispositivo
2. Genera il codice QR per l'iscrizione utilizzando uno dei due metodi seguenti:
    - Clicca in "Impostazioni generali -> Configurazione Android -> Iscrizione AE" su "Genera codice QR". Scegli se vuoi saltare la crittografia dello spazio di archiviazione e/o se tutte le app di sistema devono essere rimosse.
    - (in alternativa) Scegli un dispositivo esistente. Nella "Panoramica del dispositivo" clicca sul codice QR visualizzato. Scegli se vuoi saltare la crittografia dello spazio di archiviazione e/o se tutte le app di sistema devono essere rimosse.
3. Ora tocca 6 volte la schermata di benvenuto del tuo dispositivo. Questo dovrebbe avviare la modalità di iscrizione QR.
4. Ora connettiti a una rete wireless e attendi un po' di tempo prima che il lettore di codici QR venga installato.
5. Ora scansiona il codice QR
6. Questo è tutto. Il tuo dispositivo è ora iscritto alla modalità Android Enterprise Device.

- a. Se hai utilizzato il codice QR nelle "Impostazioni generali", puoi trovare il tuo dispositivo in "Pool -> AE Device Owner Devices". (Suggerimento: è possibile che tu debba ricaricare il sito per vedere i dispositivi). Se hai selezionato "Abilita l'Auto Discover", lo troverai all'interno del tuo utente Auto Discover.
- Se hai utilizzato il codice QR di un profilo di dispositivo esistente, il dispositivo verrà iscritto in questo profilo.

Metodo 2: Iscrizione NFC

(richiede NFC e Android 6.0 o superiore)

Preparazione: Inserisci i tuoi dati WiFi in "Impostazioni generali -> Configurazione Android -> Iscrizione AE -> Dati per il provisioning NFC". Ora usa "Dispositivo NFC" per cercare il dispositivo che diventerà il programmatore. Questo dispositivo verrà utilizzato per inviare le informazioni di iscrizione agli altri dispositivi tramite NFC.

1. Ripristino delle impostazioni di fabbrica del dispositivo
2. Apri l'applicazione di accoppiamento NFC di AppTec360 sul tuo programmatore
3. Scegli se vuoi saltare la crittografia dello spazio di archiviazione e/o se tutte le app di sistema devono essere rimosse.
4. Tieni entrambi i dispositivi schiena contro schiena
5. Ora l'iscrizione ad Android Enterprise dovrebbe essere in netto aumento.
6. Ora trovi il tuo dispositivo nella console
    - a. Nel pool, se non hai configurato l'Auto Discover
    - b. All'interno dell'utente, hai configurato l'Auto Discover
    - c. Suggerimento: è possibile che sia necessario ricaricare il sito per visualizzare i dispositivi.

Metodo 3: Account Google

(richiede Android 5.1 o superiore)

(Nota: se utilizzi questo metodo, il dispositivo non verrà iscritto automaticamente. Dovrai invece iscriverlo manualmente o automatizzare il processo utilizzando l'iscrizione automatica).

1. Ripristino delle impostazioni di fabbrica del dispositivo
2. Esegui le operazioni di configurazione fino a quando non potrai accedere con un account Google.
3. Inserisci "afw#apptec" come nome utente/mail
4. Tocca "Avanti".

5. Il tuo dispositivo è ora un dispositivo Android Enterprise

Iscrizione a KNOX

Qui puoi attivare l'iscrizione a KNOX e trovare le informazioni necessarie per creare un profilo di iscrizione a KNOX nel portale di distribuzione KNOX. Per configurare e utilizzare questo sistema è necessario avere un account sul portale di distribuzione KNOX.

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

Abilita l'iscrizione a KNOX	Attiva l'iscrizione a KNOX. Attenzione: Se disattivi l'iscrizione a KNOX, i profili MDM esistenti smetteranno di funzionare. Se attivi nuovamente KNOX Enrollment, dovrai aggiornare il campo "Custom JSON Data" del tuo profilo MDM.
Abilita la scoperta automatica	Quando un dispositivo si iscrive tramite "Iscrizione KNOX", il sistema cercherà di assegnarlo a un utente in base alle informazioni impostate nella Whitelist Seriale/IMEI ("Impostazioni generali" > "Configurazione Android" > "Iscrizione automatica").

1. Accedi al portale Samsung KNOX Mobile Enrollment https://eukme.samsungknox.com/itadmin
2. Vai a "Profili MDM".
3. Clicca su "Aggiungi".
4. Scegli "Server URI non richiesto per il mio MDM" e clicca su "Avanti".
5. Ora crea un profilo con le informazioni mostrate nella console di gestione

Ora questo profilo di iscrizione KNOX può essere installato direttamente sul dispositivo da Samsung se acquisti i dispositivi direttamente da Samsung.

In alternativa puoi scaricare l'app KNOX Deployment, accedere con il tuo account KNOX Deployment e inviare il profilo di iscrizione KNOX tramite NFC ad altri dispositivi.

Se il dispositivo ha installato un profilo di iscrizione KNOX, scaricherà la nostra app e iscriverà il dispositivo, se dispone di una connessione internet funzionante.

L'iscrizione dei dispositivi tramite KNOX Enrollment si trova in "Pool -> KNOX Enrollment", oppure all'interno dell'utente specificato nella funzione Auto Discover.

Zero-Touch

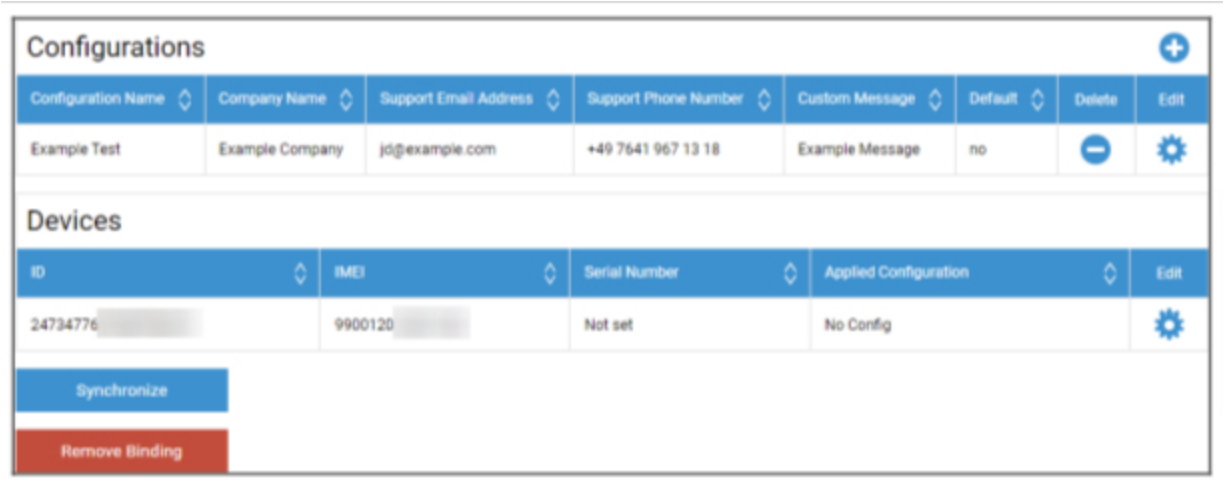
Con Zero-Touch puoi registrare facilmente i tuoi dispositivi senza doverli toccare o configurare qualcosa sul dispositivo stesso. Devi solo accenderlo, procedere alla configurazione come di consueto e il dispositivo riceverà tutte le informazioni su come configurare e connettersi all'MDM in modo completamente automatico.

Per utilizzare Zero-Touch devi acquistare i tuoi dispositivi da un rivenditore che supporta Zero-Touch. Lo stesso rivenditore sta creando un account per te nel portale Zero-Touch. Contatta il tuo rivenditore per avere maggiori informazioni sulla procedura o se riscontri problemi nell'accesso al portale Zero-Touch.

Clicca su "Start Setup" per avviare la configurazione. Verrai reindirizzato a una pagina di login dove dovrai selezionare il tuo account Google che ha accesso al portale Zero-Touch.

NOTA: è possibile selezionare QUALSIASI account. Assicurati quindi di selezionare l'Account corretto in questo passaggio. Se non vedi i tuoi dispositivi/configurazioni, è probabile che tu abbia utilizzato l'Account sbagliato.

Dopo aver completato l'accesso, l'aspetto sarà il seguente:



Clicca sul "+" per aggiungere una configurazione e compila i campi come indicato sullo schermo. Se attivi la configurazione come configurazione predefinita, questa verrà assegnata automaticamente ai nuovi dispositivi. La creazione o l'impostazione di una configurazione predefinita non la assegna ai dispositivi già esistenti.

Se un dispositivo non ha una configurazione assegnata, si configurerà come un dispositivo normale e non si connetterà all'MDM. Assicurati quindi che ai tuoi dispositivi sia assegnata una Configurazione.

Dopo aver collegato il tuo Account, i tuoi dispositivi sono visibili e hai assegnato loro una Configurazione, puoi iniziare a configurare i dispositivi.

Puoi aggiungere i dispositivi all'elenco di iscrizione automatica in modo che vengano iscritti automaticamente a un gruppo o a un utente specifico. Se non hai configurato nulla nell'elenco Iscrizione automatica, i dispositivi saranno iscritti al pool.

Configurazione di Windows

Configurazione di Windows

Qui hai l'opzione di abilitare le seguenti configurazioni sul tuo PC Windows 10:

Connessione DM istantanea	
Tempo iniziale di riprova	Stabilisce il primo tentativo di connessione con il dispositivo, questo valore aumenta in modo esponenziale
Tentativi di connessione	Indica il numero di tentativi di connessione che il DM-client deve effettuare in caso di errore di connessione.
Tempo massimo di sonno	Indica il tempo massimo di sospensione dopo un errore di connessione.
Primi tentativi di sincronizzazione	Intervalli in cui il dispositivo deve comunicare con il server, dopo la prima connessione
Intervallo del primo tentativo	Si riferisce a "Primi tentativi di sincronizzazione". Qui i tempi sono indicati in minuti Ad esempio, alla voce "First Sync Retries" è indicato il valore "2" e alla voce "First Retry Interval" è indicato il valore "4 Minutes", in questo modo il dispositivo comunica 2 volte ogni 4 minuti, dopo la prima connessione.
Secondo tentativo di sincronizzazione	Intervalli in cui il dispositivo deve comunicare con il server, dopo aver completato i "Primi tentativi di sincronizzazione".
Intervallo di ripetizione di un secondo	Il principio è lo stesso di "Intervallo di primo tentativo", solo che in questo caso si applica a "Secondo tentativo di sincronizzazione".
Riproduzione regolare della sincronizzazione	Intervalli, la frequenza con la quale il dispositivo deve comunicare con il server in futuro Predefinito: "Infinito" Si consiglia di non modificare questo valore, perché se si inserisce "10", il dispositivo comunicherà con il server per 10 volte e poi si fermerà Pertanto, la comunicazione con il server AppTec360 viene interrotta!
Intervallo regolare di ripetizione	Lo stesso principio di "Intervallo primo/secondo tentativo", solo che in questo caso applica le impostazioni per il futuro.
Intervallo regolare di ripetizione	Lo stesso principio di "Intervallo primo/secondo tentativo", solo che in questo caso applica le impostazioni per il futuro.

ContentBox

Configurazione

Qui puoi configurare il ContentBox. Puoi inserire nella ContentBox i file per i gruppi a cui puoi accedere con l'App ContentBox sul dispositivo.

Abilita il ContentBox	Abilita il ContentBox. Disabilitando questa opzione se non utilizzi il ContentBox, puoi risparmiare risorse sui computer OnPremise.
Usa un'installazione esterna di ContentBox	Il ContentBox può essere utilizzato anche con il tuo Nextcloud.
URL	URL completo dell'entità Nextcloud
Utente principale	Utente root dell'account Nextcloud
Password di root	Password di root dell'account Nextcloud
Permessi predefiniti per le cartelle del gruppo	Permessi predefiniti per le cartelle di gruppo, modificabili individualmente per gruppo (in Gestione cellulare)
Condividi la cartella del gruppo con i sottogruppi	Se attivo, ogni sottogruppo può leggere tutte le cartelle del gruppo principale; può anche essere configurato individualmente per ogni gruppo (Gestione cellulare)
Permessi per i sottogruppi	Permessi per i sottogruppi può essere configurato individualmente per ogni gruppo (Gestione mobile).
Consenti la condivisione	Permette all'utente di condividere i contenuti tramite link; può essere configurato individualmente per ogni gruppo.
Dimensione massima del file caricato in MB	Dimensione massima di un file Standard: 512 MB Configurazione massima: 2048
Credenziali WebDAV	
URL WebDAV	Puoi anche aprire il ContentBox con WebDAV. Non eliminare in nessun caso le seguenti cartelle: /apptecgroups /apptecgroups/AppTecGroup-X
Utente principale	Nome degli utenti principali
Password	Password degli utenti root

La sincronizzazione con il ContentBox avviene automaticamente. Puoi tuttavia eseguire una sincronizzazione manuale con "Sincronizza ContentBox".

Inoltre, qui puoi attivare/disattivare il ContentBox su ogni singolo dispositivo.

Questo è rilevante solo se non hai concesso una licenza aggiuntiva per il ContentBox, ma hai comunque accesso a 25 dispositivi con cui puoi testare il ContentBox - qui puoi attivarlo per i rispettivi dispositivi.

Configurazione LDAP

Panoramica su LDAP

Qui puoi stabilire una connessione alla tua Active Directory tramite LDAP per importare in massa utenti e gruppi. La sincronizzazione deve essere eseguita manualmente. Puoi configurare più connessioni LDAP a sistemi diversi o con configurazioni/filtri diversi.

Nome del server	Il nome visualizzato del server
Tipo	Attualmente sono supportate solo le Active Directory che supportano LDAP.
Dominio LDAP	Il dominio LDAP primario (es. example.com)
Host LDAP	È necessario solo se l'host LDAP non è raggiungibile nel dominio LDAP indicato.
Porto	Lascia vuoto per utilizzare la porta standard (389 o 636 per SSL).
Nome utente	Ad esempio, CN=John,OU=Users,DC=EXAMPLE,DC=COM Nota: la maggior parte dei sistemi richiede il nome utente in questo formato e non accetta "John" come nome utente.
Password	
Conferma la password	
Sicurezza delle connessioni	Nota: quando si utilizza SSL o TLS, verrà controllato il certificato di Active Directory. Se è autofirmata, devi aggiungere la CA principale all'archivio di fiducia del computer OnPremise. Se si utilizza il Cloud, l'Active Directory deve fornire un certificato attendibile, altrimenti la connessione funzionerà solo senza crittografia.
Sincronizzazione automatica.	Abilita la sincronizzazione automatica della directory LDAP nell'intervallo di tempo specificato nelle impostazioni generali di LDAP.
DN base	Se non vuoi sincronizzare l'intera directory, puoi specificare una OU. Ad esempio OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Membro di	Tutti gli utenti importati saranno aggiunti al gruppo selezionato.
Solo gli utenti attivati?	Quando è abilitato, l'attributo userAccountControl sarà preso in considerazione; gli utenti senza tale attributo non saranno importati.
Filtro LDAP	Puoi utilizzare il filtro LDAP per filtrare gli utenti che vengono importati.
Filtro Regex	Puoi utilizzare il filtro Regex per filtrare quali utenti vengono importati

Collegamento di prova	Verifica la connessione quando si salva la configurazione
Ripristinare la struttura delle directory durante la sincronizzazione?	Se è vero, tutte le voci LDAP saranno spostate nella loro posizione originale nell'albero LDAP. Si consiglia di abilitarlo.
Importare nuovamente gli utenti e i gruppi cancellati?	Se abilitato, gli utenti e i gruppi che sono stati eliminati saranno ricreati. Si consiglia di abilitarlo.
Cancellazioni di sincronizzazione?	Se abilitato, i gruppi e gli utenti verranno eliminati quando vengono cancellati dal server LDAP. Anche i dispositivi degli utenti cancellati verranno eliminati.

Sotto l'elenco delle tue configurazioni LDAP puoi definire il periodo in cui il sistema si sincronizza automaticamente. Utilizza solo le configurazioni LDAP per la sincronizzazione automatica che hanno attivato l'opzione corrispondente.

Gestione delle app

App DB in-house

Android

Qui puoi caricare le applicazioni Android che la tua azienda ha sviluppato e distribuirle in seguito in Mobile Management nei profili dei dispositivi o dei gruppi.

Ti ricordiamo che consigliamo di distribuire in questo modo solo le applicazioni che non sono disponibili nel Google Play Store.

Clicca sul "+" per caricare l'APK di un'applicazione che vuoi caricare. Attualmente è supportato solo il formato APK.

Il limite di upload sulle appliance OnPremise può essere aumentato nel passaggio 3 della configurazione dell'appliance. Se desideri aumentare il limite di caricamento su Cloud, contatta l'assistenza per maggiori informazioni.

Tieni presente che di solito gli APK sono un po' più piccoli del loro contenuto. È possibile che il caricamento fallisca per questo motivo, poiché l'APK viene scompattato durante il processo. Ad esempio, è possibile che un APK di 95 MB non riesca a funzionare con un limite di upload di 100 MB. In questo caso, aumenta il limite di upload come indicato sopra.

Ti consigliamo inoltre di spostare manualmente l'APK su un dispositivo di prova (ad esempio tramite USB) e di provare a installarlo manualmente con l'app Files del dispositivo. Se questo non funziona per qualsiasi motivo, fallirà anche tramite MDM.

Obiettivo di aggiornamento

Con la funzione "Obiettivo di aggiornamento" puoi scegliere quale versione di un'app deve essere installata o a quale versione un'app deve essere aggiornata se hai attivato "Mantieni aggiornato" per un'app.

Se non hai selezionato un obiettivo di aggiornamento, verrà utilizzata la versione più alta.

Tieni presente che Android non può effettuare il downgrade delle applicazioni. Tieni presente che il "Codice versione" determina se una versione è superiore, inferiore o uguale. Assicurati quindi di aumentare correttamente questa versione nella tua applicazione quando crei un aggiornamento.

iOS

Qui puoi caricare le app iOS che hai sviluppato e distribuirle successivamente in Gestione dispositivi mobili nel profilo del tuo dispositivo o gruppo.

Clicca sul "+" per caricare l'IPA dell'app che vuoi caricare. Al momento è supportato solo il formato IPA.

Il limite di upload sulle appliance OnPremise può essere aumentato nel passaggio 3 della configurazione dell'appliance. Se desideri aumentare il limite di caricamento su Cloud, contatta l'assistenza per maggiori informazioni.

Obiettivo di aggiornamento

Con la funzione "Obiettivo di aggiornamento" puoi scegliere quale versione di un'app deve essere installata o a quale versione un'app deve essere aggiornata se hai attivato "Mantieni aggiornato" per un'app.

Se non hai selezionato un obiettivo di aggiornamento, verrà utilizzata la versione più alta.

MacOS

Qui puoi caricare le app MacOS che hai sviluppato e distribuirle successivamente in Gestione dispositivi mobili nel profilo del tuo dispositivo o gruppo.

Clicca sul "+" per caricare il PKG di un'applicazione che vuoi caricare. Al momento è supportato solo il formato PKG.

Il limite di upload sulle appliance OnPremise può essere aumentato nel passaggio 3 della configurazione dell'appliance. Se desideri aumentare il limite di caricamento su Cloud, contatta l'assistenza per maggiori informazioni.

Obiettivo di aggiornamento

Con la funzione "Obiettivo di aggiornamento" puoi scegliere quale versione di un'applicazione deve essere installata o a quale versione un'applicazione deve essere aggiornata se hai attivato "Mantieni aggiornato" per un'applicazione.

Se non hai selezionato un obiettivo di aggiornamento, verrà utilizzata la versione più alta.

Windows 10

Qui puoi caricare le app di Windows 10 e distribuirle successivamente in Gestione dispositivi mobili nel profilo del tuo dispositivo o gruppo.

Clicca sul "+" per caricare l'APPX, l'APPXBUNDLE o l'MSI di un'applicazione che vuoi caricare. Al momento è supportato solo il formato APPX, APPXBUNDLE o MSI.

Puoi anche caricare e definire le dipendenze di un'app, che verranno distribuite e installate automaticamente prima di installare l'app desiderata.

Il limite di upload sulle appliance OnPremise può essere aumentato nel passaggio 3 della configurazione dell'appliance. Se desideri aumentare il limite di caricamento su Cloud, contatta l'assistenza per maggiori informazioni.

Obiettivo di aggiornamento

Con la funzione "Obiettivo di aggiornamento" puoi scegliere quale versione di un'applicazione deve essere installata o a quale versione un'applicazione deve essere aggiornata se hai attivato "Mantieni aggiornato" per un'applicazione.

Se non hai selezionato un obiettivo di aggiornamento, verrà utilizzata la versione più alta.

Pacchetto Win32 (.exe)

Puoi anche distribuire file .exe/installatori ai tuoi dispositivi.

Nome del pacchetto	Il nome che verrà visualizzato nell'MDM
Descrizione	Descrizione mostrata nell'MDM
File del pacchetto	Sono ammessi solo i file .zip. Inserisci i file che vuoi distribuire in questo file zip.
Contesto di distribuzione	**Sistema**: Il comando di installazione viene eseguito con privilegi di sistema superiori a quelli di "Utente". Inoltre, quando si utilizza "System" il processo non ha un'interfaccia utente, quindi sarà silenzioso e il profilo dell'utente, ad esempio le variabili d'ambiente come %AppDat%, non è accessibile. **Utente**: il comando di installazione ha accesso al profilo utente e può visualizzare l'interfaccia utente se necessario. Nota: alcuni processi possono funzionare solo in un contesto. Ad esempio, se un software si installa in AppData, funzionerà solo quando si seleziona "Utente".
Installa il comando	Il comando utilizzato per installare il programma. Ad esempio, il comando di installazione per un file zip contenente "setup.exe" nella sua radice, che supporta il parametro "/s" per un'installazione silenziosa, sarà "setup.exe /s". Tieni presente che i diversi software possono avere parametri diversi.
Comando di disinstallazione	Il comando da eseguire per disinstallare il software tramite MDM. Di solito questo indica il programma di disinstallazione. Ad esempio "C:\Program Files\ExampleSoftware\uninstall.exe".
Requisiti	
Nota: affinché il software venga installato, devono essere soddisfatti tutti i requisiti indicati. Altrimenti non verrà installato. Alcuni campi possono essere obbligatori. Se non viene impostato alcun valore per un requisito, il requisito verrà ignorato.	
Architettura del sistema operativo	Architettura del sistema operativo
Versione minima del sistema operativo	Versione minima del sistema operativo
Spazio libero minimo su disco (MB)	Spazio libero minimo su disco (MB)

Memoria fisica minima (MB)	Memoria fisica minima (MB)
Numero minimo di processori logici	Numero minimo di processori logici
Velocità minima della CPU (MHz)	Velocità minima della CPU (MHz)
Requisiti aggiuntivi	Se vuoi, puoi anche definire manualmente delle regole o caricare uno script per eseguire ulteriori controlli sui requisiti.
Regole di rilevamento	
Metodo di rilevamento	Qui puoi definire come rilevare se l'app è installata sul dispositivo. I comandi di installazione verranno eseguiti solo quando queste regole rilevano che l'applicazione NON è installata. I comandi di disinstallazione vengono eseguiti solo quando queste regole rilevano che l'applicazione non è installata. **Definizione manuale delle regole**: Ti permette di definire manualmente una o più regole per verificare, ad esempio, la presenza di un determinato file, cartella, MSI o chiave di registro. Se tutte le regole di rilevamento indicate sono vere, l'applicazione sarà considerata presente. **Usa script**: Carica il tuo script con i tuoi controlli. Se lo script restituisce "$TRUE", l'applicazione sarà considerata presente.
Regole di rilevamento	

Impostazioni dell’app

Impostazioni dell’app iOS

Qui puoi definire le impostazioni predefinite per l'aggiunta di un'applicazione all'app store obbligatorio o all'app store aziendale.

Nota: questo imposta solo ciò che è selezionato di default quando si aggiungono le app. Questo NON modifica le impostazioni esistenti per le app già aggiunte nell'app store obbligatorio o nell'app store aziendale.

Tieniti aggiornato	Mantiene automaticamente l'app aggiornata. Tieni presente che possono trascorrere fino a 7 giorni dal rilascio di un aggiornamento prima che l'app venga aggiornata.
Superare quando non è gestito	Se un'app è già stata installata come non gestita (dall'utente), l'app verrà superata e gestita dall'MDM.
Rimuovi l'app quando il profilo MDM viene rimosso	Disinstalla l'app quando l'MDM viene rimosso.
Impedisci il backup dei dati dell'app	Impedisce il backup dei dati dell'app.

Impostazioni dell’app Android

Qui puoi definire le impostazioni predefinite per l'aggiunta di un'applicazione all'app store obbligatorio o all'app store aziendale.

Nota: questo imposta solo ciò che viene selezionato per impostazione predefinita al momento dell'aggiunta. Questo NON modifica le impostazioni delle app già aggiunte nell'app store obbligatorio o nell'app store aziendale.

Tieniti aggiornato	Mantiene automaticamente l'app aggiornata. Disponibile solo per le applicazioni InHouse.
Aggiornamento del client EMM controllato AppTec360	Se abilitato, gli amministratori possono specificare il target di aggiornamento per AppTec360 EMM Client. L'elenco di tutte le versioni disponibili del client EMM AppTec360 sarà visualizzato in "Impostazioni generali" → "Gestione delle app" → "DB delle app in-house" → "Android".

Applicazioni di terze parti

Android

Qui puoi impostare il tuo codice di attivazione per Ikarus.

Imposta questa opzione su "Usa codice di attivazione" e inserisci qui il tuo codice di attivazione.

Nota: dopo aver inserito il codice e salvato, il codice non viene ancora aggiunto al profilo che viene inviato al dispositivo. Per aggiungere il codice al profilo, devi effettuare una modifica al tuo profilo. Ad esempio, modifica un interruttore del profilo da off → on → off - Salva → Assegna ora.

iOS

Qui puoi inserire la tua licenza SecurePIM. Dopo aver inserito la licenza, premi "Salva modifiche" e potrai utilizzare le opzioni di SecurePIM.

VPP / KNOX Premium

Il Volume Purchase Program (VPP) di Apple ti permette di distribuire facilmente applicazioni gratuite e a pagamento sui tuoi dispositivi. Questa soluzione è altamente consigliata in quanto non è necessario un ID Apple sui dispositivi, gli utenti non devono confermare l'installazione (supervisionata), gli utenti non devono inserire la password dell'ID Apple e puoi distribuire facilmente le app a pagamento senza doverle acquistare nuovamente su ogni dispositivo.

Per utilizzare il VPP devi registrarti nell'Apple Business Manager.

Licenze VPP

Qui puoi avere una panoramica delle tue applicazioni VPP, quante licenze sono utilizzate e quante sono disponibili.

Cliccando sulla Ruota potrai vedere quali dispositivi hanno una licenza assegnata e qual è lo stato di questa assegnazione.

Cliccando su aggiorna la Cache VPP che confronta le licenze assegnate nell'MDM con le licenze assegnate sul lato Apple. In alcuni casi questo può risolvere i problemi di licenza.

Gettone VPP

Qui puoi caricare il tuo VPP Token, che puoi trovare nell'Apple Business Manager in Impostazioni → App e Libri. Puoi caricare più gettoni VPP.

Puoi rinnovare un Token semplicemente scaricandone uno nuovo nell'Apple Business Manager, cliccando sulla ruota "Modifica" e caricando il nuovo Token.

La "Modalità VPP" decide come viene gestita l'assegnazione della licenza. A seconda dello scenario, dovrai utilizzare modalità diverse:

"Basato sul dispositivo" deve essere utilizzato quando si registrano i dispositivi tramite QR Code, Link, Apple Configurator o DEP.

"Basato sull'utente" è necessario se i dispositivi sono registrati con l'iscrizione dell'utente o come iPad condiviso.

Se attivi la "Gestione automatica delle licenze", agli utenti spostati da un gruppo all'altro verranno automaticamente assegnate le licenze Apple VPP in base al profilo del gruppo in cui sono stati spostati.

Le licenze Apple VPP esistenti del gruppo da cui sono state trasferite non saranno revocate.

Ai nuovi utenti aggiunti a un gruppo verranno automaticamente assegnate le licenze Apple VPP in base al rispettivo profilo del gruppo.

Chiave KNOX Premium

Qui puoi inserire la tua KNOX Premium Key per utilizzare il Samsung KNOX Container.

Tieni presente che questa funzione non è più supportata da Android 10. Usa invece l'Android Enterprise Container.

Impostazioni dell’App Store

Regione e lingua

Qui puoi impostare la lingua e la regione predefinite per la ricerca delle app in Gestione applicazioni.

Tieni presente che l'impostazione di iTunes definisce anche il modo in cui il sistema acquisisce le informazioni su determinate app. Se nei tuoi elenchi ci sono applicazioni che vengono visualizzate in modo strano (ad esempio, senza icona), forse hai impostato una regione in cui l'applicazione specifica non è disponibile.

AE Play Store

Qui puoi trovare tutte le opzioni del Play Store per dispositivi Android Enterprise per approvare le applicazioni, caricare le tue applicazioni sul Play Store o creare le tue applicazioni web.

Applicazioni approvate

Qui puoi avere una panoramica di tutte le applicazioni che hai approvato.

Applicazioni del Play Store

In questo modo verrà caricato un iFrame che mostra il Play Store. Cerca l'applicazione che desideri, cliccaci sopra e approvala. Durante l'approvazione dell'app puoi anche definire che l'approvazione venga revocata se i permessi richiesti cambiano. Si consiglia di lasciare queste impostazioni predefinite quando si approvano le applicazioni.

Dopo che un'app è stata approvata, puoi aggiungerla ai tuoi profili.

Il pulsante "Approva" cambierà in "Revoca approvazione" dopo l'approvazione, in modo che tu possa sempre rimuovere le applicazioni se non ne hai più bisogno.

Applicazioni private

Qui puoi caricare la tua applicazione come applicazione privata sul Google Play Store. Questo ti permette di distribuire l'app attraverso i servizi di Google e di aggiornarla attraverso di essi. Questo ha

anche il vantaggio che le tue applicazioni possono essere installate senza la conferma dell'utente che normalmente è necessaria.

Applicazioni web

Qui puoi creare delle Web App, ovvero dei link a determinate pagine web che possono essere assegnate come App.

Puoi anche assegnare un'icona personalizzata e definire ulteriormente il modo in cui viene visualizzata.

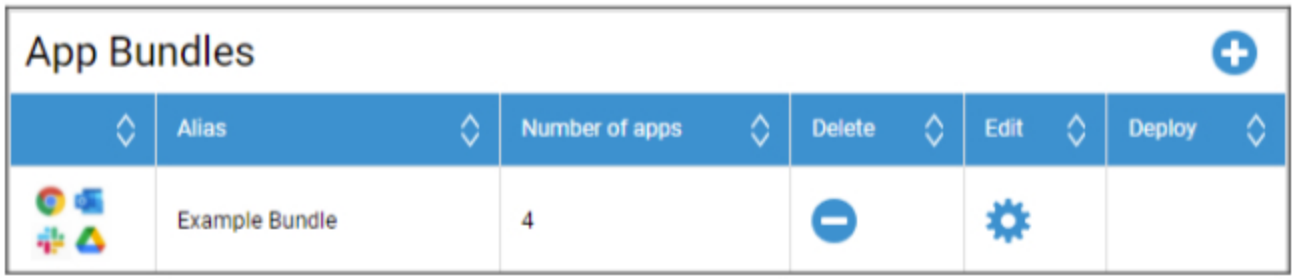
Layout del negozio

Il Layout dello Store definisce il modo in cui le app vengono visualizzate nel Play Store o se vengono visualizzate affatto.

Tieni presente che se vuoi mostrare le applicazioni del Play Store che l'utente deve installare manualmente, queste devono essere aggiunte qui nel layout. **E** nel profilo del Play Store aziendale. Se aggiungi un'app a una sola di esse, non verrà visualizzata.

Pacchetto di applicazioni

Con i bundle di app puoi definire gruppi di applicazioni che possono essere assegnate ai profili dei dispositivi o dei gruppi con un solo clic.



Clicca sul "+" per creare un nuovo bundle di app. Dopo aver creato un bundle di app, puoi cliccare su "Modifica" per aggiungere al bundle app provenienti da varie fonti.

I bundle possono essere aggiunti ai profili come tutte le altre app. Quando aggiungi le applicazioni, avrai una scheda aggiuntiva denominata "App Bundles" in cui sono presenti i tuoi bundle.

Se apporti una modifica a un bundle di applicazioni, apparirà un pulsante nella colonna "Deploy". In questo modo potrai inviare le modifiche a tutti i profili che contengono questo bundle. Tieni quindi presente che dovrai farlo manualmente dopo aver aggiunto o rimosso le app in un bundle.

Telecomando

TeamViewer

Connettore TeamViewer

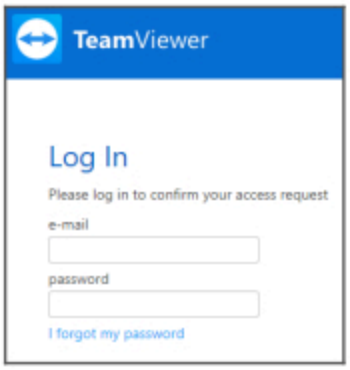
Nota: nella versione di prova gratuita della nostra versione cloud non puoi collegare il tuo account TeamViewer. Avrai invece un conto demo gratuito collegato automaticamente.

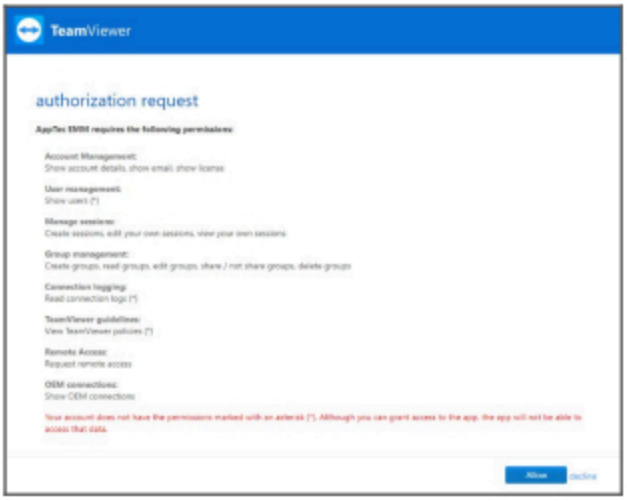
Vai su Impostazioni generali -> Controllo remoto -> TeamViewer. Qui puoi collegare il tuo account TeamViewer alla console o vedere le informazioni sul tuo account attualmente connesso. Inoltre, se vai su "Sessioni attive", puoi visualizzare tutte le sessioni attualmente attive.

Per collegare il tuo account clicca su "Avvia configurazione".

In questo modo verrai indirizzato a una nuova pagina in cui dovrai effettuare il login con il tuo account TeamViewer.

Dopo aver effettuato il login, devi autorizzare AppTec360 MDM a utilizzare questo account. Dopo aver confermato, dovrai attendere qualche secondo e l'account sarà connesso.


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


TeamViewer
authorization request

Installare TeamViewer QuickSupport

Aggiungi l'applicazione "TeamViewer QuickSupport" alle applicazioni obbligatorie del profilo del tuo dispositivo o del tuo gruppo e clicca su "Assegna ora". Attendi che l'app sia installata sul dispositivo.

Se provi ad accedere a un dispositivo su cui l'app non è installata, verrà installata o ti verrà chiesto di installarla, a seconda della configurazione del dispositivo.

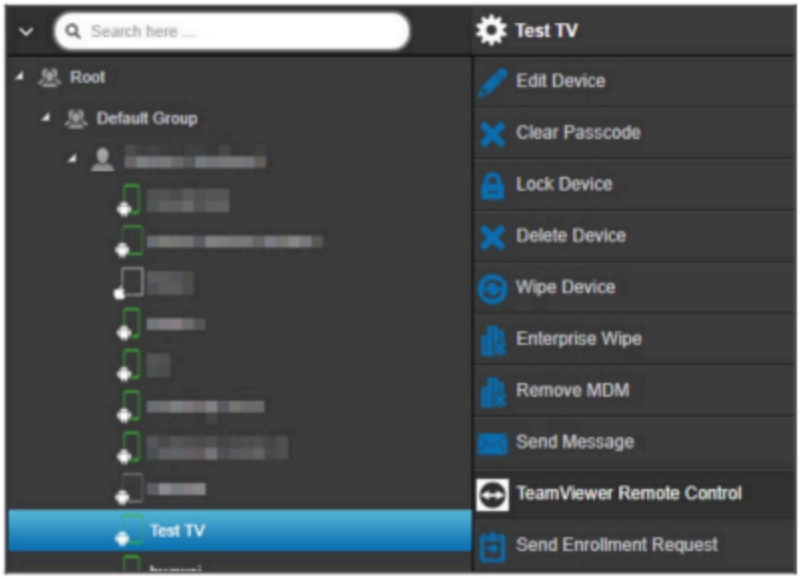
Controlla a distanza il tuo dispositivo

Per controllare a distanza il tuo dispositivo, seleziona il dispositivo, clicca sulla rotella e scegli "Controllo remoto TeamViewer".

Se c'è già una sessione attiva, puoi utilizzare la vecchia sessione o crearne una nuova.

Conferma di voler creare una nuova sessione di TeamViewer.

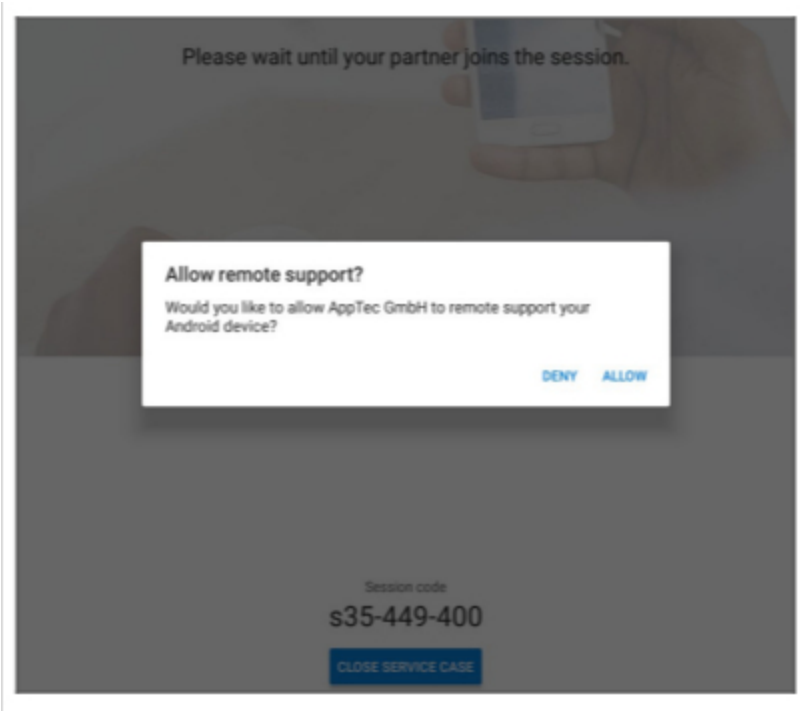
Dopo pochi secondi otterrai un link per la tua sessione TeamViewer. Puoi cliccare su "Inizia" per aprire questo link in una nuova finestra.


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

Questo link aprirà il TeamViewer installato e ti collegherà al tuo dispositivo.

Ora devi confermare la connessione sul dispositivo stesso per poterlo controllare a distanza.

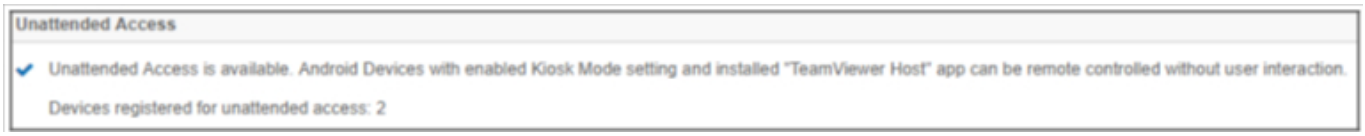


Se stai utilizzando iOS, riceverai un messaggio nel client MDM di AppTec360. Con questo collegamento il dispositivo si unirà alla sessione remota. A seconda delle impostazioni di notifica del dispositivo, è possibile che non riceva una notifica e che debba aprire manualmente AppTec360 MDM Client.

Su alcuni dispositivi Android (ad esempio Samsung) è necessario installare un'applicazione aggiuntiva come addon. L'applicazione TeamViewer sul dispositivo ti informerà su questo aspetto, se è necessario sul tuo dispositivo.

Accesso non presidiato

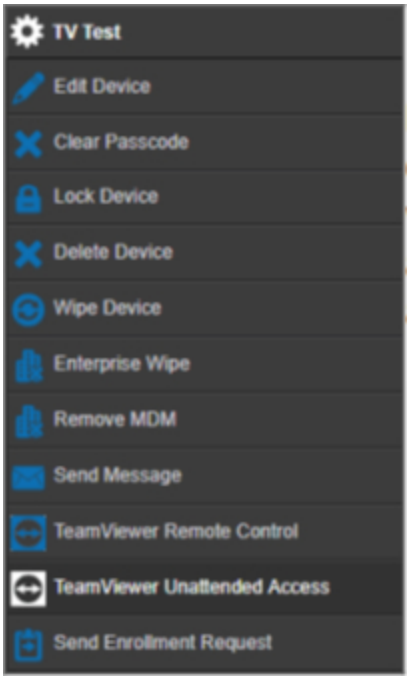
Nota: l'accesso non presidiato è possibile solo sui dispositivi Android.



Puoi connetterti ai tuoi dispositivi, senza accettare la connessione sul dispositivo, solo se il tuo account TeamViewer utilizza una licenza "Tensor" o "Corporate".

Puoi controllare questo aspetto, dopo aver collegato il tuo account, in "Impostazioni generali".

Per utilizzare l'accesso non presidiato, devi installare l'applicazione "TeamViewer Host" e attivare "Abilita accesso non presidiato" alla voce "Modalità Kiosk & Launcher" del tuo profilo. Tieni presente che questo è possibile solo se utilizzi la modalità Chiosco.



Ora puoi selezionare l'accesso non presidiato selezionando il tuo dispositivo e cliccando sulla rotella. In questo modo ti connetterai al tuo dispositivo senza bisogno di conferme sul dispositivo stesso. Tieni presente che potrebbero essere necessari alcuni istanti prima di ottenere il link per accedere al tuo dispositivo.

Splashtop

Se attivi l'opzione Splashtop, vedrai le opzioni di configurazione di Splashtop nei tuoi profili.

Per utilizzare Splashtop, devi impostare Splashtop Streamer (com.splashtop.streamer.csrs) come app obbligatoria nel tuo profilo. Successivamente potrai abilitare la configurazione di Splashtop nel tuo profilo in "Controllo remoto". Abilitando questa opzione si configura l'applicazione Splashtop Streamer. Se stai usando Splashtop Streamer ma non in combinazione con l'MDM, dovresti lasciare questa opzione disattivata.

Nel tuo profilo, alla voce "Controllo remoto", dovrai anche impostare un codice di distribuzione. Vai su https://my.splashtop.com e accedi al tuo account Splashtop. Clicca su "Aggiungi computer" e copia il codice di distribuzione di 12 cifre dalla pagina risultante.

Senza il Deploy Code il controllo remoto NON è possibile.

Dopo aver fatto ciò, puoi cliccare con il tasto destro del mouse sul tuo dispositivo e avviare una sessione remota cliccando su "Splashtop Remote Control".

Gestione della scheda Sim

Importazione massiva CSV

Mostra una panoramica delle Sim Card assegnate e tutte le informazioni su di esse. Questo ti aiuta ad avere tutte le informazioni, non solo sui tuoi dispositivi ma anche sulle tue Sim Card, in un unico sistema.

NOTA: Si tratta di una gestione/documentazione manuale. Non è possibile ottenere questi dati automaticamente dai dispositivi a causa dei meccanismi di privacy/sicurezza dei sistemi operativi.

Puoi anche importare questo elenco come CSV.

Vettore e tariffa

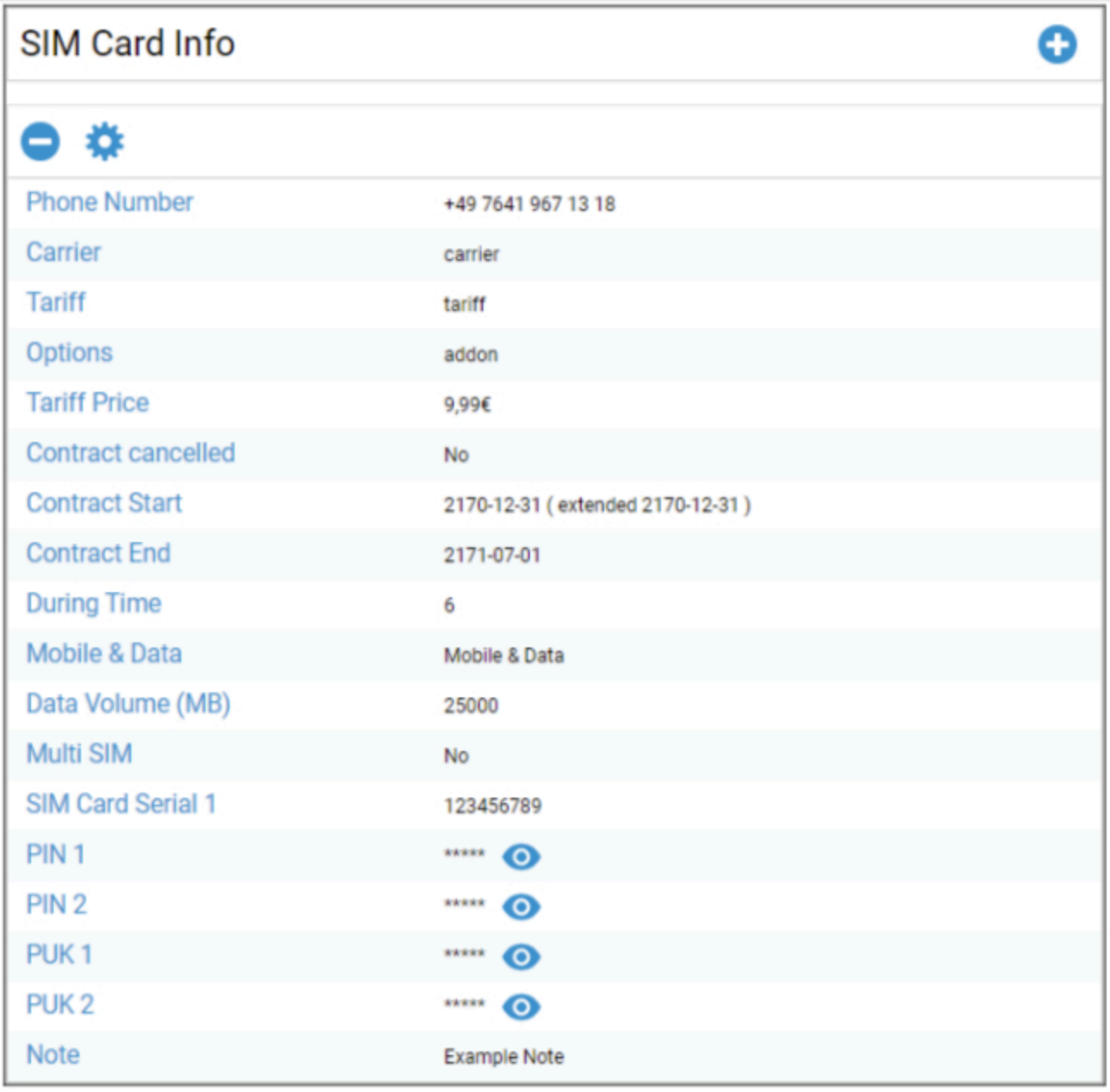
Per aggiungere una scheda Sim, clicca prima sul pulsante per aggiungere uno o più operatori.

Successivamente clicca sul "+" in "Informazioni sulle tariffe" per aggiungere una tariffa a un vettore.

Se hai qualcosa di simile, puoi aggiungere degli Add-On opzionali qui sotto.

Questo ha preparato tutto ciò di cui hai bisogno per aggiungere una scheda Sim vera e propria. Le schede Sim sono attualmente assegnate a un utente. Pertanto, accedi alla Gestione cellulare, seleziona un utente e vai a "Panoramica della scheda Sim".

Qui puoi vedere le schede Sim di questi utenti. Se c'è, puoi modificarlo o rimuoverlo. Gli utenti possono avere più schede Sim.

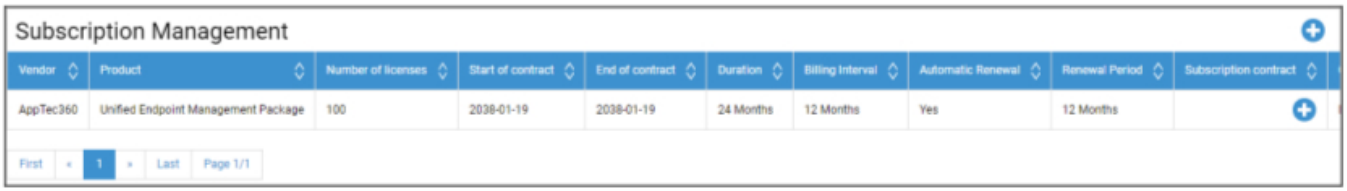


Clicca sul "+" per aggiungere una scheda Sim e aggiungi tutte le informazioni necessarie. Queste schede Sim saranno anche elencate nella lista di tutte le tue schede Sim in Impostazioni generali → Gestione schede Sim.

Gestione degli abbonamenti

Gestione degli abbonamenti

Qui puoi documentare gli abbonamenti in corso, i loro dettagli e anche archiviare diversi file, ad esempio il contratto firmato, la lettera di disdetta, ecc. Puoi anche impostare dei promemoria che ti ricordano per posta prima della scadenza dell'abbonamento e magari lo prolungano automaticamente.



Clicca sul "+" in alto per aggiungere un abbonamento. Puoi aggiungere tutti gli abbonamenti che vuoi.

Clicca sul "+" nei vari campi per caricare i file relativi a questa Sottoscrizione. Tecnicamente puoi caricare qualsiasi tipo di file, ma sappi che non tutti i tipi di file possono essere visualizzati in anteprima nel browser.

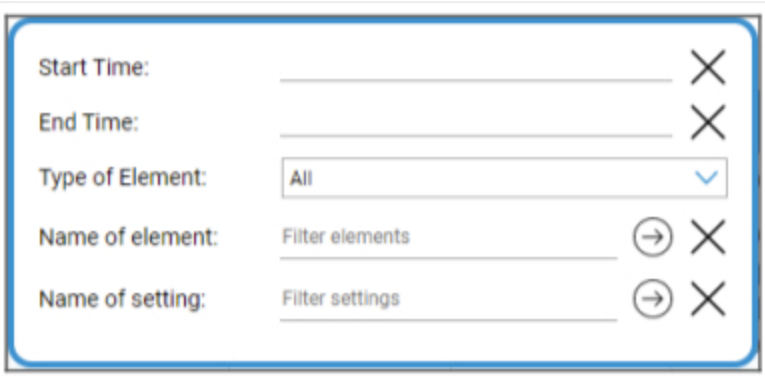
Registro di controllo generale

Registro di controllo

Qui c'è un registro di controllo generale che mostra tutte le modifiche apportate. Mentre il Registro di controllo di un utente o di un gruppo mostra solo le modifiche relative a tale utente o gruppo, questo mostra OGNI modifica effettuata in qualsiasi punto della console.

Puoi vedere cosa è stato modificato, da chi, quando e dove. In alcuni casi puoi anche estendere la voce per vedere ulteriori dettagli.

È possibile fare clic sull'utente o sulla voce in "Percorso / Tipo" per raggiungere la posizione in cui è stata effettuata la modifica.



In alto a destra puoi anche definire un filtro che può aiutarti a trovare determinati cambiamenti in un ambiente in cui ne avvengono molti.

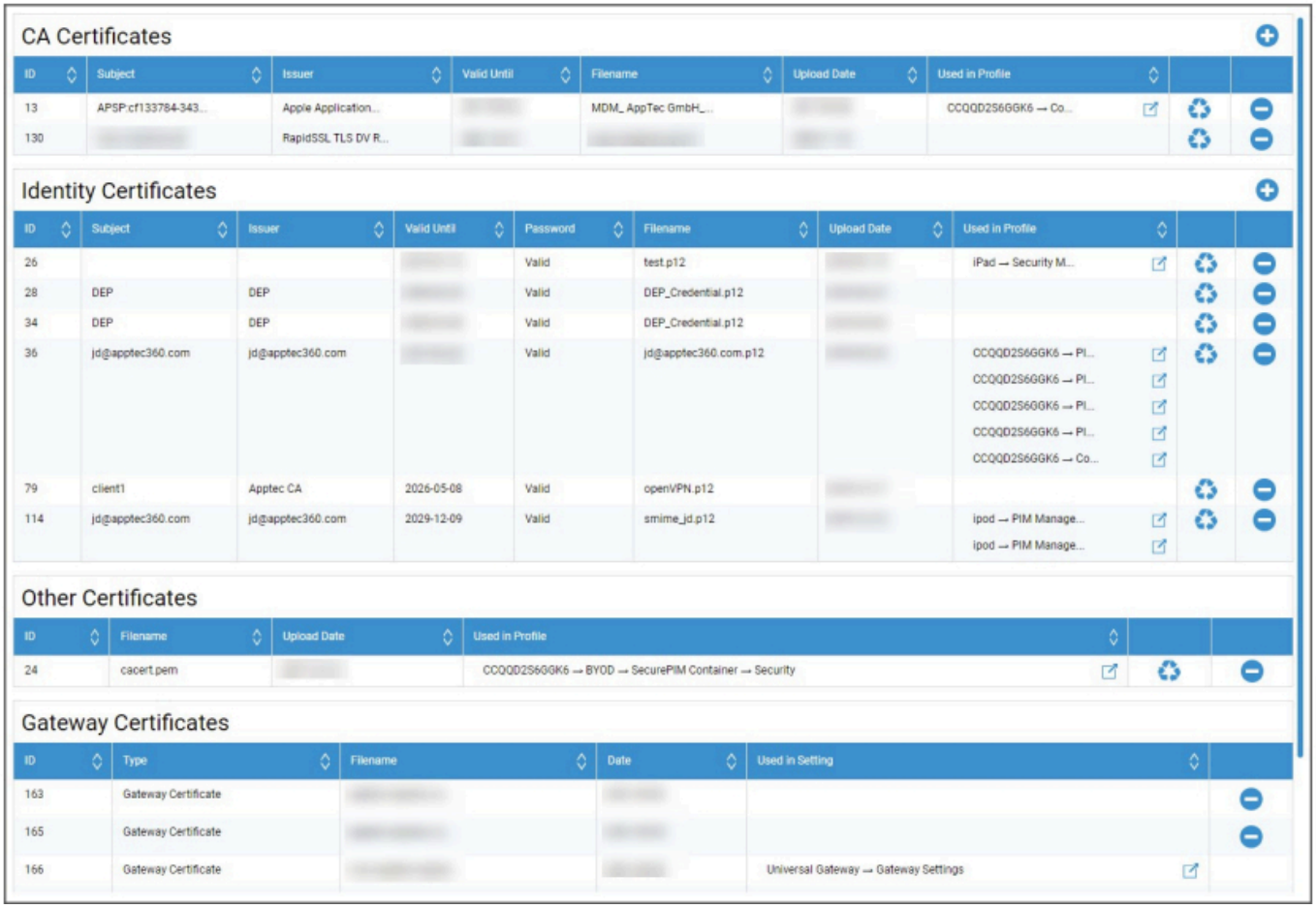
Impostazioni del registro di audit

"Periodo di conservazione dei registri di audit" definisce per quanto tempo i registri di audit devono essere conservati prima di essere eliminati.

Gestione dei certificati

Qui potrai avere una panoramica di tutti i certificati caricati e utilizzati nella Console. Questa è solo una panoramica. La configurazione vera e propria dei certificati Wi-Fi, ad esempio, viene effettuata nel profilo nella posizione corrispondente.

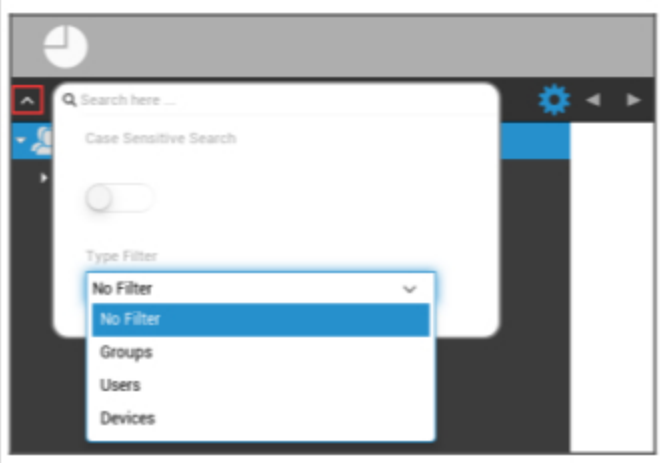
Qui puoi anche rimuovere o aggiornare i certificati, che si rifletteranno automaticamente sui profili interessati. Clicca sulle informazioni in "Usato nel profilo" per vedere dove sono assegnati i certificati.



Gestione dei dispositivi mobili

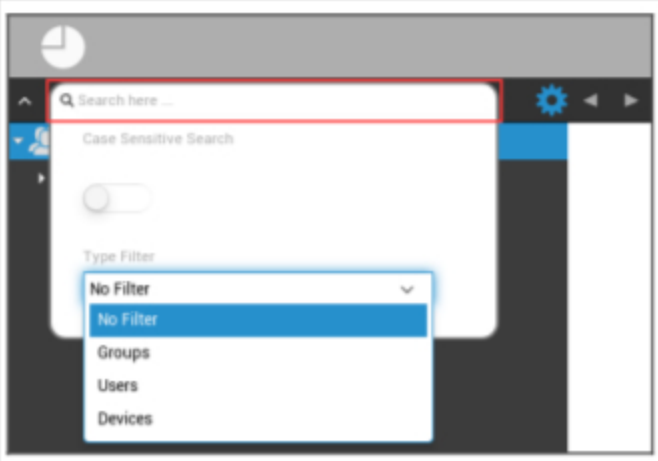
Schermata di gestione dei dispositivi mobili

Filtro del dispositivo



Con un clic nell'angolo superiore sinistro dello schermo, puoi trovare una serie di filtri per la visualizzazione dei dispositivi.

Finestra di ricerca



La finestra di ricerca ti permette di cercare tutti i dispositivi e/o gli utenti con una parola chiave specifica.

Ingranaggio delle opzioni

Dopo aver cliccato sul rispettivo simbolo, viene visualizzato un elenco di opzioni disponibili.

Questi cambiano con ogni finestra corrente e sono spiegati nei rispettivi capitoli.

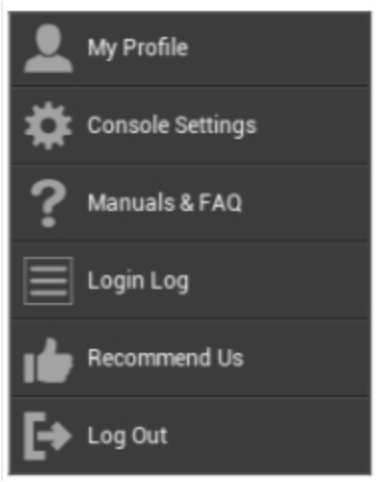
Frecce di navigazione

Cliccando sulla freccia a sinistra, verrai portato alla pagina precedente.

In seguito, cliccando sulla freccia a destra, verrai riportato alla pagina che hai appena lasciato.

Impostazioni dell’account di amministrazione

Cliccando sull'indirizzo e-mail come visto sopra, viene visualizzato il seguente menu:



Il mio profilo	Modifica i dettagli dell'account dell'amministratore
Impostazioni della console	Configura le impostazioni della console per l'account Admins
Manuali e FAQ	Visualizza la pagina "Manuali e FAQ" in "Impostazioni generali".
Registro di accesso	Accedi al "Registro di accesso"
Raccomandaci	Visualizza la pagina "Raccomandaci" nelle "Impostazioni generali".
Esci	Esci dalla console MDM

Informazioni sull’utente

Qui puoi modificare i dettagli dell'account dell'amministratore attualmente collegato.

Nome utente	Nome utente e/o indirizzo e-mail dell'account
Nome	Nome dell'amministratore
Cognome	Cognome dell'amministratore
Nome utente	Nome di login degli amministratori
Indirizzo e-mail	Indirizzo e-mail degli amministratori
Indirizzo e-mail alternativo	Indirizzo e-mail alternativo degli amministratori
Immagine	Immagine del profilo
Numero di telefono	Numero di telefono dell'amministratore
Numero di cellulare	Numero di cellulare dell'amministratore
Estensione del telefono	Estensione del telefono
Posizione	Posizione
Posizione	Posizione in azienda
Gruppo di utenti	Seleziona a quale gruppo di utenti vuoi assegnare l'account di amministratore
Commento	Inserisci un commento
Inserisci la nuova password	Inserisci la password per cambiare la password
Ripeti la nuova password	Ripeti la nuova password per confermarla

Tieni presente che l'accesso all'amministrazione può essere archiviato anche come account utente locale nella struttura gerarchica. Senza l'istituzione di un ulteriore amministratore, questo non dovrebbe essere cancellato!

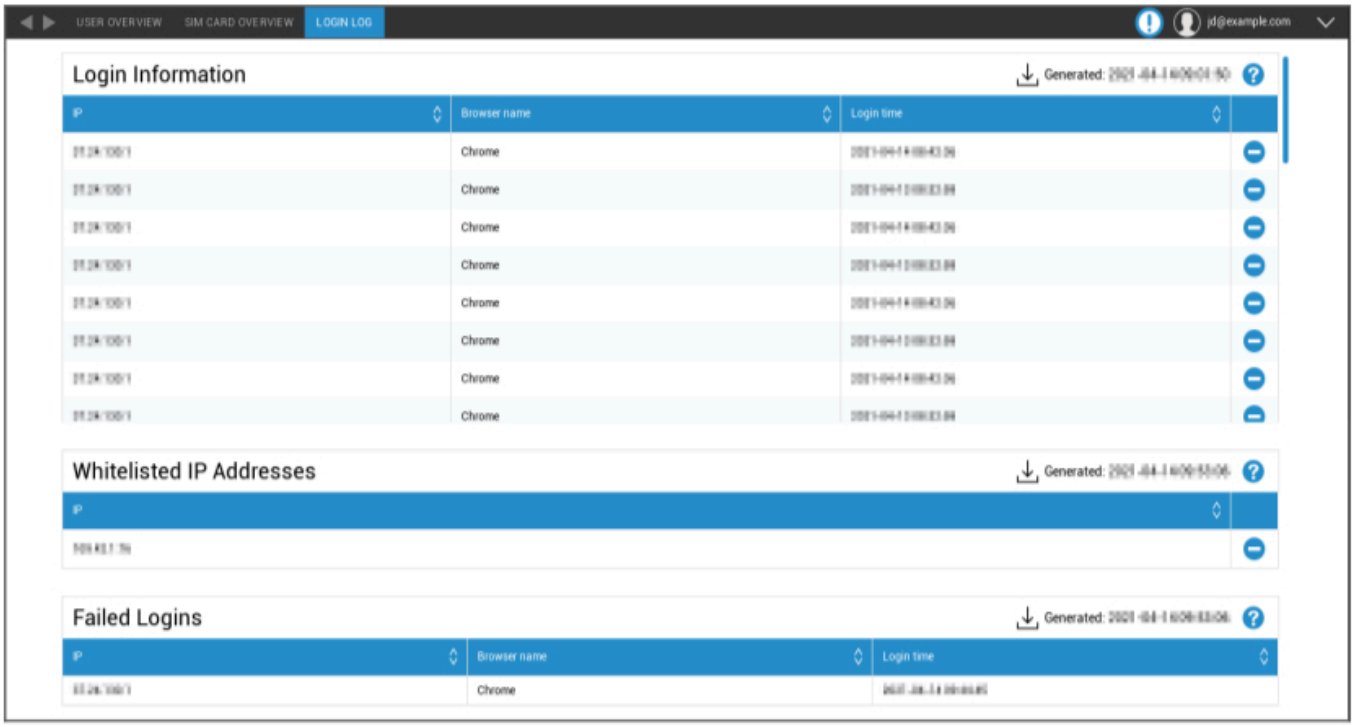
Impostazioni della console

Qui puoi configurare le seguenti impostazioni della console per l'account Admins:

Opzioni di visualizzazione della directory utenti	Definisci il modo in cui gli utenti devono essere etichettati nell'albero
Opzioni di visualizzazione del dispositivo directory	Definisci come devono essere etichettati i dispositivi nella struttura ad albero
Timeout della sessione	Se l'utente non fa nulla nel tempo specificato, verrà disconnesso. Il valore predefinito è 60 minuti. Effettua il logout e riaccedi dopo aver modificato questa impostazione.
Fuso orario	Scegli il fuso orario da utilizzare
Formato del tempo	Scegli come visualizzare i timestamp
Lingua della console	Scegli la lingua in cui visualizzare la console. Sono disponibili l'inglese e il tedesco.
Colore principale	Puoi impostare un colore che verrà utilizzato come base per la combinazione di colori della console. Puoi utilizzare il selezionatore di colori o inserire un colore in notazione HTML HEX. Anche i formatori RGB come 'rosa' e 'giallo' funzionano.
Salva il comando	La combinazione di tasti per attivare un salvataggio senza premere il pulsante "Salva".
Usa l'autenticazione a due fattori	Abilita l'uso dell'autenticazione a due fattori per l'accesso. Al momento dell'accesso riceverai un'e-mail con un codice che dovrai inserire per accedere.
Timeout dell'autenticazione a due fattori	Imposta un periodo di tempo durante il quale non ti verrà richiesta l'autenticazione a due fattori dopo un'autenticazione già andata a buon fine.
Invia il codice di verifica tramite	Il codice di verifica verrà inviato alle opzioni selezionate. Il messaggio del dispositivo verrà visualizzato nell'AppTec360 MDM su tutti i dispositivi Android e iOS di tua proprietà.
Invia il messaggio di login dopo l'accesso	Se abilitato, verrà inviata un'e-mail per ogni accesso da un indirizzo ip non inserito nella whitelist. L'e-mail contiene informazioni sull'accesso (ad esempio IP, Browser).

Registro di accesso

Qui puoi vedere le informazioni relative ai login dell'account amministratore attualmente connesso.



Informazioni di accesso	Un elenco contenente i login dell'account amministratore attualmente connesso che sono stati registrati dalla console. Questo elenco mostra tutti i tuoi accessi riusciti negli ultimi 30 giorni.
Indirizzi IP inseriti nella whitelist	Questo è l'elenco di tutti gli indirizzi IP inseriti nella whitelist. Se accedi da un IP che è elencato qui, non riceverai il messaggio di accesso. Puoi aggiungere un indirizzo IP a questo elenco cliccando sul pulsante accanto a una voce dell'elenco "Informazioni di accesso". Puoi rimuovere un indirizzo IP da questo elenco cliccando sul pulsante accanto a una voce in questo elenco o nell'elenco "Informazioni di accesso" in alto.
Accesso non riuscito	Questo è un elenco di tutti i tentativi di accesso falliti negli ultimi 30 giorni. Se non sei riuscito a inserire la password corretta almeno 3 volte in 20 minuti, una voce apparirà in questo elenco. Verrai inoltre informato via e-mail dei tentativi di accesso falliti.

Amministrazione aziendale (Root-Node) nella gestione mobile

Una volta raggiunto il Root-Node (primo gruppo), puoi eseguire una serie di impostazioni per la tua azienda, per quanto riguarda la gestione dei dispositivi mobili.

Creare un sottogruppo	Crea un sottogruppo
Rinomina il nodo radice	Rinominare il nodo radice (ad esempio il nome della tua azienda)
Iscrizione di massa	Iscrivere più dispositivi/utenti contemporaneamente
Assegnazione di massa	Assegnare un profilo per i rispettivi gruppi, con un solo sguardo
Amministrazione rapida delle app	Invia le richieste di (dis)installazione di un'applicazione ai rispettivi gruppi di dispositivi.
Importazione utenti CSV	Importa gli utenti da CSV nel rispettivo gruppo

Creare un sottogruppo

Con "Crea un sottogruppo" puoi creare un ulteriore sottogruppo.

Puoi stabilire a quale gruppo assegnare il sottogruppo.

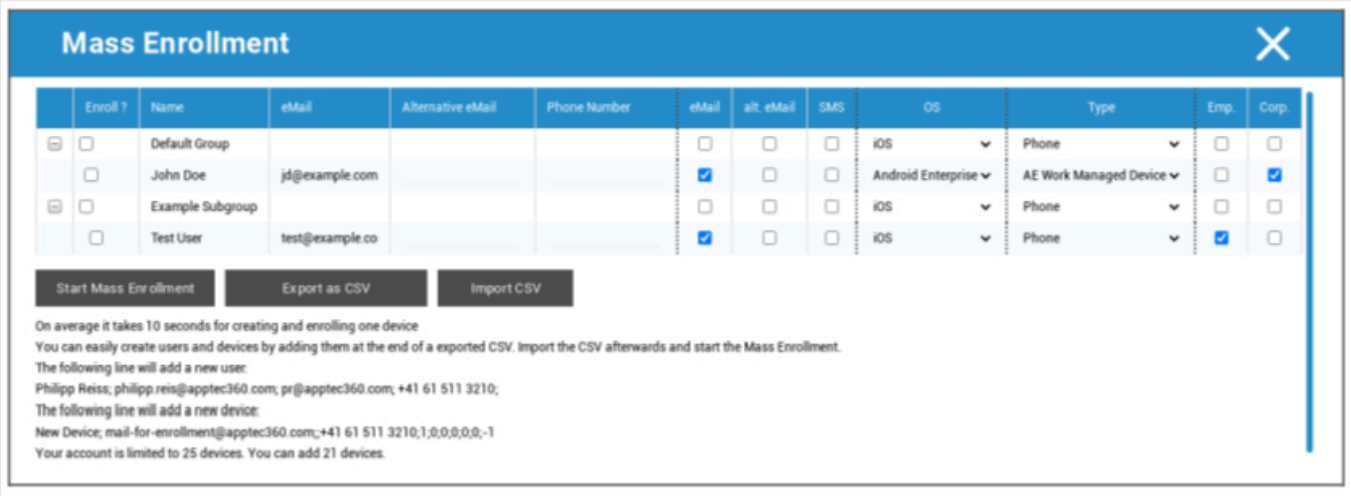
(Per impostazione predefinita, viene creato un nuovo gruppo che viene assegnato come sottogruppo al nodo principale).

Rinomina il nodo radice

Qui puoi rinominare il tuo nome-radice. È comune che in questo caso venga utilizzato il nome dell'azienda.

Iscrizione di massa

Con "Iscrizione di massa" puoi iscrivere più dispositivi e utenti.



Puoi selezionare direttamente il modo in cui l'utente deve ricevere l'iscrizione (eMail; eMail alternativa; SMS).

A seconda del dispositivo che l'utente riceverà (iOS, Android, Windows Phone), puoi contrassegnarlo direttamente qui.

Qui si può configurare anche la distinzione tra smartphone e tablet, che dovrai selezionare correttamente con un segno di spunta.

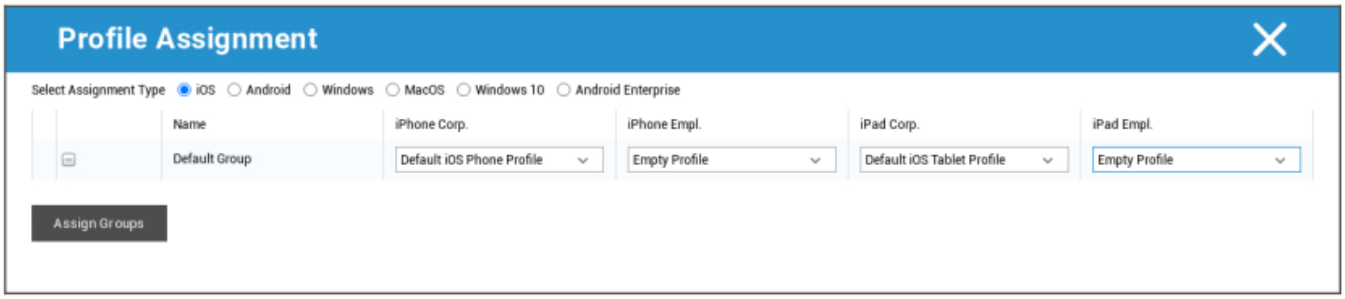
Come ultimo passo, puoi stabilire se il dispositivo in questione è aziendale o privato (BYOD).

Con "Esporta come CSV" puoi esportare le informazioni come file di dati CSV. In cambio, puoi anche importare il file di dati CSV con "Importa CSV"; il file dovrebbe avere l'aspetto dell'esempio seguente:

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

Assegnazione di massa

Alla voce Assegnazione di massa puoi assegnare un profilo a tutti i gruppi, suddivisi in iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

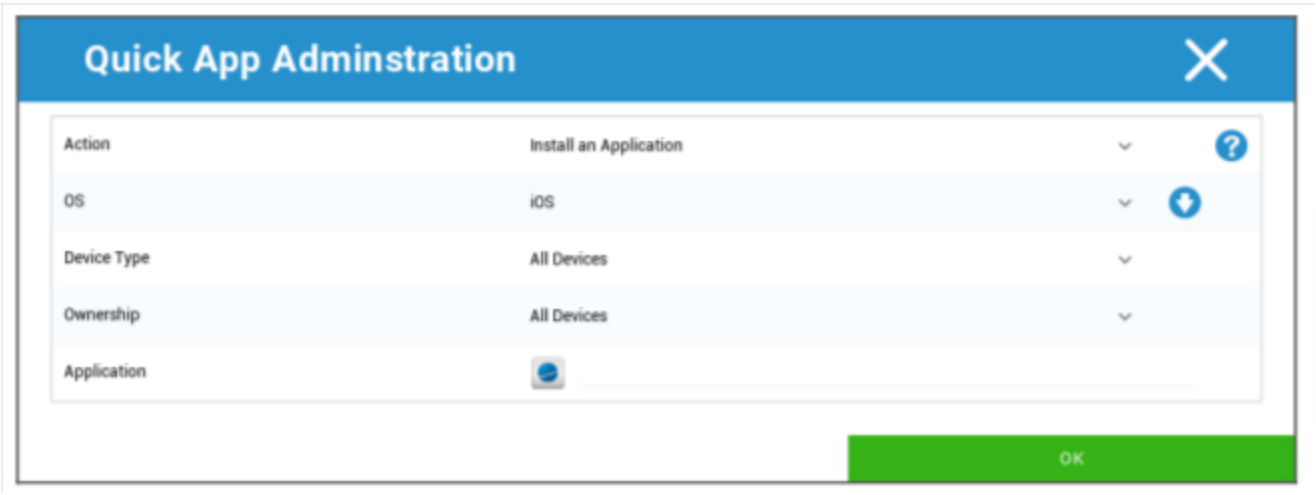


Windows - MacOS - Windows 10 - Android Enterprise

Amministrazione rapida delle app

In Amministrazione rapida delle applicazioni puoi inviare richieste di installazione o disinstallazione di un'applicazione specifica a un sistema operativo di tua scelta.

Puoi anche definire se la richiesta deve essere inviata a tutti i tipi di dispositivi del sistema operativo selezionato o solo a un tipo specifico di dispositivo.



Importazione utenti CSV

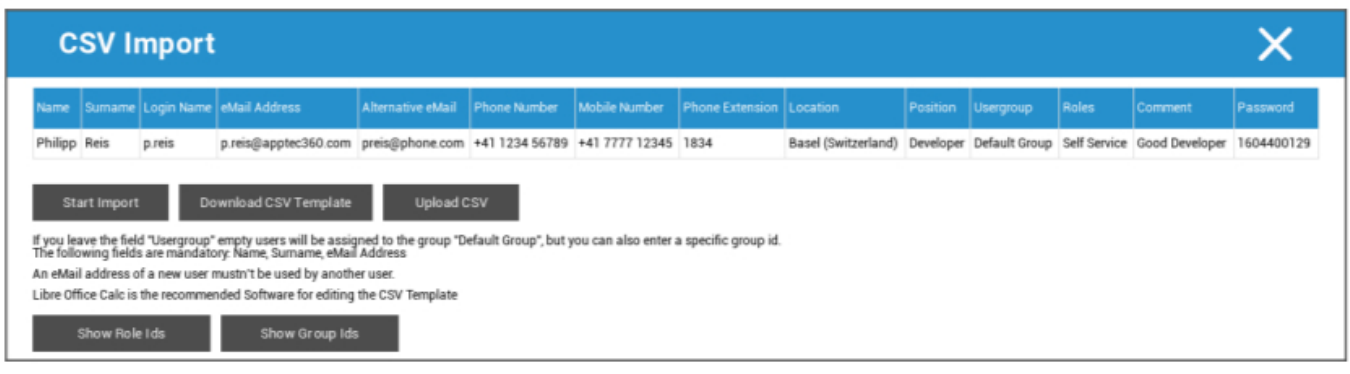
Importa gli utenti da CSV nel rispettivo gruppo.

Con "Scarica modello CSV" puoi esportare un file modello CSV da compilare (o da usare come riferimento).

Puoi anche usare le opzioni "Mostra gli ID dei ruoli" e "Mostra gli ID dei gruppi" come riferimento per creare il tuo file CSV.

Il file CSV può essere caricato nell'MDM con "Upload CSV".

Come ultimo passo, puoi avviare l'importazione cliccando su "Avvia importazione".



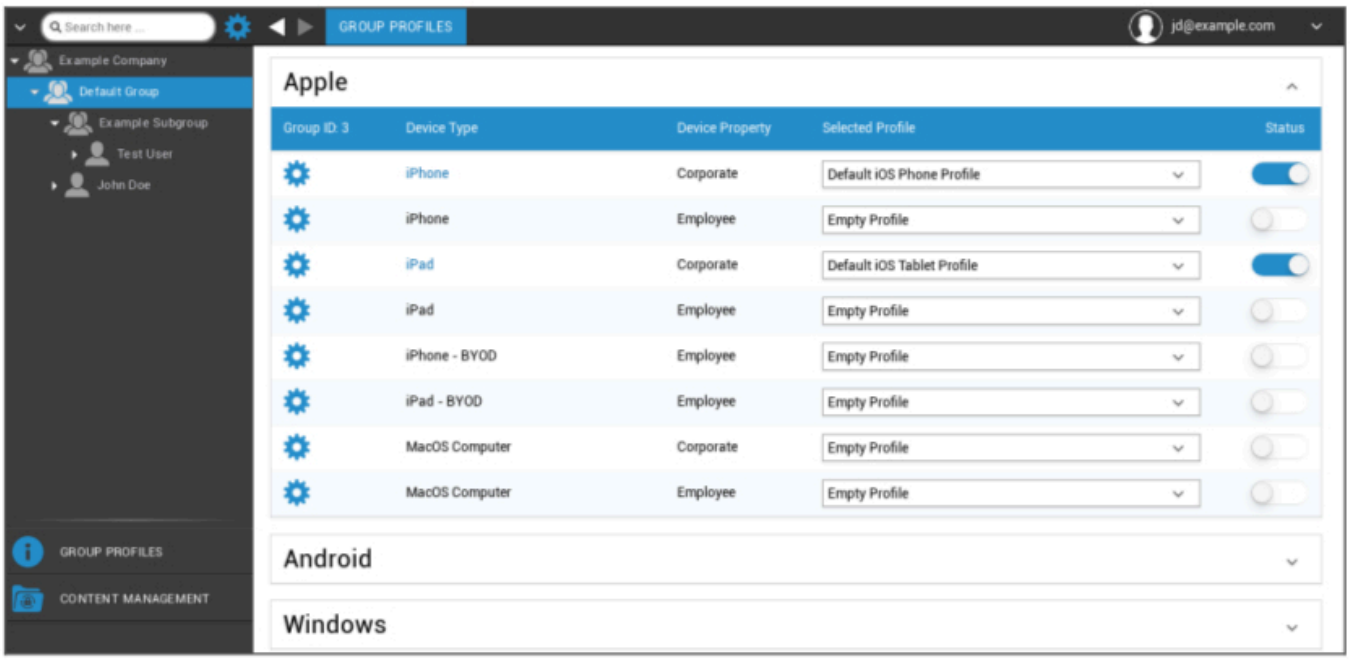
Gestione dei gruppi nella gestione dei dispositivi mobili

Con un clic sulla panoramica vengono visualizzati i diversi profili di configurazione per le rispettive piattaforme.

Un profilo contiene tutte le opzioni di impostazione che possono essere stabilite in anticipo con AppTec360 sul dispositivo dell'utente finale. Su ogni piattaforma puoi creare profili per i dispositivi aziendali (Corporate) o per i dispositivi Bring-Your-Own-Device (Employee).

Per differenziare le configurazioni dei gruppi di dispositivi, ad esempio in base alla posizione o alla funzione, si consiglia di creare diversi sottogruppi.

Tieni presente la gestione dei profili in Gestione cellulare



Con il menu delle marce puoi configurare una serie di impostazioni per il rispettivo (sotto)gruppo.

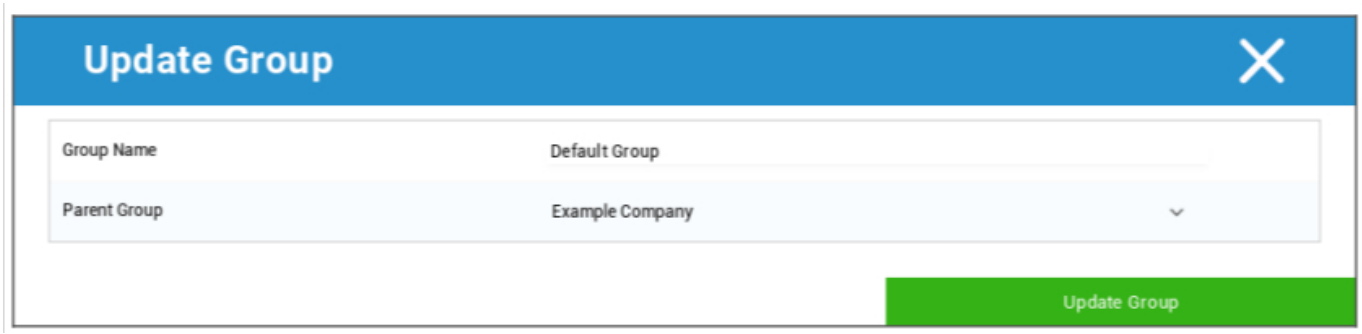
Creare un sottogruppo	Crea un sottogruppo per il rispettivo (sotto)gruppo
Modifica il gruppo selezionato	Modifica il gruppo selezionato
Elimina il gruppo selezionato	Elimina il gruppo selezionato
Iscrizione di massa	Iscrivi molti dispositivi/utenti in una sola volta per il profilo selezionato
Assegnazione di massa	Assegnare i profili al gruppo attualmente selezionato
Creare un sottogruppo	Crea un sottogruppo per il rispettivo (sotto)gruppo
Crea un utente	Creare un utente per il rispettivo (sotto)gruppo

Creare un sottogruppo

Con "Crea un sottogruppo" puoi creare un ulteriore sottogruppo.

Puoi stabilire a quale gruppo deve essere assegnato il sottogruppo (come impostazione predefinita, il sottogruppo viene assegnato al gruppo attualmente selezionato).

Modifica il gruppo selezionato



Qui puoi modificare il profilo: sono possibili le seguenti impostazioni:

- Il nome del gruppo può essere cambiato
- Il gruppo di genitori può essere cambiato

Elimina il gruppo selezionato

Alla voce "Elimina il gruppo selezionato" vengono elencati tutti gli utenti e i dispositivi che fanno parte del gruppo in questione. Qui hai la possibilità di eliminarli.

Per un utente puoi eseguire i seguenti comandi di cancellazione:

Elimina utente	L'utente è stato eliminato
Sposta l'utente nel gruppo:	Puoi spostare l'utente in un altro gruppo (colonna seguente, ad esempio "Admins").

Per un dispositivo puoi eseguire i seguenti comandi di cancellazione:

Pulisci e cancella	Pulisci e cancella il dispositivo
Elimina dal sistema	Rimuovi il dispositivo solo da AppTec

Riferimento: Iscrizione di massa

Riferimento: Assegnazione di massa

Crea un utente

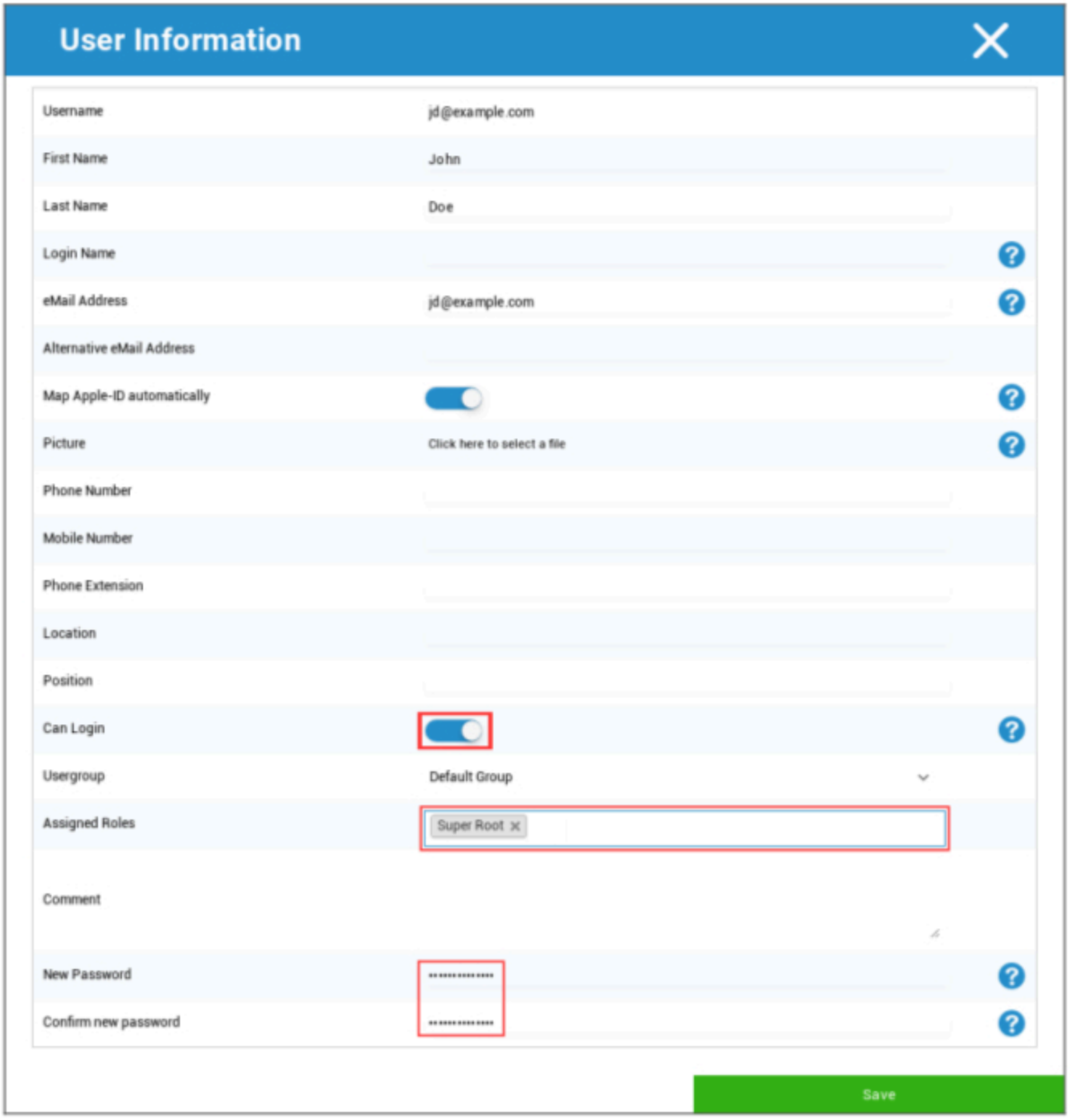
Con "Crea un utente" puoi aggiungere un nuovo utente.

Crea un nuovo utente amministratore

Puoi impostare un utente come Admin-User. In questo modo otterrà i permessi per accedere alla console e cambiare utenti/gruppi/dispositivi.

Crea un Utente normale o utilizza un Utente esistente. Scegli l'utente a cui vuoi dare i permessi di amministrazione, clicca sulla rotella e scegli "Modifica utente":

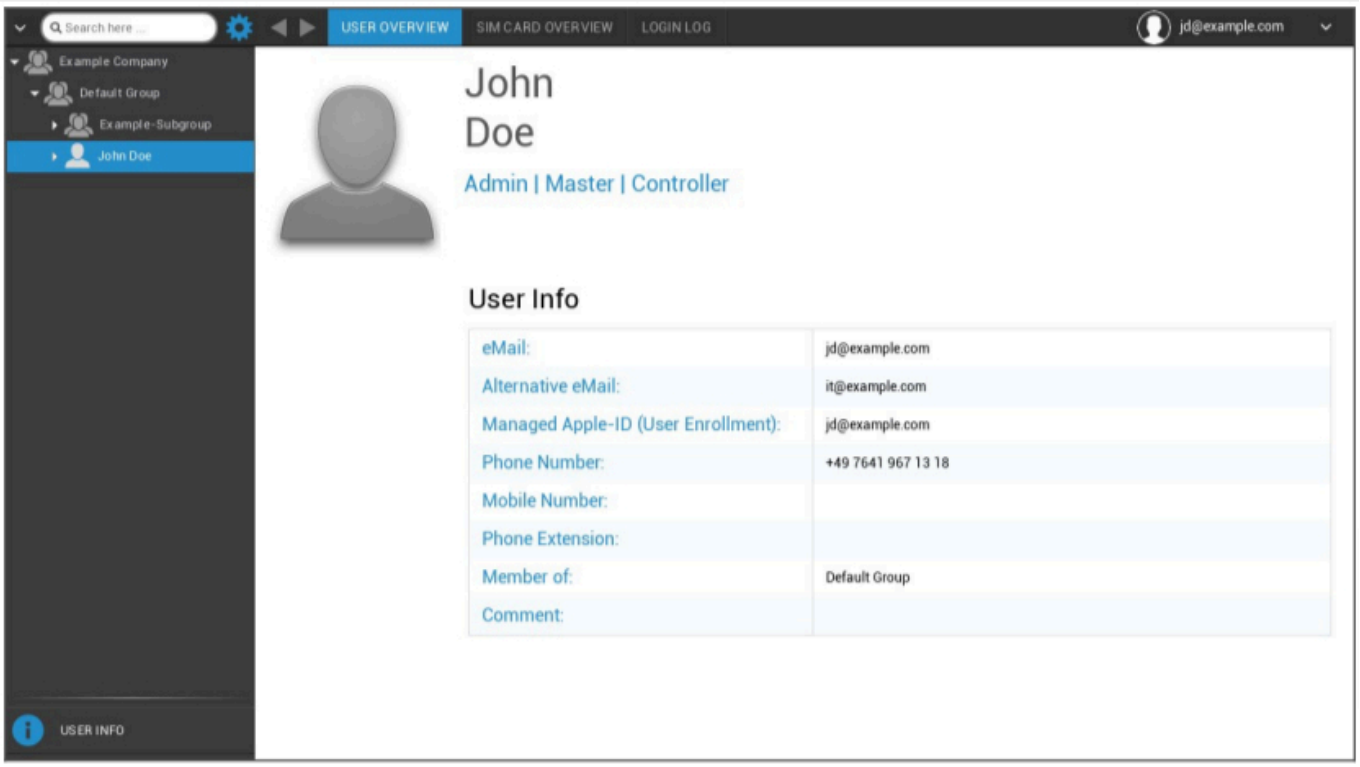
Attiva l'interruttore "Può accedere", assegna il ruolo "Super-Root" all'utente e imposta una password.



Salva il tutto e l'utente potrà ora accedere con il nome utente e la password.

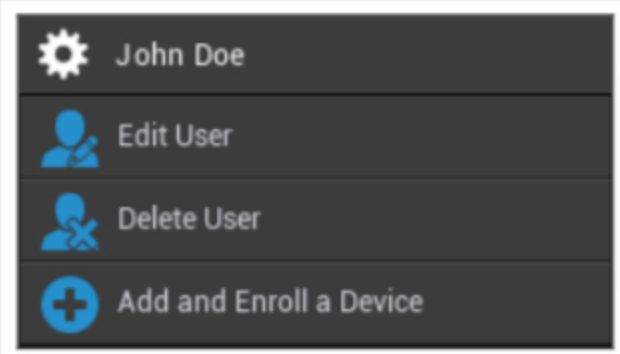
Gestione degli utenti nella gestione dei dispositivi mobili

Quando selezioni un determinato utente, vedrai la seguente panoramica:



Riceverai una panoramica di tutte le informazioni che hai inserito in precedenza in "Crea un utente".

Con l'ingranaggio installato in alto, puoi eseguire le seguenti configurazioni:



Nome utente	Nome dell'utente selezionato
Modifica utente	Modifica le informazioni dell'utente
Elimina l'utente	Elimina l'utente • Elimina dal sistema = Il dispositivo verrà rimosso da AppTec.

	• Wipe & Delete = Il dispositivo verrà ripristinato alle impostazioni di fabbrica e rimosso da AppTec.
Aggiungere e registrare un dispositivo	Iscrivi un dispositivo per l'utente selezionato

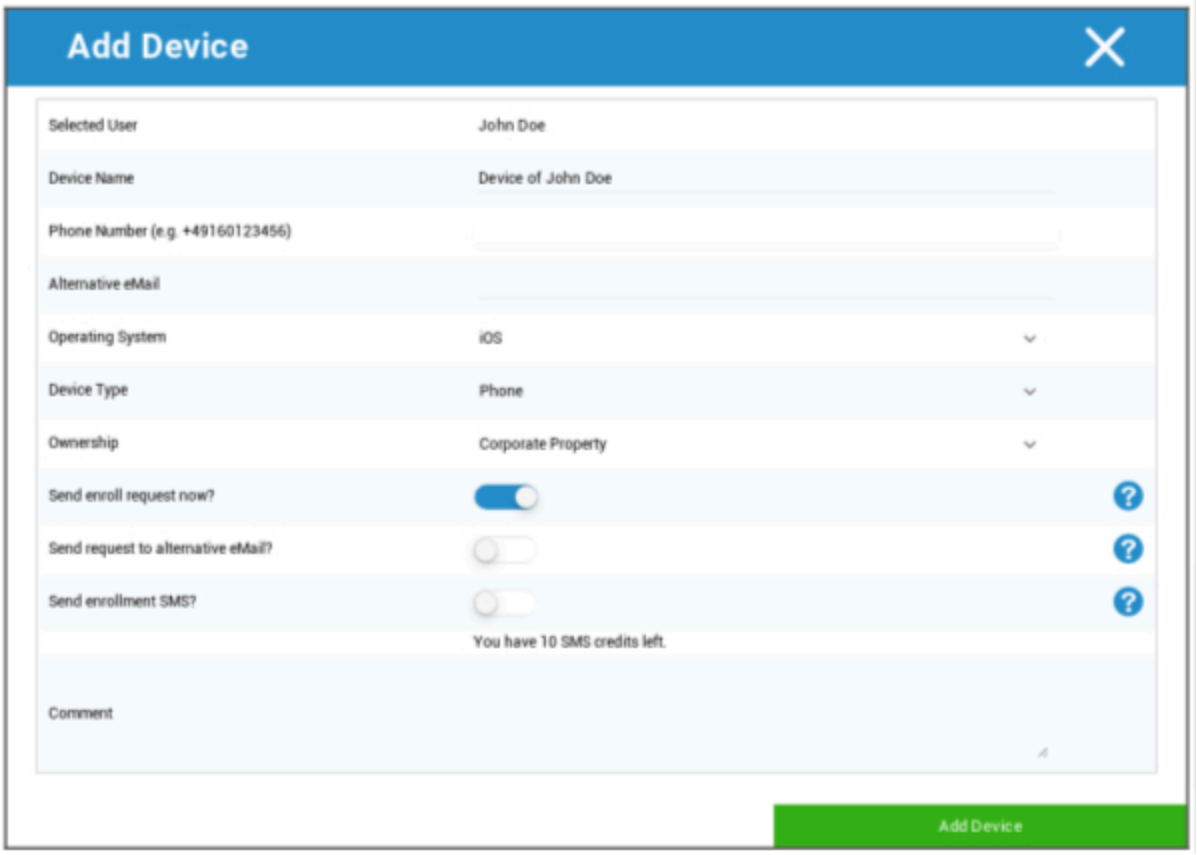
Tieni presente che l'accesso all'amministrazione può essere archiviato anche come account utente locale nella struttura gerarchica. Senza l'istituzione di un ulteriore amministratore, questo non dovrebbe essere cancellato!

Aggiungere e registrare un dispositivo

Qui puoi selezionare un dispositivo per l'uso selezionato.

In alternativa puoi iscrivere direttamente i dispositivi a un gruppo. Per farlo, clicca sul gruppo, clicca sulla rotella e seleziona "Aggiungi e iscrivi un dispositivo".

Dovresti vedere la seguente panoramica:



A seconda del tipo di dispositivo che vuoi registrare, devi eseguire le seguenti configurazioni:

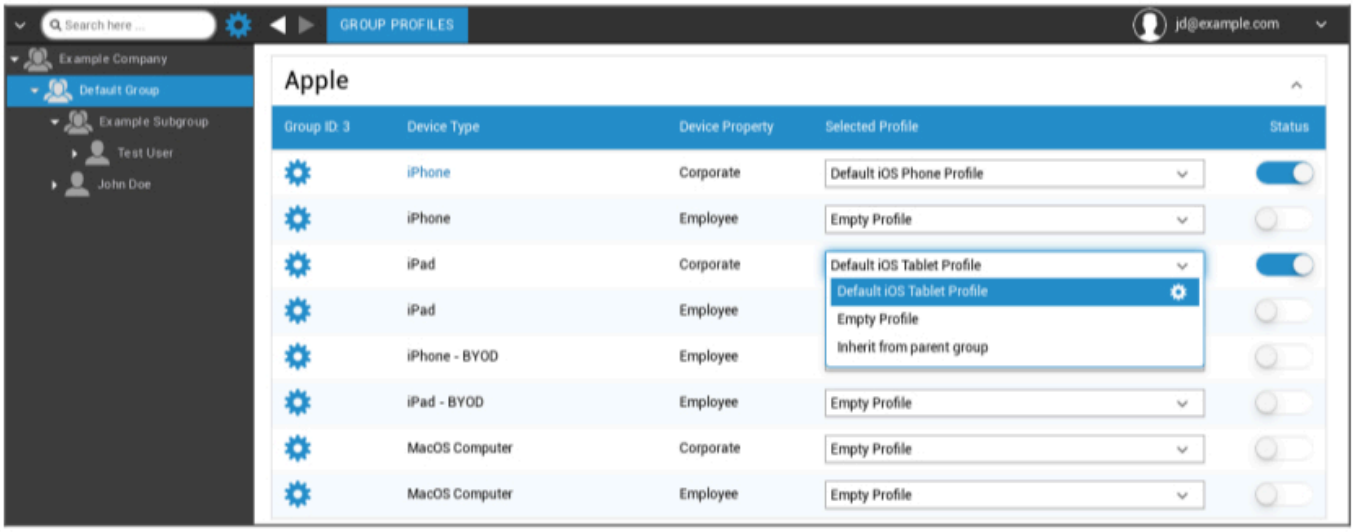
Utente selezionato	Utente selezionato (verrà compilato automaticamente)
Nome del dispositivo	Verrà compilato automaticamente (dispositivo per "nome dell'utente"), ma può essere modificato.
Numero di telefono	Il numero di telefono verrà inserito automaticamente (a patto che sia stato fornito dall'utente) - qui, tuttavia, può essere aggiunto o modificato.
Email alternative	L'email alternativa verrà compilata automaticamente (a patto che sia stata fornita dall'utente) - qui, tuttavia, può essere aggiunta o cambiata
Proprietario del dispositivo	Proprietà aziendale = dispositivo aziendale Proprietà del dipendente = dispositivo BYOD
Scegli il sistema operativo	Qui puoi scegliere tra i seguenti sistemi operativi: • iOS • iOS BYOD (iscrizione dell'utente) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Inviare una richiesta di iscrizione?	L'e-mail viene inviata immediatamente all'indirizzo e-mail principale e all'utente viene richiesto di collegare il proprio dispositivo.
Inviare la richiesta a un'e-mail alternativa?	Invia l'e-mail in aggiunta o esclusivamente (nel caso in cui l'opzione "Invia richiesta di iscrizione?" sia stata disattivata) all'indirizzo e-mail alternativo (l'e-mail è diversa dall'e-mail di richiesta di iscrizione "normale").
Inviare un SMS di iscrizione?	Invia una richiesta di iscrizione via SMS (il "Numero di telefono" deve essere inserito)

Dopo l'invio della richiesta di iscrizione, il dispositivo verrà subito visualizzato (contrassegnato in rosso).

Non appena il dispositivo è stato collegato con successo, poco dopo sarà contrassegnato con il colore verde e sarà quindi pronto a ricevere restrizioni, applicazioni, ecc.

Gestione dei profili nella gestione dei dispositivi mobili

Dopo aver cliccato su un gruppo, riceverai una panoramica di tutte le piattaforme di dispositivi da configurare e dei rispettivi profili assegnati.



	Esegui la configurazione del profilo selezionato
Tipo di dispositivo	Tipo e/o modello di dispositivo
Proprietà del dispositivo	Proprietario del dispositivo (Corporate = proprietà aziendale, Employee = dispositivo privato di un dipendente)
Profilo selezionato	Profilo selezionato (l'ingranaggio apre la finestra di configurazione del profilo)
Stato	On/Off (il profilo è attivato/disattivato)

Quando selezioni la marcia, riceverai le seguenti opzioni:

Crea un profilo

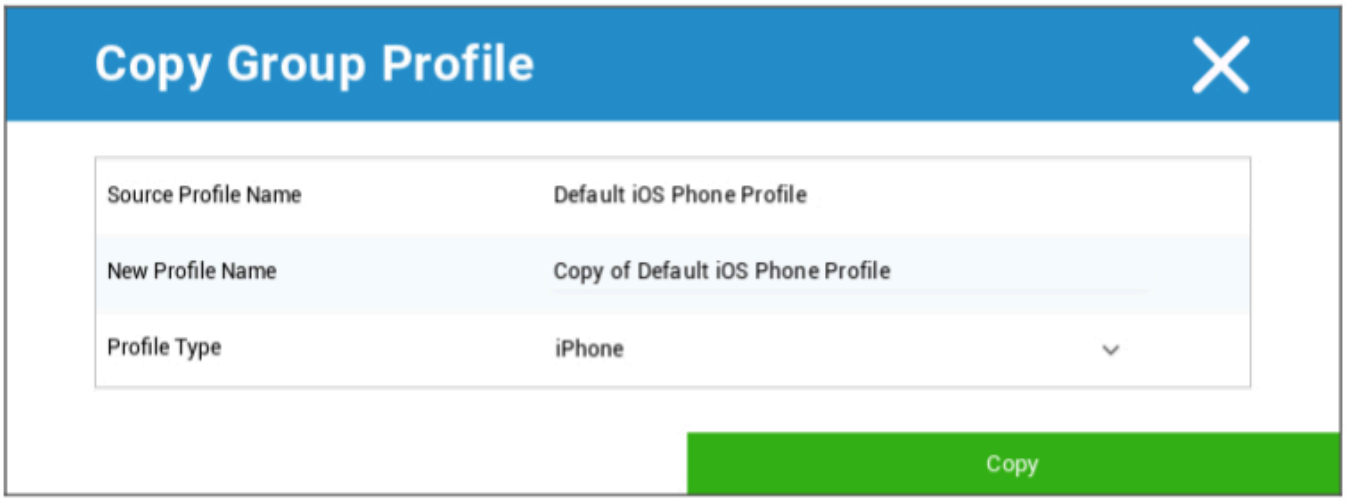
Puoi creare e configurare un nuovo profilo per ogni voce e/o piattaforma. Dopo aver cliccato su questo punto secondario, il profilo verrà creato immediatamente e potrai iniziare subito la configurazione di iOS, Android e Windows Phone.

Modifica il profilo

Dopo aver cliccato su "Modifica profilo", raggiungerai la schermata di configurazione del profilo in questione, dove potrai impostare le configurazioni.

Copia del profilo

Con l'aiuto della funzione "Copia profilo", puoi copiare le impostazioni/configurazioni di un profilo già esistente e aggiungerle a un nuovo profilo.

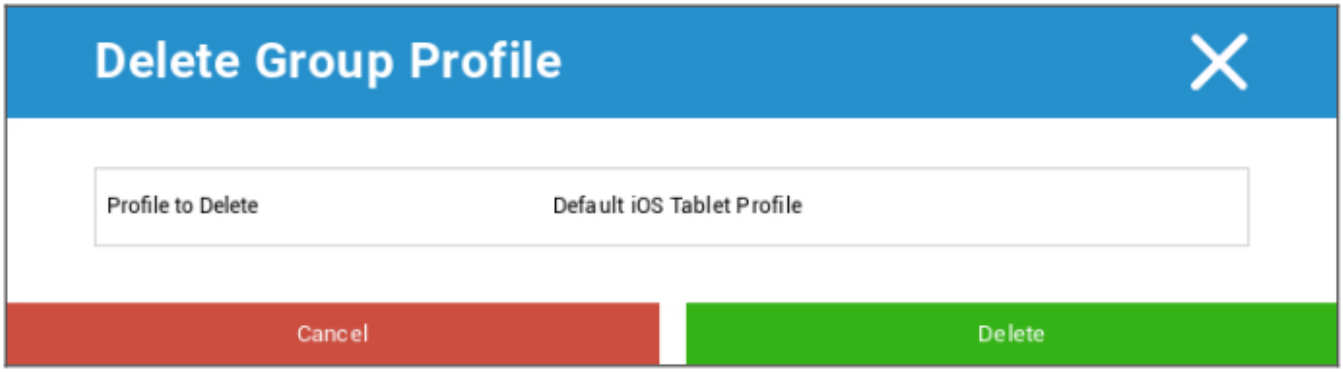


Nome del profilo sorgente	Nome del profilo da copiare
Nome del nuovo profilo	Nome del nuovo profilo
Tipo di profilo	Tipo di profilo (Telefono/Tablet)

Una volta cliccato su "Copia", il profilo verrà creato e potrà essere assegnato al gruppo.

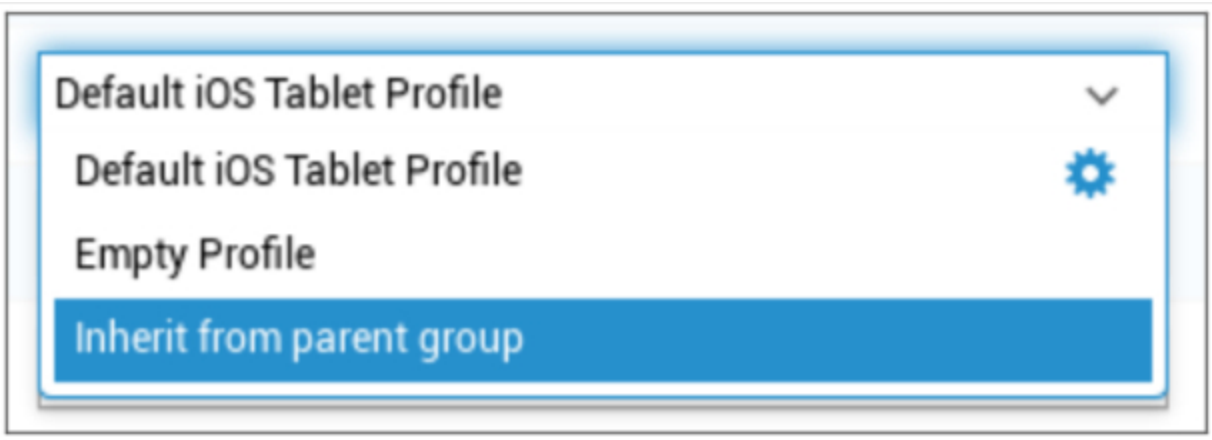
Elimina il profilo

Qui puoi eliminare definitivamente un profilo. Tieni presente che durante il processo di cancellazione e il successivo processo di "Assegnazione ora" del profilo, la configurazione scomparirà sui rispettivi dispositivi di un gruppo interessato e non potrà essere recuperata!


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

Ereditarietà dei profili

Durante la selezione dei profili, è disponibile l'opzione "Eredita dal gruppo di genitori".



Quando il profilo viene attivato, verrà utilizzato il profilo del gruppo padre per il dispositivo selezionato (e il relativo tipo di dispositivo). Tieni inoltre presente che le modifiche a questo profilo potrebbero riguardare numerosi gruppi.

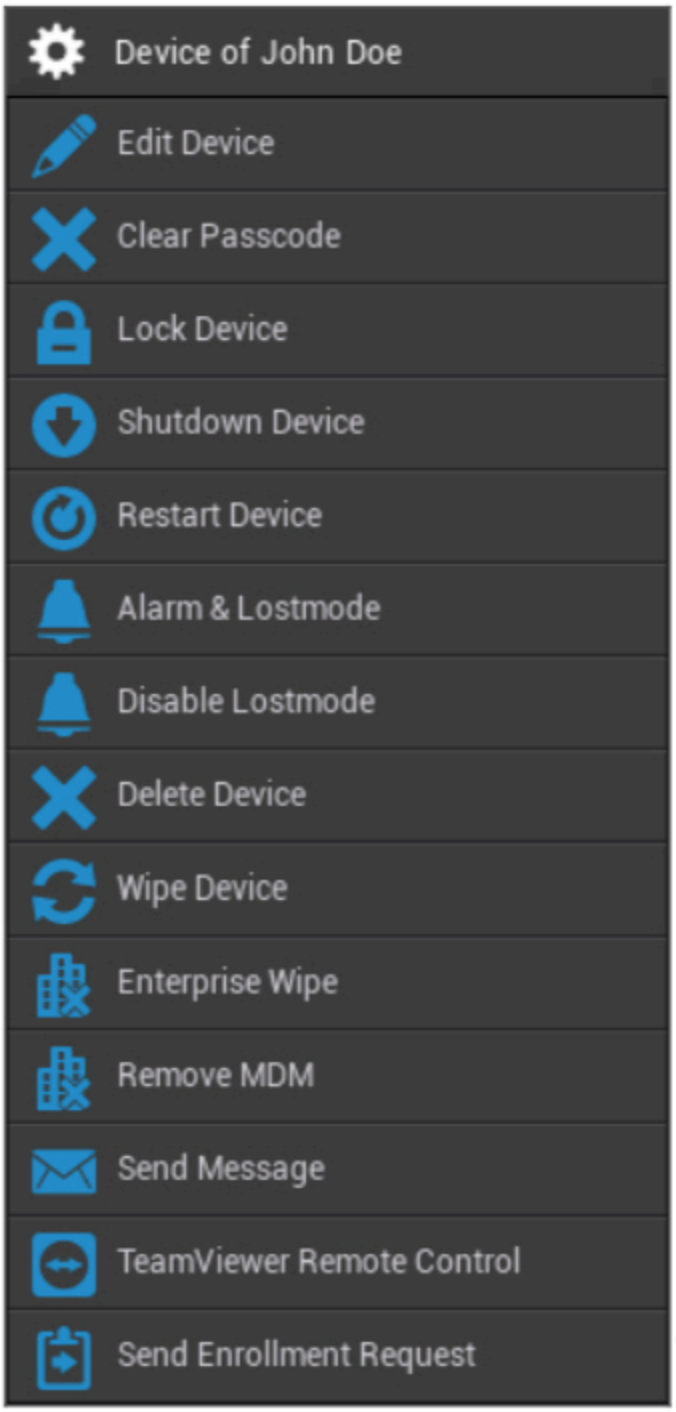
Questa configurazione è impostata come valore predefinito quando viene creato un nuovo sottogruppo.

È disponibile anche la configurazione "Profilo vuoto", che corrisponde a un profilo vuoto, il che significa che alla fine non verranno eseguite nuove configurazioni sul dispositivo dell'utente finale.

Gestione dei dispositivi nella gestione dei dispositivi mobili

Quando selezioni un dispositivo, puoi eseguire una serie di operazioni tramite l'"ingranaggio". Questi sono diversi, a seconda delle piattaforme OS (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

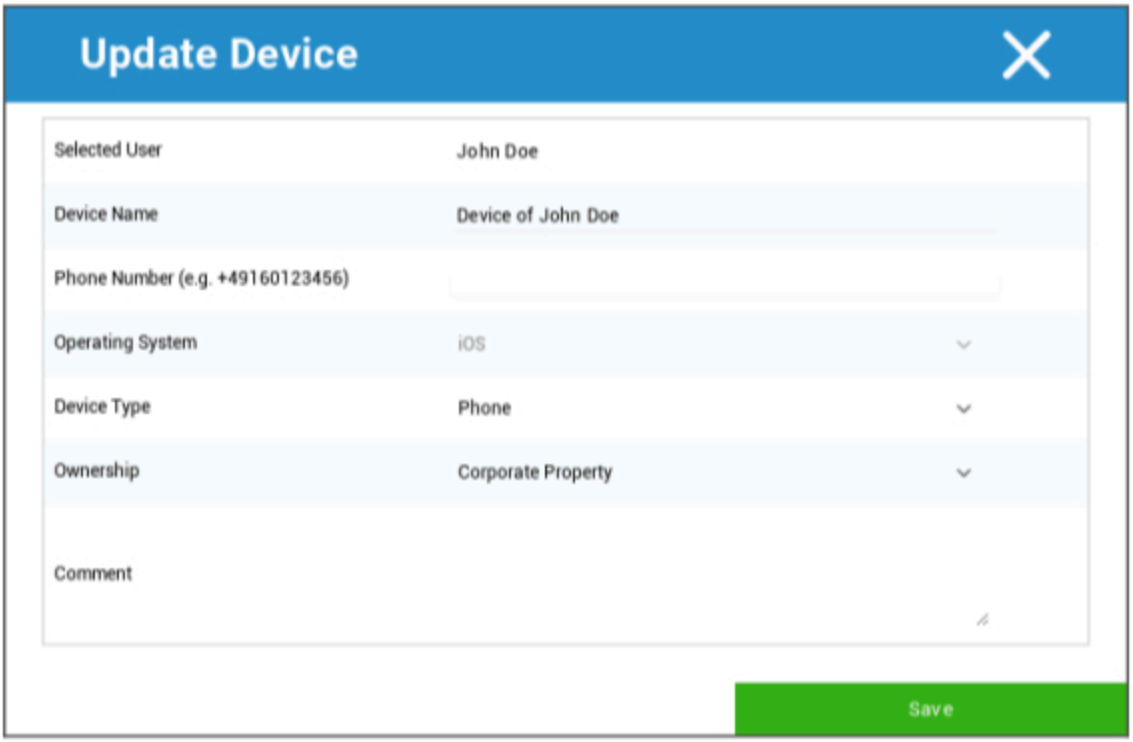
IOS



Modifica dispositivo	Modifica dispositivo
Cancella il codice di accesso	Il codice di accesso del dispositivo viene cancellato
Dispositivo di blocco	Blocca il dispositivo (schermata di blocco)

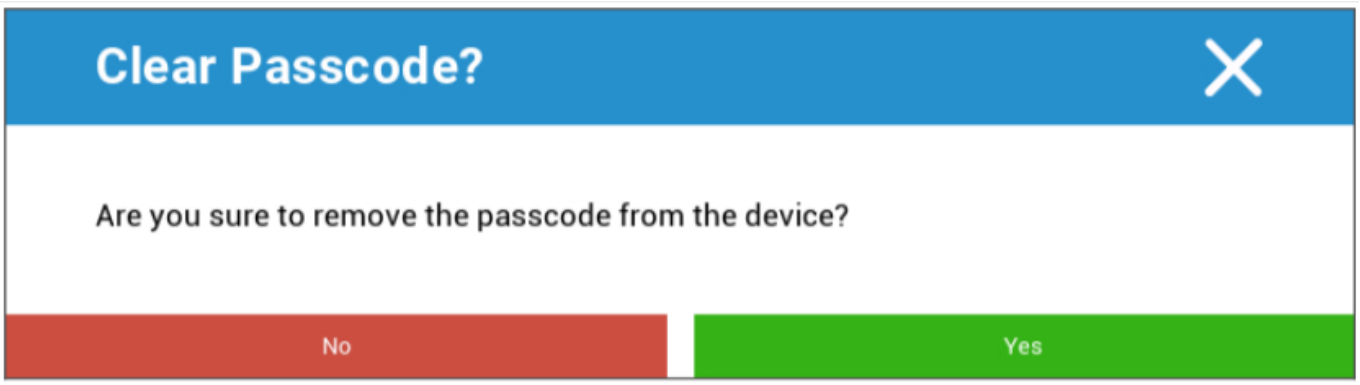
Dispositivo di spegnimento	Dispositivo di spegnimento
Riavvia il dispositivo	Riavvia il dispositivo
Allarme e modalità di smarrimento	Avvio dell'allarme e della modalità Lostmode
Disabilita la modalità Lostmode	Disabilita la modalità Lostmode
Elimina il dispositivo	Rimuovi il dispositivo da AppTec
Pulisci il dispositivo	Ripristina le impostazioni di fabbrica del dispositivo
Pulizia aziendale	Le informazioni, le applicazioni e i profili forniti da AppTec360 vengono eliminati (il dispositivo viene separato dall'MDM)
Rimuovi MDM	
Invia un messaggio	Invia notifiche push al dispositivo Il messaggio verrà visualizzato nell'AppTec360 (scheda Messaggio).
Controllo remoto di TeamViewer	Avvia la sessione di controllo remoto con TeamViewer
Invia la richiesta di iscrizione	Invia (ripetutamente) la richiesta di iscrizione

Modifica dispositivo



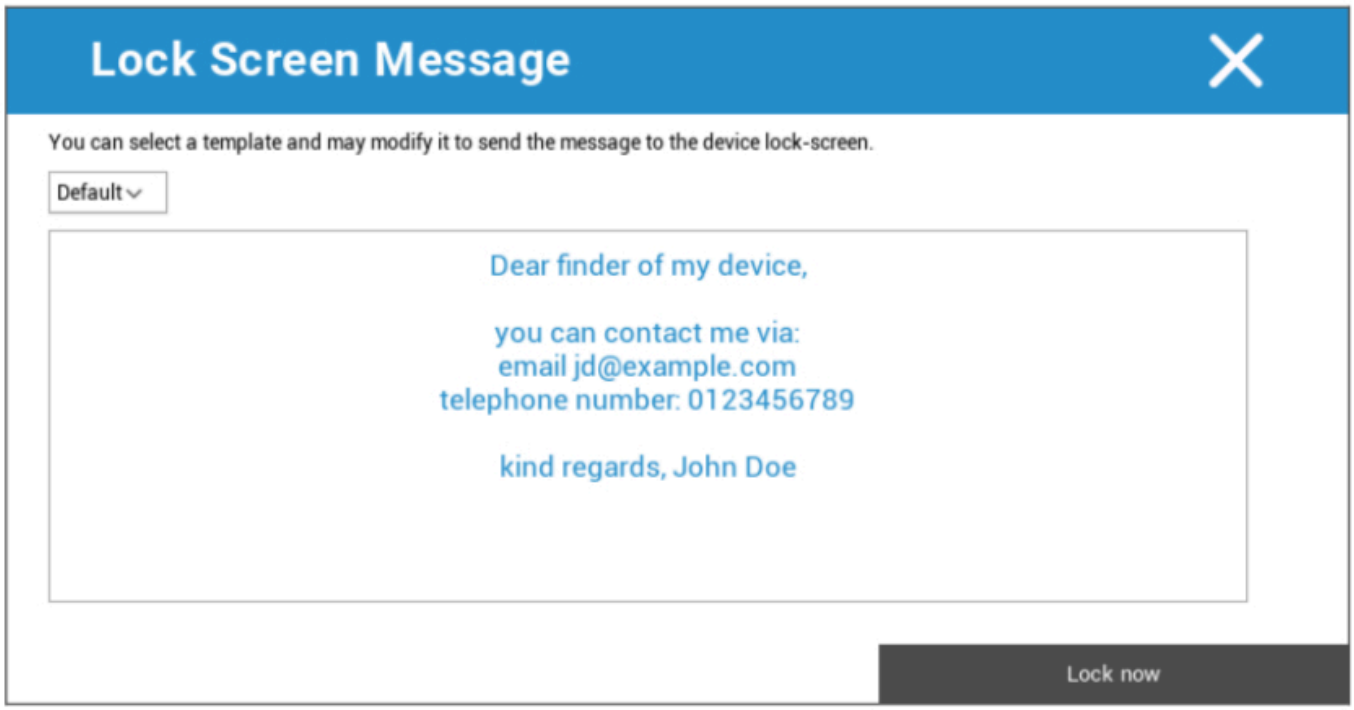
Qui puoi aggiornare una serie di informazioni sul dispositivo.

Cancella il codice di accesso



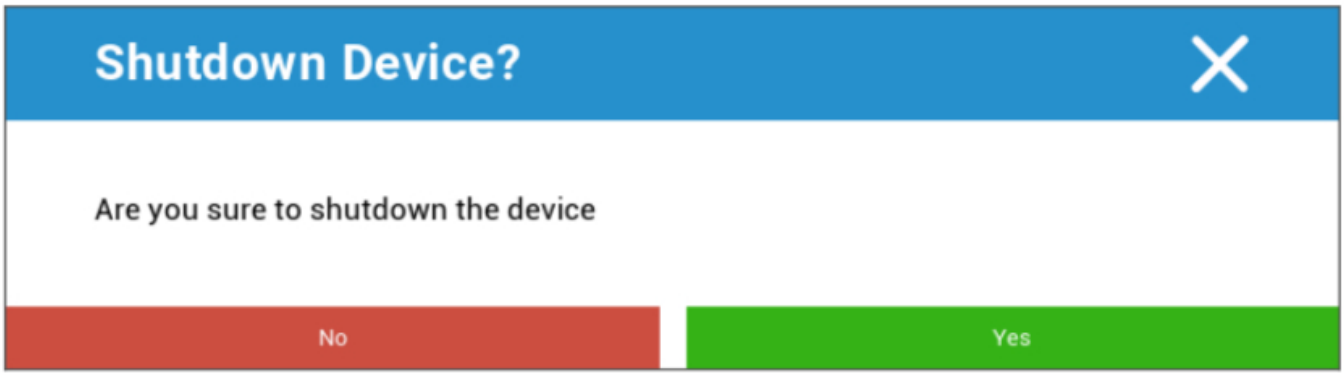
Alla voce "Clear Passcode" puoi rimuovere da remoto il codice di accesso dal dispositivo. Successivamente, all'utente verrà richiesto di inserire una nuova password (a seconda delle linee guida del Passcode).

Dispositivo di blocco



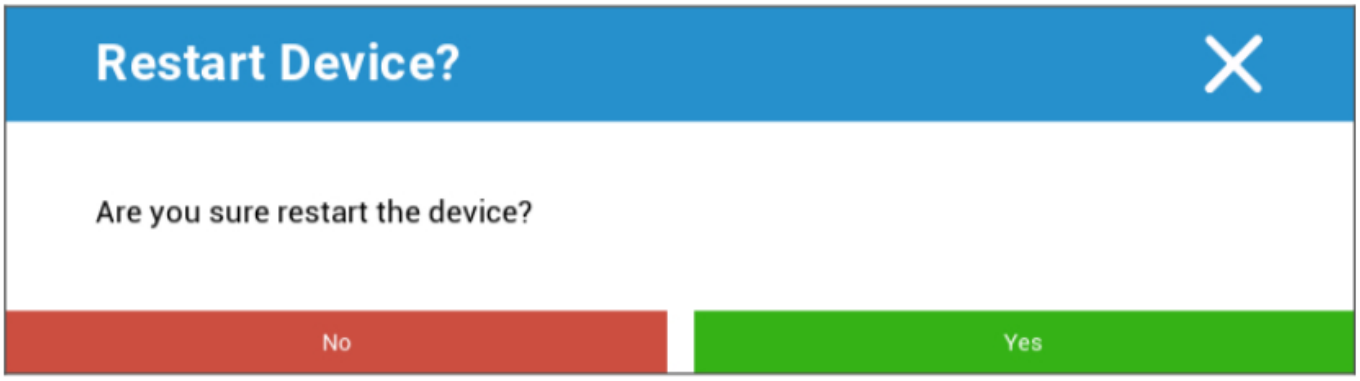
Qui viene inviato un comando di blocco al dispositivo dell'utente finale (schermata di blocco).

Dispositivo di spegnimento



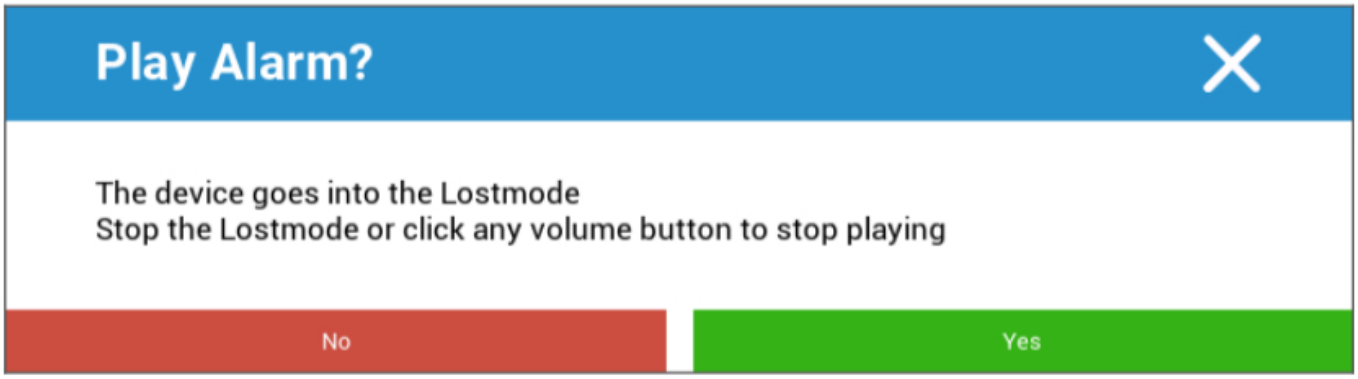
Qui viene inviato un comando di spegnimento al dispositivo dell'utente finale.

Riavvia il dispositivo

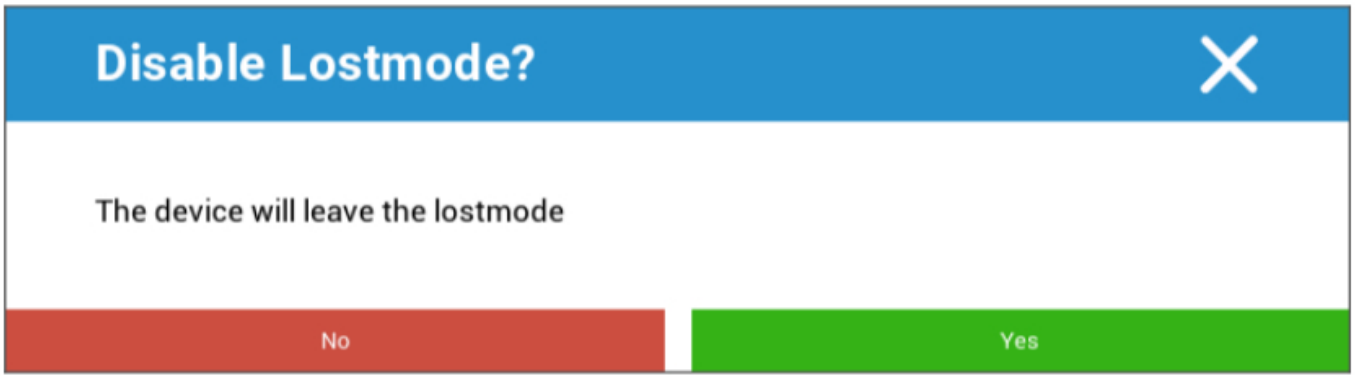


Qui viene inviato un comando di riavvio al dispositivo dell'utente finale.

Allarme e Lostmode | Disattiva Lostmode



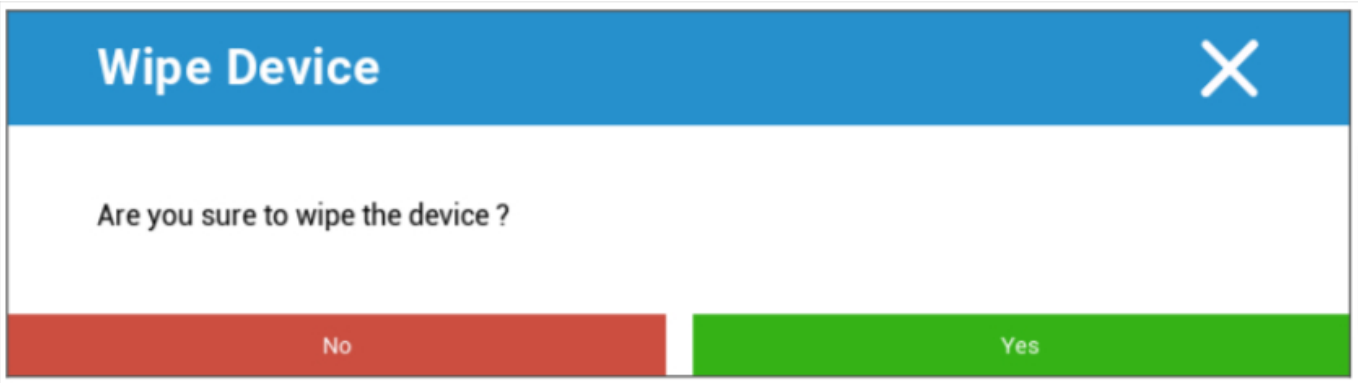
Qui il dispositivo può essere impostato in modalità Lostmode, che prevede la riproduzione costante di un suono di allarme. La modalità Lostmode può essere interrotta premendo un qualsiasi tasto del volume del dispositivo o da remoto cliccando su "Disable Lostmode":



Elimina il dispositivo

Qui è possibile eseguire il comando di cancellazione. Puoi ancora una volta decidere se il dispositivo deve essere rimosso solo da AppTec360 ("Delete from System") o se deve essere rimosso da AppTec360 e ripristinato alle impostazioni di fabbrica ("Wipe & Delete").

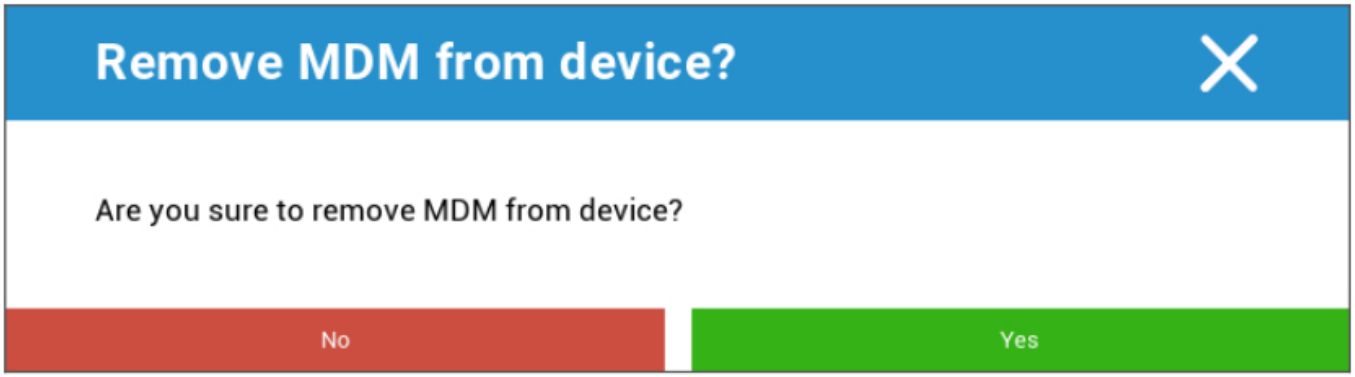
Pulisci il dispositivo



Alla voce "Wipe Device" puoi eseguire una cancellazione completa del dispositivo. Il dispositivo verrà ripristinato alle impostazioni di fabbrica.

Enterprise Wipe | Rimuovi MDM

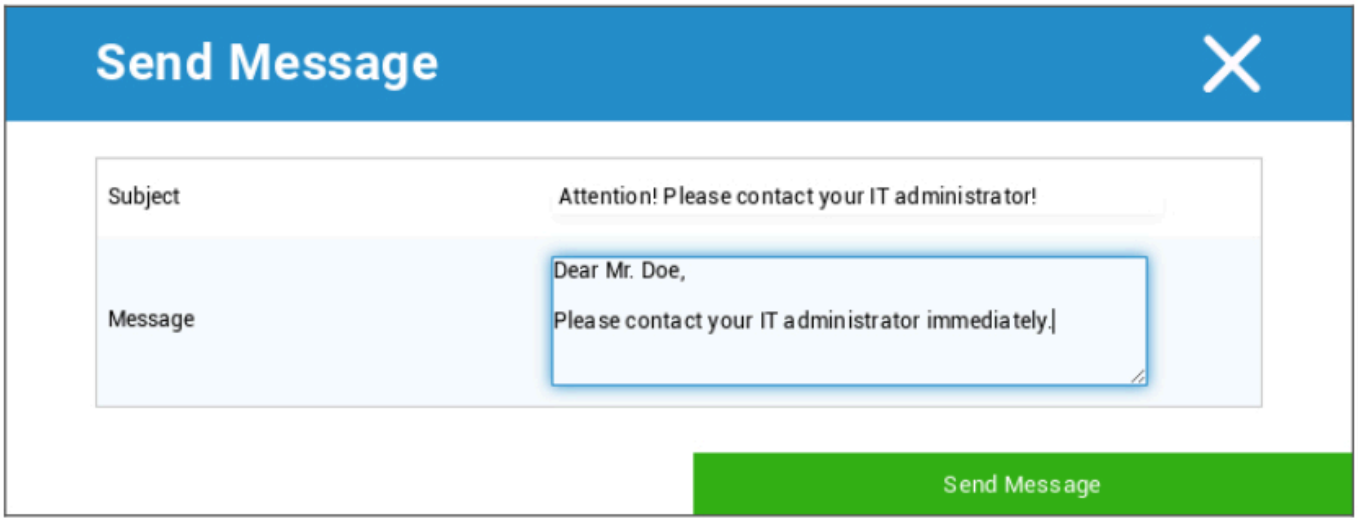
Solo le informazioni, le applicazioni e i profili forniti da AppTec360 vengono cancellati. In questo modo, i dati aziendali non saranno più disponibili sul dispositivo dell'utente finale. L'area privata non viene toccata e continua a rimanere sul dispositivo dell'utente finale.



Con "Rimuovi MDM" puoi rimuovere il profilo MDM sul dispositivo dell'utente finale e tutti gli altri elementi forniti da AppTec.

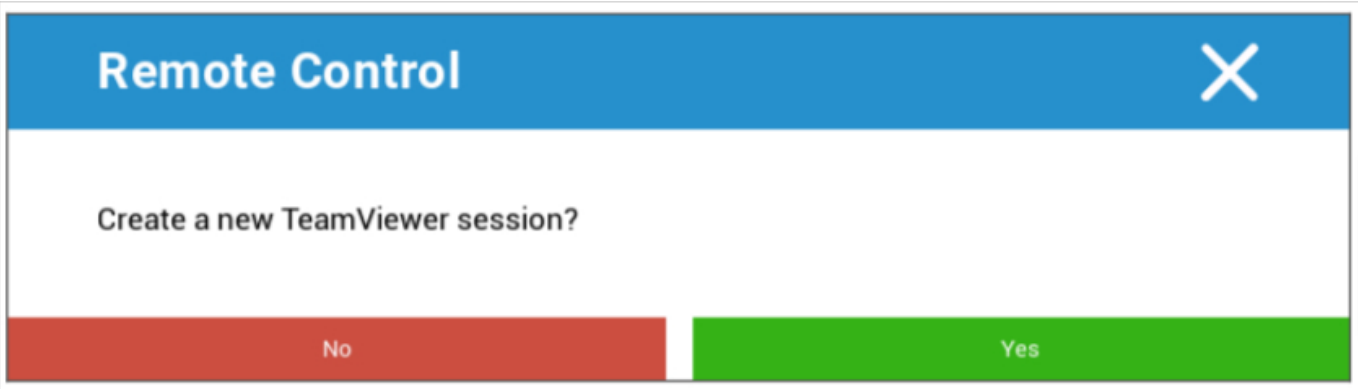
Questo comando esegue la stessa azione di "Enterprise Wipe".

Invia un messaggio



Qui puoi inviare una notifica push al rispettivo dispositivo.

Controllo remoto di TeamViewer



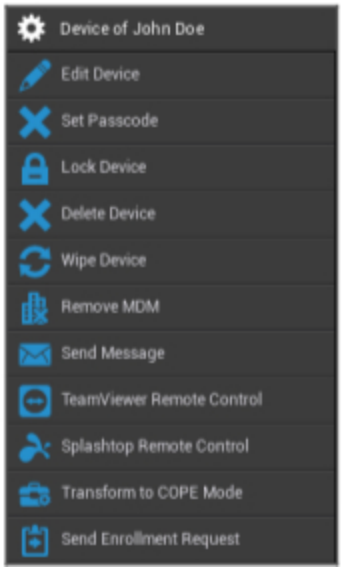
Qui è possibile avviare una sessione di controllo remoto di Teamviewer.

Invia la richiesta di iscrizione

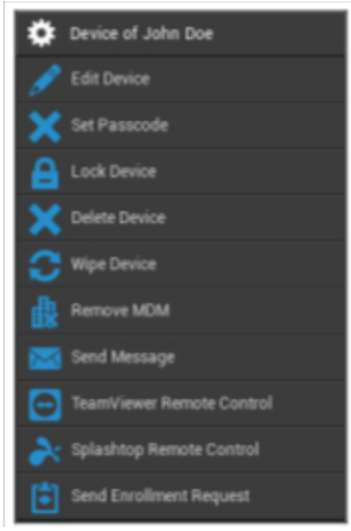
Con "Invia richiesta di iscrizione", puoi inviare una richiesta di iscrizione (di nuovo) al rispettivo utente.

Android

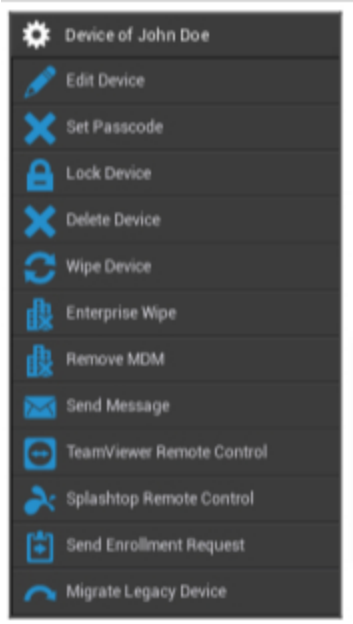
Dispositivo AE completamente gestito (gestito dal lavoro)



Profilo di lavoro AE (contenitore)



Telefono Android | Tablet

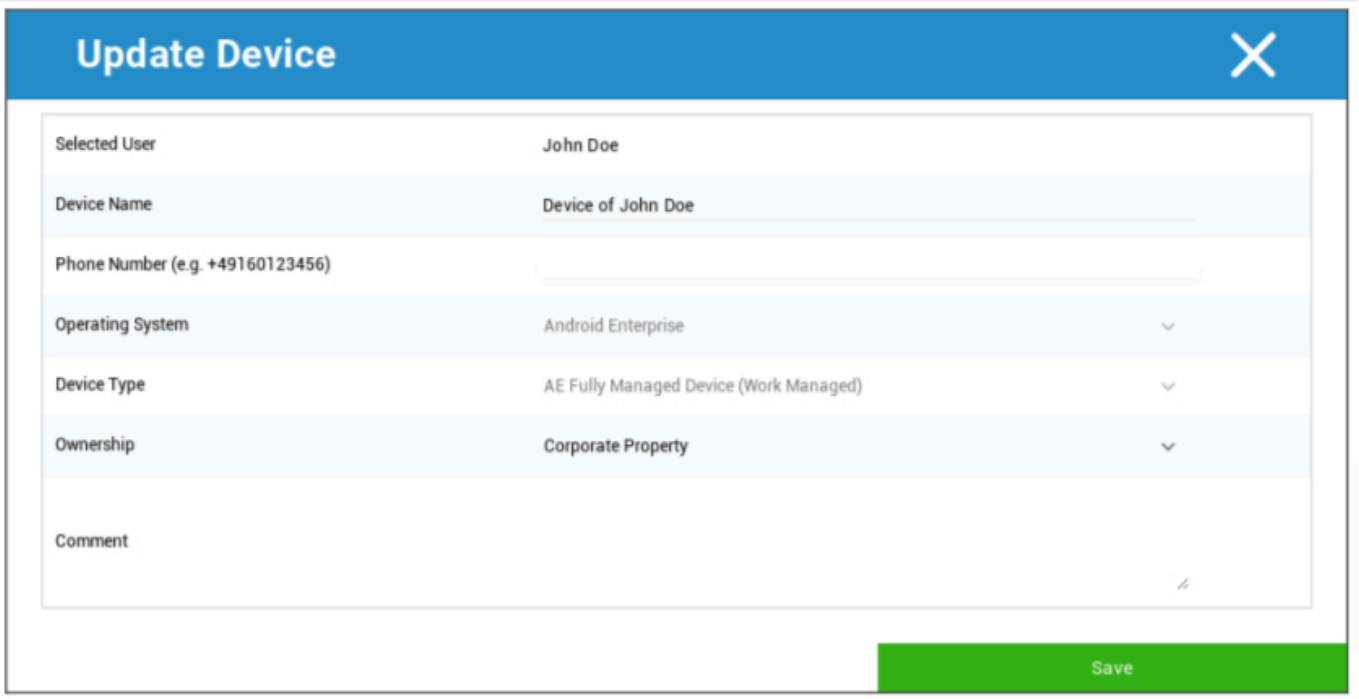


Modifica dispositivo	Modifica le informazioni del dispositivo
Imposta codice di accesso	Imposta il codice di accesso del dispositivo
Dispositivo di blocco	Blocca il dispositivo (schermata di blocco)
Elimina il dispositivo	Elimina il dispositivo da AppTec
Pulisci il dispositivo	Ripristina le impostazioni di fabbrica del dispositivo
Pulizia aziendale	Le informazioni, le applicazioni e i profili forniti da AppTec360 vengono eliminati (il dispositivo viene separato dall'MDM).
Rimuovi MDM	
Invia un messaggio	Invia notifiche push al dispositivo Il messaggio verrà visualizzato nell'AppTec360 (scheda Messaggio).
Controllo remoto di TeamViewer	Avvia una sessione di controllo remoto per questo dispositivo utilizzando TeamViewer
Telecomando Splashtop	Avvia una sessione di controllo remoto per questo dispositivo usando Splashtop
Trasformazione in modalità COPE (solo su dispositivi AE completamente gestiti (gestiti dal lavoro))	Creare un profilo di lavoro su questo dispositivo AE a gestione completa (gestito dal lavoro)
Invia la richiesta di iscrizione	Invia una richiesta di iscrizione (ripetuta)

Migrazione di un dispositivo legacy (solo su telefoni/tablet Android se registrati utilizzando la modalità di provisioning del proprietario del dispositivo)	Migrare il profilo di un telefono/tablet Android in un profilo AE di dispositivo completamente gestito (gestito dal lavoro)

Modifica dispositivo

Qui puoi aggiornare una serie di informazioni sul dispositivo.



Utente selezionato	Utente del dispositivo
Nome del dispositivo	Nome del dispositivo
Numero di telefono	Numero di telefono del dispositivo
Sistema operativo	Android Enterprise Android
Tipo di dispositivo	Android Enterprise: • Dispositivo AE completamente gestito (gestito dal lavoro) • Modalità profilo di lavoro AE (solo container) • Dispositivo AE completamente gestito con profilo di lavoro (COPE) Android: • Telefono • Tavoletta
Proprietà	Corporate = proprietà aziendale

	Dipendente = proprietà del dipendente
Commento	Descrizioni aggiuntive per il dispositivo

Cancella il codice di accesso

Qui puoi rimuovere il passcode del dispositivo selezionato. Per impostazione predefinita su Android, il codice di accesso sarà impostato su "123456" - questo può e deve essere modificato dall'utente in seguito.

Dispositivo di blocco

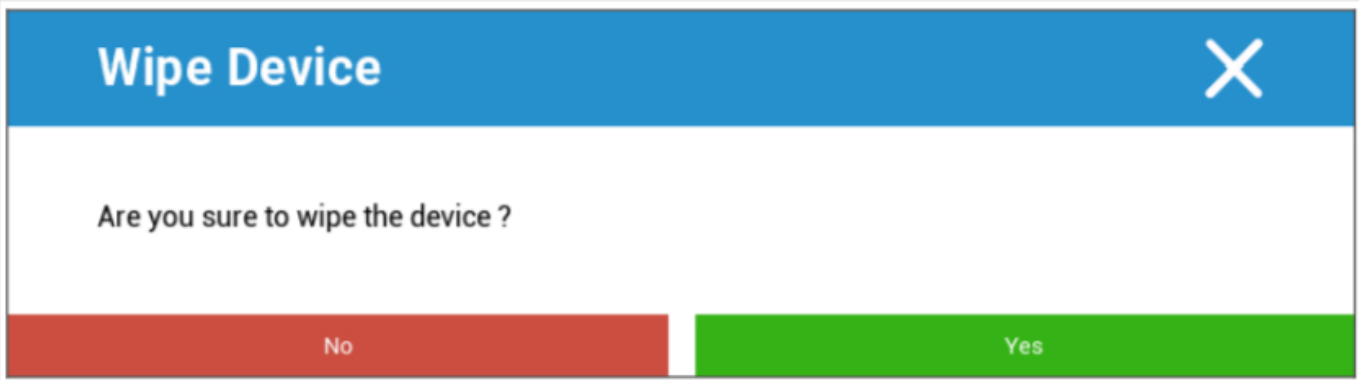
Qui verrà inviato un comando di blocco del dispositivo (schermata di blocco).

Elimina il dispositivo

Qui è possibile eseguire un comando di cancellazione. Puoi ancora una volta decidere se il dispositivo deve essere rimosso solo da AppTec360 ("Delete from System") o se deve essere rimosso da AppTec360 e ripristinato alle impostazioni di fabbrica ("Wipe & Delete").

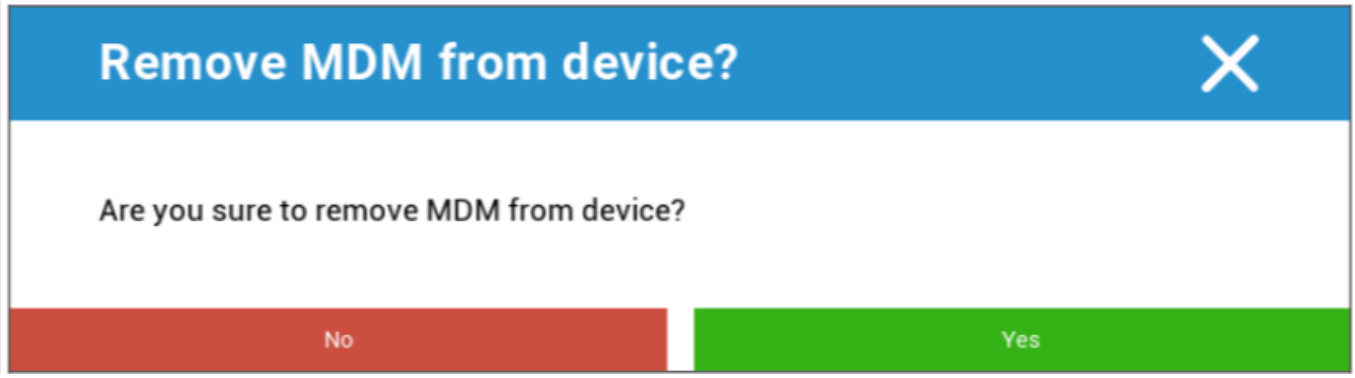
Pulisci il dispositivo

Alla voce "Wipe Device" puoi eseguire una cancellazione completa del dispositivo. Il dispositivo verrà quindi riportato alle impostazioni di fabbrica.



Inoltre, se il dispositivo contiene una scheda SD, puoi cancellare la scheda SD. Puoi ottenere questo risultato impostando "Wipe SD Card too? " a "On".

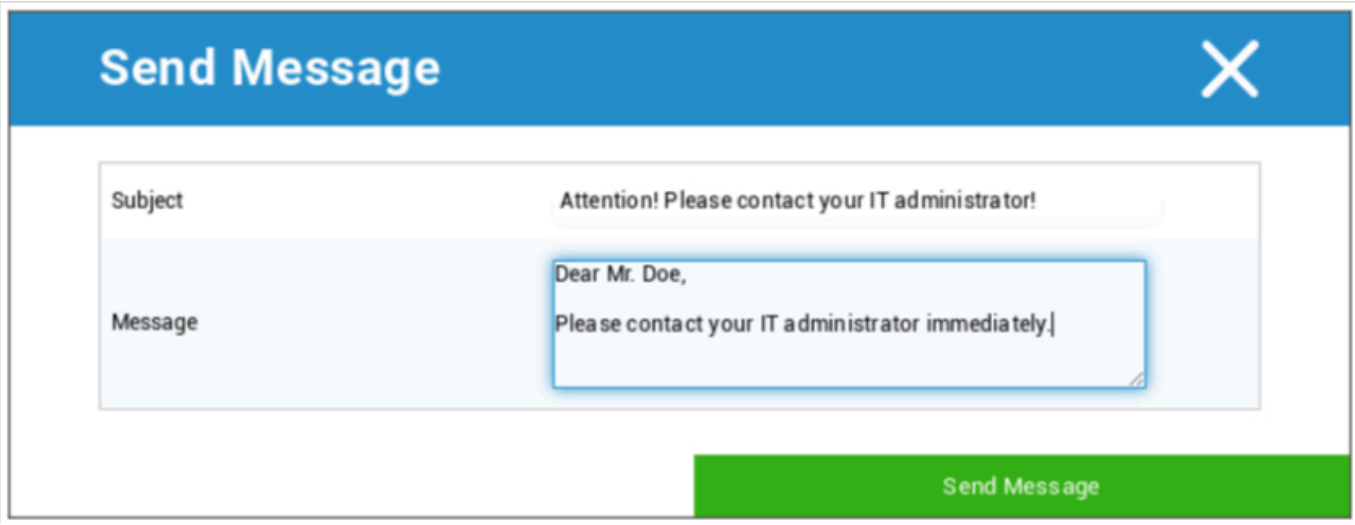
Rimuovi MDM



Questo è il metodo consigliato per creare una separazione da MDM.

Solo le informazioni, le app e i profili forniti da AppTec360 vengono eliminati, il che significa che tutti i dati aziendali non saranno più disponibili sul dispositivo dell'utente finale. La sfera privata, invece, non viene toccata e continua a rimanere sul dispositivo dell'utente finale.

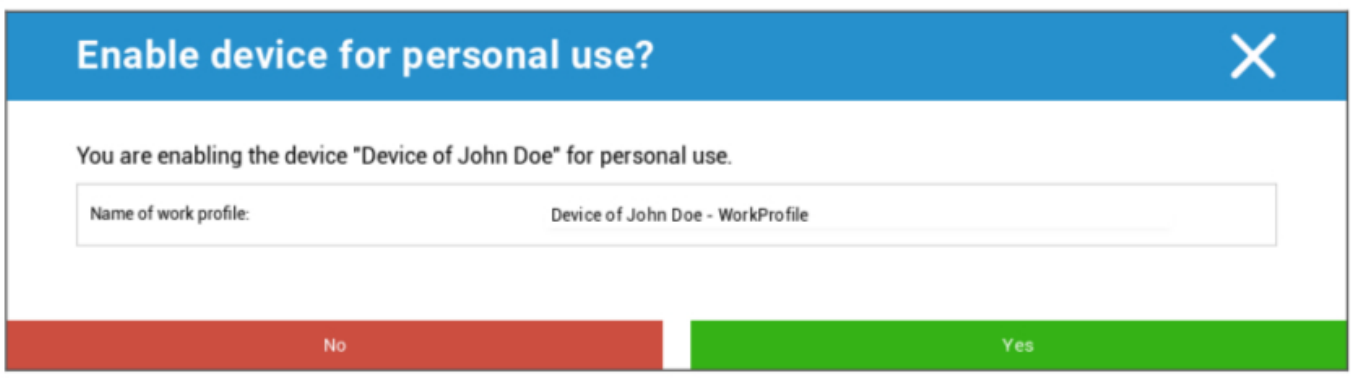
Invia un messaggio



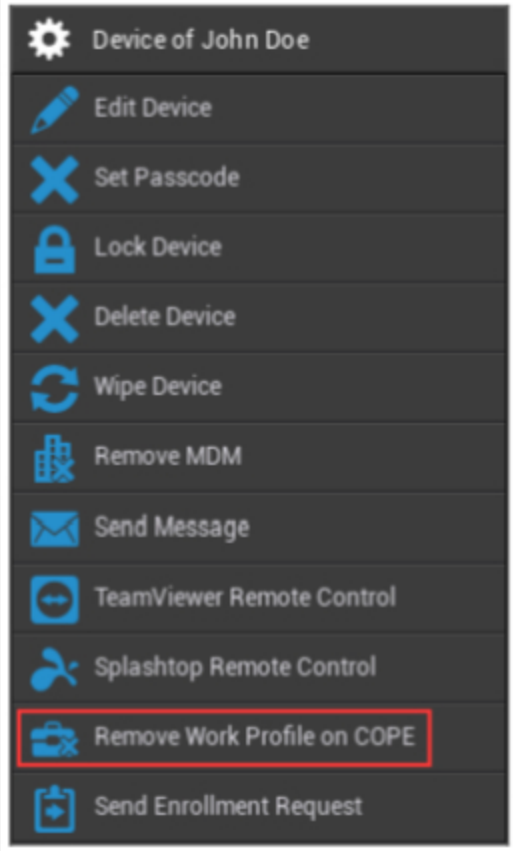
Qui puoi inviare una notifica push al rispettivo dispositivo dell'utente finale.

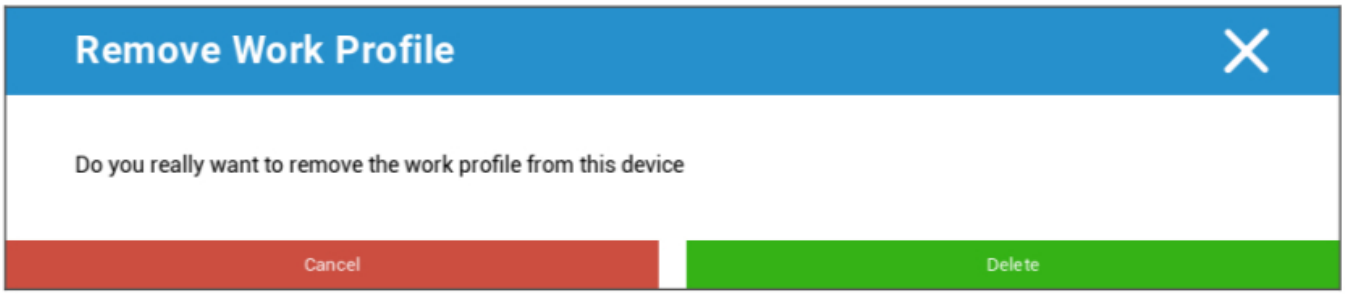
Trasforma in modalità COPE

Creare un profilo di lavoro su questo dispositivo AE a gestione completa (gestito dal lavoro)



Dopo aver trasformato il dispositivo in modalità COPE, puoi rimuovere il profilo di lavoro cliccando sull'opzione **Rimuovi profilo di lavoro su COPE:**




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

Invia la richiesta di iscrizione

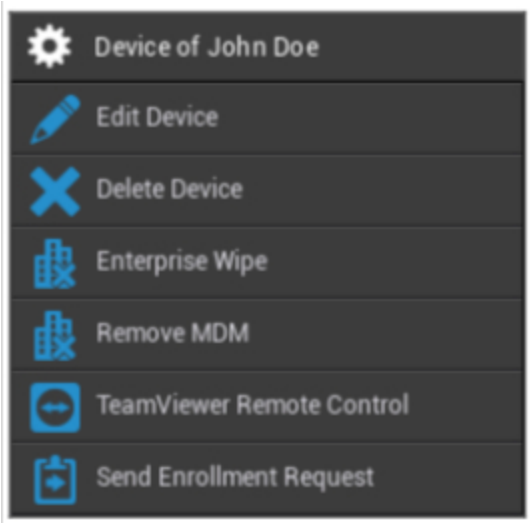
Con "Invia richiesta di iscrizione" puoi inviare una richiesta di iscrizione (di nuovo) al rispettivo utente.

Tieni presente che solo la richiesta di iscrizione più recente è valida.

Migrare un dispositivo legacy

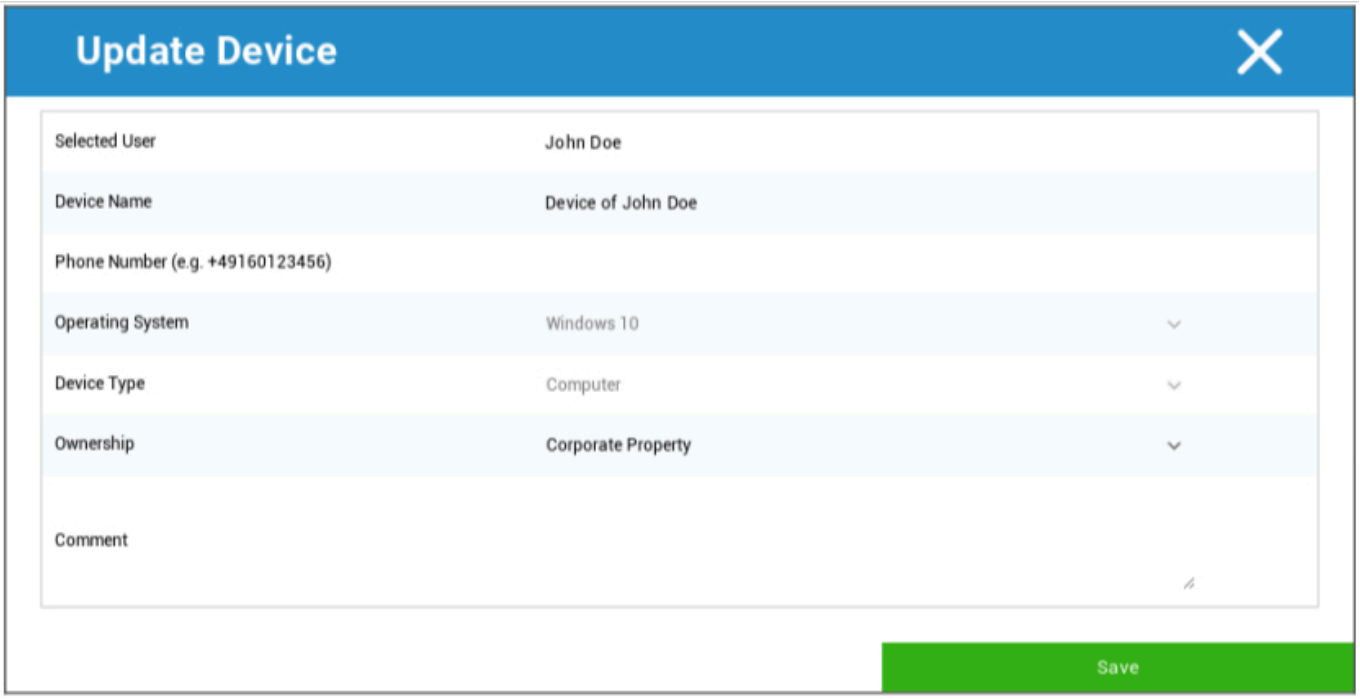
Migrare il profilo di un telefono/tablet Android in un profilo AE di dispositivo completamente gestito (gestito dal lavoro)

Finestre



Nome del dispositivo	Nome del dispositivo selezionato
Modifica dispositivo	Modifica dispositivo
Elimina il dispositivo	Rimuovi il dispositivo da AppTec
Pulizia aziendale	Le informazioni, le applicazioni e il profilo forniti da AppTec360 vengono eliminati
Rimuovi MDM	
Controllo remoto di TeamViewer	Controlla il dispositivo in remoto con TeamViewer
Invia la richiesta di iscrizione	Invia la richiesta di iscrizione (di nuovo)

Modifica dispositivo

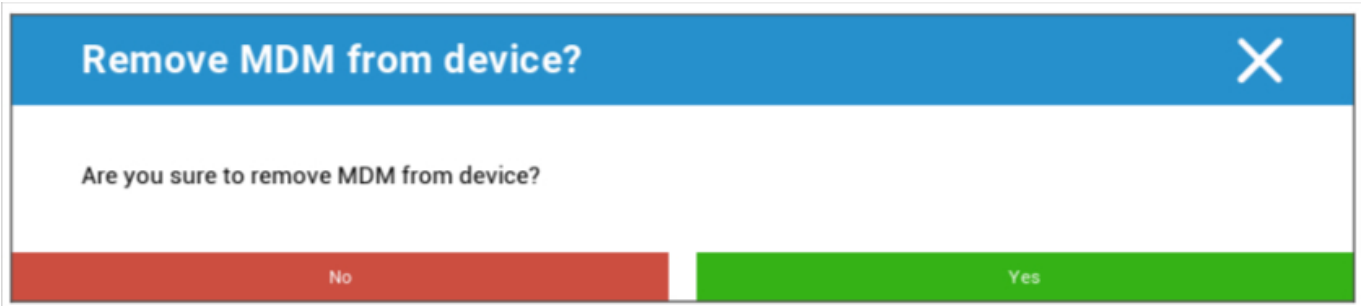


Qui puoi aggiornare una serie di informazioni sul dispositivo.

Elimina il dispositivo

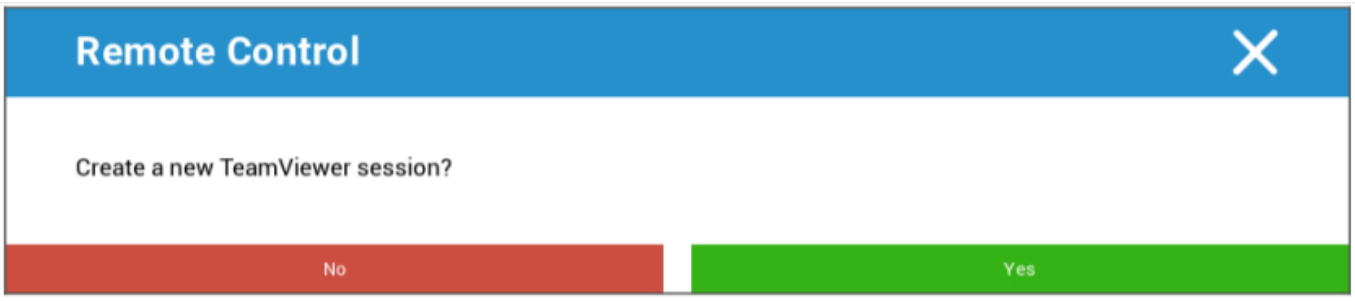
Qui è possibile eseguire il comando di cancellazione che rimuove il dispositivo da AppTec360.

Enterprise Wipe | Rimuovi MDM



Solo le informazioni, le applicazioni e i profili forniti da AppTec360 vengono cancellati. In questo modo, i dati aziendali non saranno più disponibili sul dispositivo dell'utente finale. L'area privata non viene toccata e continua a rimanere sul dispositivo dell'utente finale.

Controllo remoto di TeamViewer



Qui puoi avviare una sessione di Controllo remoto di TeamViewer per questo dispositivo.

Invia la richiesta di iscrizione

Con "Invia richiesta di iscrizione", puoi inviare una richiesta di iscrizione (di nuovo) al rispettivo utente.

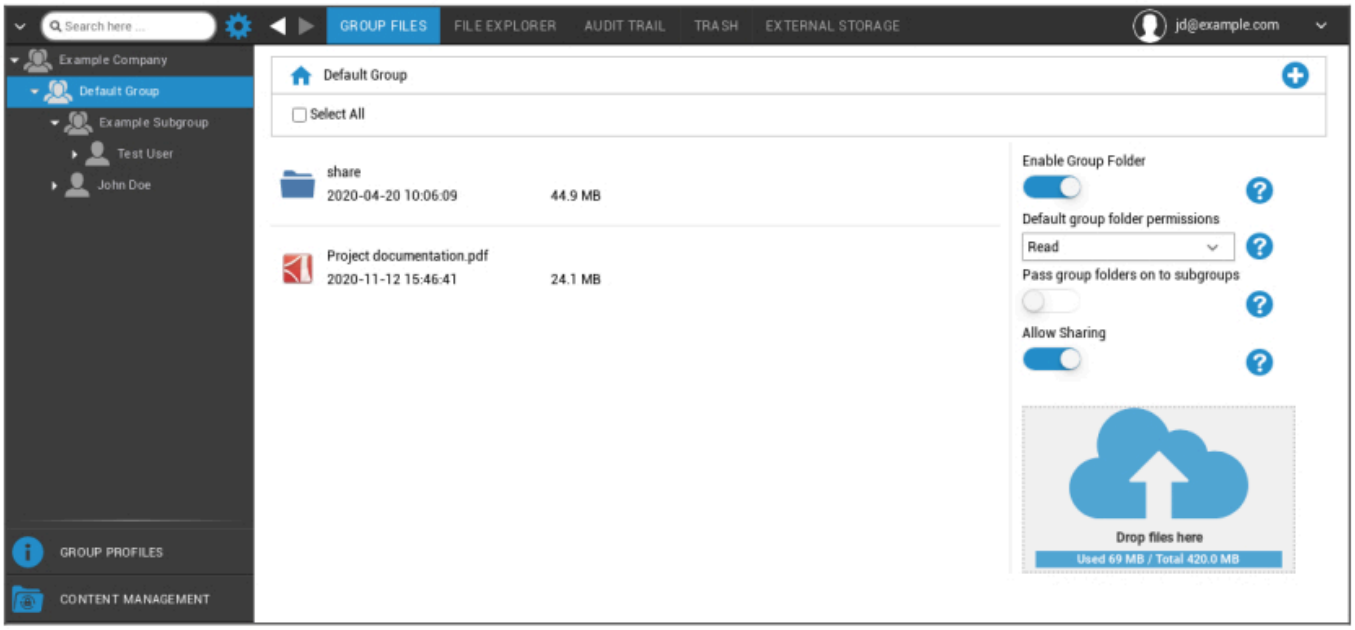
Gestione dei contenuti

Quando sei in un gruppo, puoi gestire il ContentBox di AppTec con "Gestione dei contenuti".

Con la Content Box puoi distribuire in modo sicuro documenti e altri dati aziendali ai dispositivi degli utenti finali.

File di gruppo

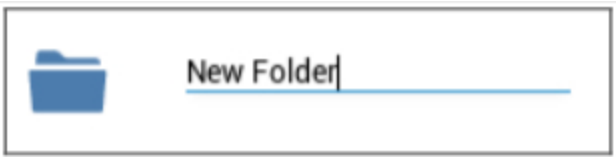
"File di gruppo" rappresenta una parte fondamentale di ContentBox. Qui puoi stabilire le impostazioni, caricare documenti, creare nuove cartelle, ecc.



Con il simbolo in alto a destra puoi creare nuove cartelle da assegnare al rispettivo gruppo con "Aggiungi cartella".

Con il simbolo in alto a destra, puoi creare una nuova cartella tramite "Aggiungi cartella", da assegnare al rispettivo gruppo.

Puoi dare alla cartella il nome che vuoi.



Tramite "Carica file" puoi caricare i dati. Qui si aprirà lo Standard-Explorer. Naturalmente puoi eseguire queste due azioni in ogni (sotto)cartella.

Con il simbolo in alto a sinistra puoi tornare al menu principale.

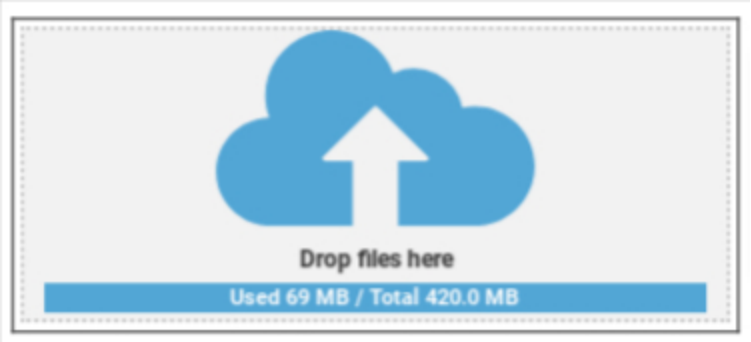
Puoi selezionare diverse cartelle e file e scaricarli con "Download" oppure cancellarli cliccando su "Delete".

Puoi anche selezionare tutti i file e le cartelle ed eseguire i comandi "Scarica" e "Elimina".

Quando passi il mouse su una cartella o un file, vedrai la seguente panoramica:

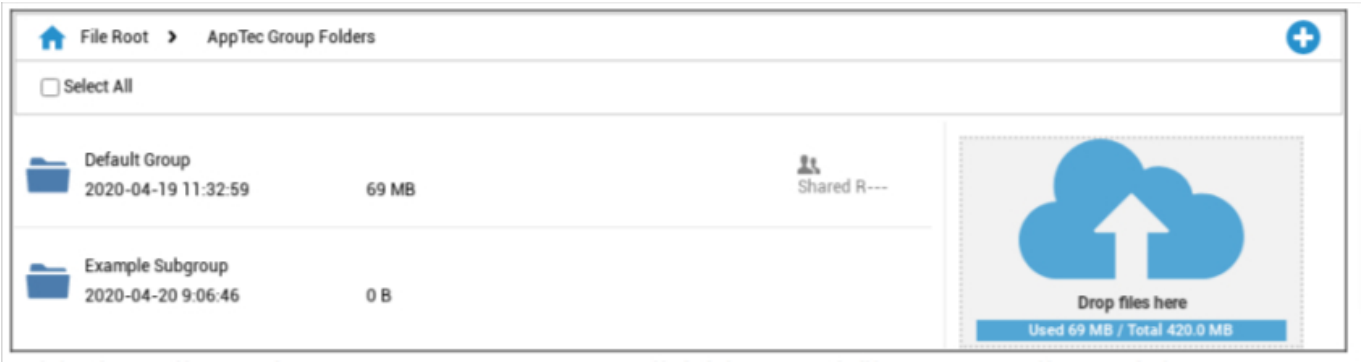
- Con "Rinomina", puoi rinominare la cartella/file
- Con "Download", puoi scaricare la cartella/file
- Con "Elimina", puoi cancellare la cartella/file

Abilita la cartella di gruppo	Se attivato, tutti i membri del gruppo hanno accesso alla rispettiva cartella.
Permessi predefiniti per le cartelle del gruppo	Permessi degli utenti del gruppo selezionato: Read = permesso di sola lettura Aggiornamento = permesso di aggiornamento Crea = permesso di creare Elimina = cancella il permesso
Passa le cartelle del gruppo ai sottogruppi	Se attivati, i rispettivi sottogruppi possono avere accesso ai file di dati della casa madre.
Permessi per i sottogruppi	Permessi degli utenti del sottogruppo selezionato: Read = permesso di sola lettura Aggiornamento = permesso di aggiornamento Crea = permesso di creare Elimina = cancella il permesso
Consenti la condivisione	Se attivato, l'utente può condividere i file tramite un link.



Per caricare i file, puoi utilizzare questo campo, estraendo un file tramite Drag & Drop in questa finestra. Puoi anche cliccare su questo campo per selezionare e caricare un file con l'aiuto di Internet Explorer.

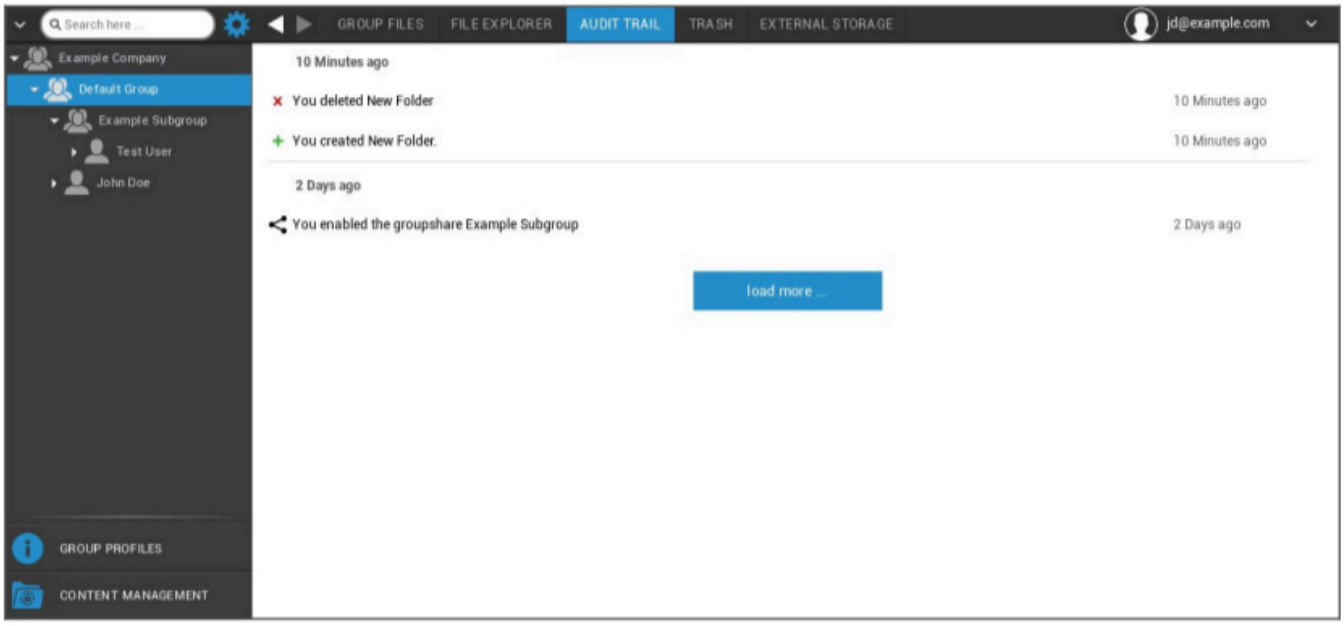
Esplora file



Con "File Explorer" puoi gestire tutte le cartelle e i file, indipendentemente dal gruppo in cui sono archiviati.

Troverai anche le impostazioni e i pulsanti che hai imparato a conoscere in "File di gruppo".

Traccia di controllo



In "Audit Trail" puoi vedere dalla cronologia quale utente ha creato, cancellato o condiviso cosa. In questo modo, potrai stabilire in qualsiasi momento cosa è stato fatto con i dati aziendali.

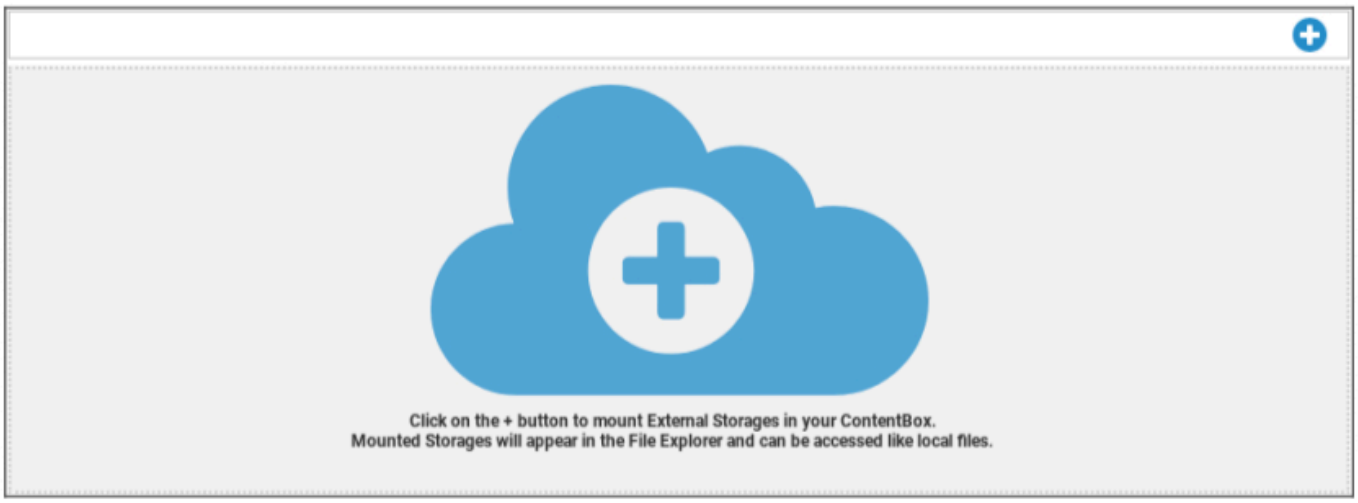
Cestino

Se hai cancellato qualcosa (per sbaglio), puoi vedere le cartelle e i file sotto la voce "Cestino" e recuperarli, secondo i tuoi desideri.

- Con "Undelete" puoi recuperare i dati/cartelle.
- Con "Elimina", puoi eliminare definitivamente i dati/cartelle; devi confermare il comando di eliminazione ancora una volta.

Tieni presente che la capacità di archiviazione utilizzata nel cestino riduce lo "Spazio totale" disponibile: questo è un requisito di ownCloud.

Archiviazione esterna



Alla voce "Memoria esterna" puoi collegare una memoria esterna.

Con il simbolo è possibile aggiungere (ulteriore) memoria.

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

Amazon S3	
Nome visualizzato	Nome visualizzato
Chiave di accesso	Chiave di accesso
Chiave segreta	Chiave di sicurezza
Secchio	L'identità definitiva della sottocartella che ti è stata assegnata
Nome host (opzionale)	Nome host (opzionale)
Porta (opzionale)	Porta (opzionale)
Regione	Regione (opzionale)
Abilita SSL	Abilita SSL
Abilita lo stile del percorso	Indirizzo Clear Path che ti è stato assegnato

FTP	
Nome visualizzato	Nome visualizzato
Ospite	Indirizzo host
Nome utente	Nome utente
Password	Password
Radice	Menu principale
Sicurezza ftps://	

SFTP	
Nome visualizzato	Nome visualizzato
Ospite	Indirizzo host
Nome utente	Nome utente
Password	Password
Radice	Menu principale

ownCloud	
Nome visualizzato	Nome visualizzato
URL	URL ownCloud
Nome utente	Nome utente
Password	Password
Sottocartella remota	Cartella standard
Sicurezza https://	

WebDAV	
Nome visualizzato	Nome visualizzato
URL	URL WebDAV
Nome utente	Nome utente
Password	Password
Radice	Menu principale
Sicurezza https://	
Condividi con Windows	Il supporto per Windows Share sarà presto disponibile
SharePoint	Il supporto per Microsoft SharePoint sarà presto disponibile

Registro di controllo

Qui puoi trovare un registro che registra le informazioni sulle azioni eseguite nella console MDM.

Con l'icona del filtro puoi applicare dei filtri all'elenco visualizzato.

Con il menu a tendina **Voci per pagina**: puoi selezionare la quantità di voci da visualizzare in una pagina dell'elenco.

Azione intrapresa / Impostazione modificata	L'azione intrapresa / L'impostazione modificata
Valore	Il valore dell'azione intrapresa/impostazione modificata
Utente	Il nome dell'utente che ha eseguito l'azione/modificato l'impostazione
Data	Il timestamp di quando questa azione è stata eseguita / questa impostazione è stata modificata
Percorso / Tipo	Il percorso in cui è stata eseguita questa azione o è stata modificata questa impostazione

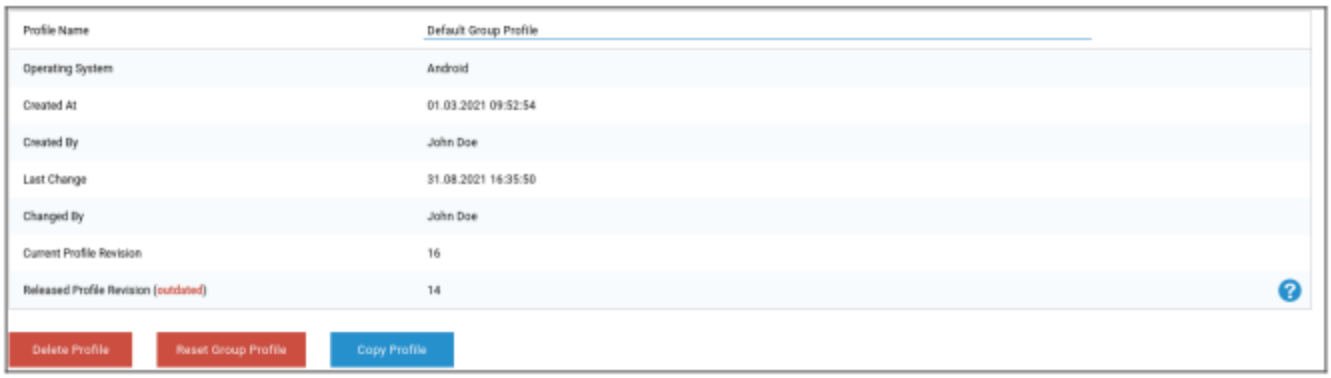
Configurazione iOS

Generale

A seconda che tu abbia selezionato un gruppo o un dispositivo, la visualizzazione e i relativi punti secondari sono diversi: presta molta attenzione a questo aspetto!

Panoramica del profilo del gruppo (solo a livello di gruppo)

Quando apri il profilo di un gruppo, otterrai una rapida panoramica del profilo stesso.



Nome del profilo	Nome del profilo (può essere modificato qui)
Sistema operativo	Sistema operativo per cui è stato creato il profilo
Creato a	Tempo della creazione
Creato da	Il creatore del profilo
Ultimo cambiamento	Ora dell'ultima modifica al profilo
Modificato da	Account che ha apportato le ultime modifiche
Revisione del profilo attuale	Revisione dello stato del profilo salvato
Revisione del profilo rilasciata	Revisione del profilo assegnata ("Assegna ora"). Se l'etichetta mostra " (outdated)" dietro il testo, significa che hai salvato il profilo ma non l'hai ancora assegnato, quindi i dispositivi riceveranno ancora la versione più vecchia.

Informazioni generali

Se ti trovi direttamente sul dispositivo, riceverai una breve panoramica del dispositivo selezionato.

Nome del dispositivo	Nome del dispositivo
Numero di telefono	Numero di telefono del dispositivo
Modello	Numero di modello
Sistema operativo	OS
Numero di serie	Numero di serie del dispositivo
Proprietà del dispositivo	Dispositivo aziendale o privato Corporate = dispositivo aziendale Dipendente = dispositivo privato
Tipo di dispositivo	Tipo di dispositivo (tablet o telefono)
Jailbroken	Se è presente un Jailbreak sul dispositivo
Supervisionato	Indica se si tratta di un dispositivo supervisionato
Conforme	Se sono state violate le linee guida
Ultimo visto	Stato dell'ultima comunicazione del dispositivo con il server AppTec360

Impostazioni

Queste impostazioni contengono il nome del dispositivo e uno sfondo predefinito.

Assegna al dispositivo il nome di sistema	Il nome che verrà assegnato nella Console di AppTec360 (nella struttura gerarchica di sinistra) sarà lo stesso del dispositivo dell'utente finale (visibile nelle impostazioni del dispositivo).
Usa uno sfondo personalizzato (solo per i dispositivi supervisionati)	Qui puoi predefinire lo sfondo che deve essere visualizzato sul dispositivo dell'utente finale (ad esempio per un tipo di branding aziendale per il dispositivo). È disponibile solo in modalità supervisionata!
Aggiornamenti automatici del sistema operativo	Forza gli aggiornamenti del sistema operativo se disponibili. Solo per i dispositivi DEP in modalità supervisionata.
Caratteri personalizzati	Qui puoi aggiungere dei font personalizzati.
Nome	Opzionale. Il nome visibile all'utente del font. Questo campo viene sostituito dal nome effettivo del font dopo l'installazione.
Carattere	Carica il file del font (.otf o .ttf).

Revisione della configurazione

Qui potrai vedere quale profilo di gruppo è stato assegnato al dispositivo.

Se clicchi sul profilo del gruppo, accederai direttamente al profilo e potrai eseguire le impostazioni.

Con il simbolo, puoi riportare le app assegnate alle impostazioni del profilo del gruppo.

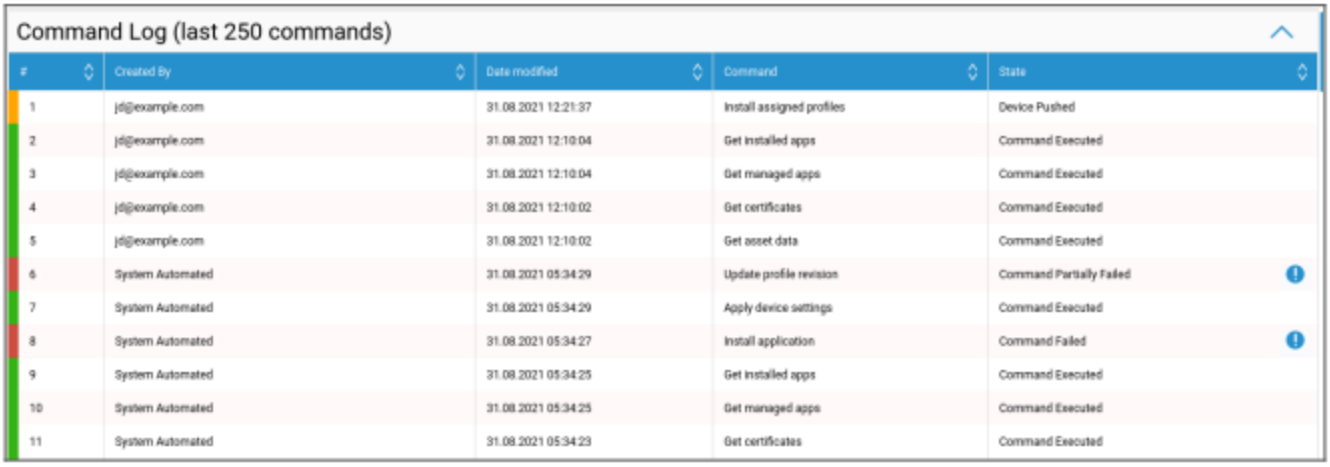
Con il simbolo, puoi reimpostare il profilo del dispositivo in modo che non abbia alcuna impostazione.

L'indicazione "Revisione più recente disponibile" indica che il profilo del gruppo è stato modificato e salvato ma non assegnato. Il profilo del gruppo deve essere assegnato con "Assegna ora" a livello di gruppo per applicare le modifiche ai dispositivi.

Registro del dispositivo (solo a livello di dispositivo)

Registro dei comandi

Qui puoi vedere quali comandi sono stati emessi per il dispositivo e qual è il loro stato.



I comandi creati da "Sistema automatico" vengono creati automaticamente dal sistema.

Possibili stati del comando

Dispositivo spinto	È stata inviata una richiesta push al servizio push (ad esempio APNS) per indicare al dispositivo di connettersi nuovamente al server EMM.
Comando creato	Il comando è stato creato nel sistema.
Comando inviato	Il comando è stato inviato al dispositivo dopo la connessione al server.
Comando eseguito	Il comando è stato eseguito con successo.
Comando fallito	Il comando è fallito. *
Comando parzialmente fallito	A seconda del sistema operativo del dispositivo, alcuni comandi possono essere raggruppati. In questo caso alcune parti di questo gruppo di comandi sono fallite. *
Comando eseguito, alla fine fallito	Il comando è stato eseguito ma forse non lo è stato.
Comando Riportato	Il comando è stato ripreso da un utente.
Scartato	Il comando è stato scartato. Ad esempio perché è stato sostituito da un altro comando o perché il dispositivo è stato reinserito e i vecchi comandi sono stati rimossi.

Se dietro il messaggio c'è un punto esclamativo, puoi ottenere maggiori informazioni passando il cursore sull'icona.

Gestione delle risorse (solo a livello di dispositivo)

Gestione delle risorse (solo a livello di dispositivo)

Info sul dispositivo

Modello	Numero di modello del dispositivo
Sistema operativo	OS
Versione OS	Versione del sistema operativo
Numero di serie	Numero di serie
UDID	UDID del dispositivo
Nome del dispositivo	Nome del dispositivo
Supervisionato	Visualizza se il dispositivo è supervisionato
Stato della batteria	Stato della batteria

Wi-Fi

Indirizzo IP	Indirizzo IP del dispositivo
WiFi MAC	Indirizzo MAC WiFi

Cellulare

Stato	Stato (scheda SIM presente)
Numero di telefono	Numero di telefono
Stato del roaming	Stato attuale del roaming
Roaming (voce/dati)	Stato del roaming per voce/dati
Indirizzo IP	Indirizzo IP
IMEI	Numero IMEI
Operatore/Vettore	Fornitore di servizi cellulari
SIM Rete del vettore	Rete del vettore SIM
Versione per il trasporto	Versione per portatori
Firmware del modem	Firmware del modem
Attuale MCC/MNC	Vedere "SIM MCC/MNC"
SIM MCC/MNC	Il Mobile Country Code è un codice di identificazione del paese stabilito dall'ITU in base alla norma E.212. Standard che, insieme al Mobile Network Code (MNC), viene utilizzato per identificare una rete cellulare (=codice paese). Quando entri in un'altra rete cellulare, il "Current MCC/MNC" e il "SIM MCC/MNC" sono quindi diversi.

Bluetooth

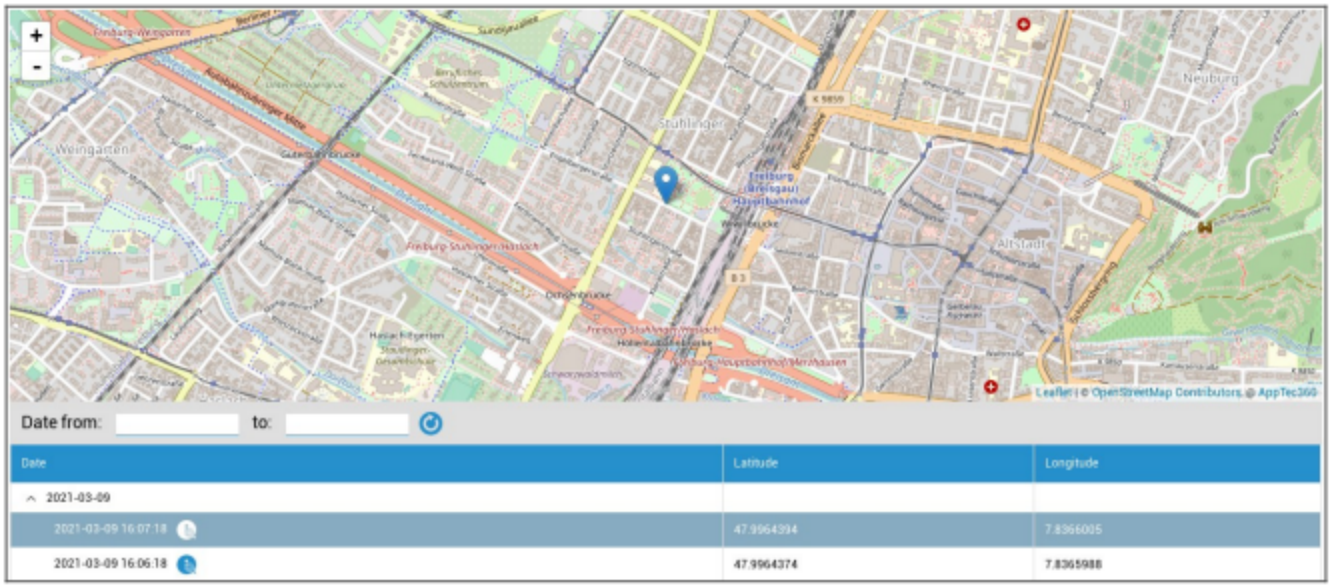
MAC Bluetooth	Indirizzo MAC Bluetooth

Gestione della sicurezza

Antifurto (solo a livello di dispositivo)

Informazioni GPS (solo a livello di dispositivo)

Qui puoi valutare la posizione attuale/ultima del dispositivo. La localizzazione può essere protetta con una o anche due password - Vedi: Impostazioni generali - Privacy - Accesso GPS



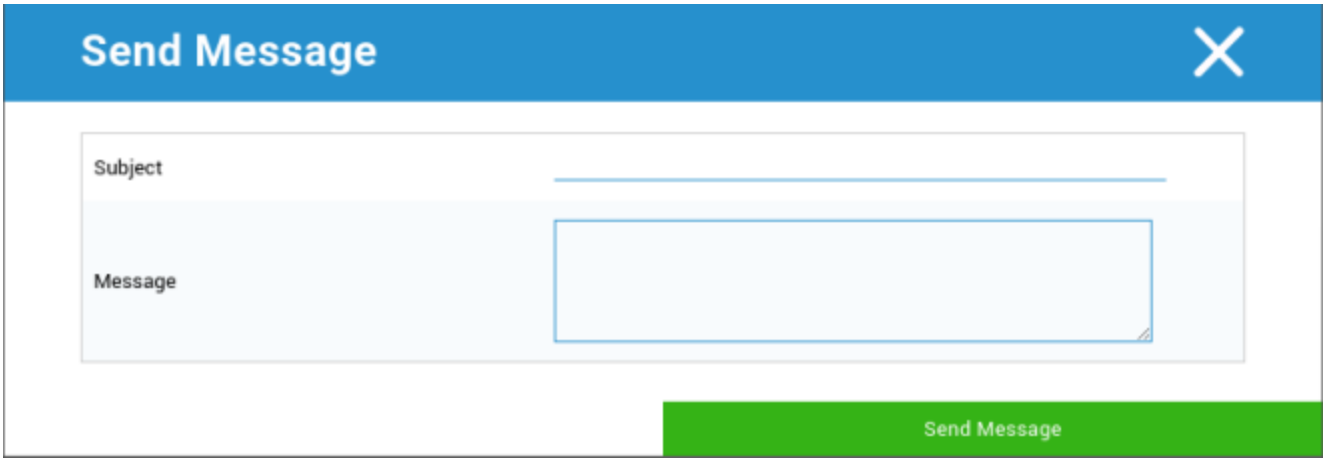
Pulisci e blocca (solo a livello di dispositivo)

In "Pulisci e blocca" puoi eseguire le seguenti tre azioni:

Pulizia completa	Il dispositivo viene riportato alle impostazioni di fabbrica (i dati aziendali e quelli personali vengono cancellati).
Pulizia aziendale	Solo i dati aziendali vengono rimossi dal dispositivo dell'utente finale (tutte le applicazioni, i dati, ecc. che sono stati forniti da AppTec)
Schermata di blocco	Il blocco dello schermo è attivato, è sufficiente sbloccare il dispositivo con la password/PIN del dispositivo.
Blocco forense (solo dispositivi supervisionati)	Se questa funzione viene attivata con il simbolo  , il dispositivo verrà bloccato, visualizzando un messaggio che non potrà essere chiuso. Il dipendente non può nemmeno sbloccare il dispositivo. Solo l'amministratore può sbloccare il dispositivo nella console con il simbolo di sblocco  .
Consenti il blocco dell'attivazione (solo per i dispositivi supervisionati)	Se questa funzione è attivata, il dispositivo sarà bloccato non appena "Trova il mio iPhone" sarà attivato nelle impostazioni di iCloud.

Messaggio (solo a livello di dispositivo)

Nella finestra seguente puoi inserire l'oggetto e un messaggio e inviarlo a un dispositivo dell'utente finale:



Configurazione della sicurezza

Codice di accesso

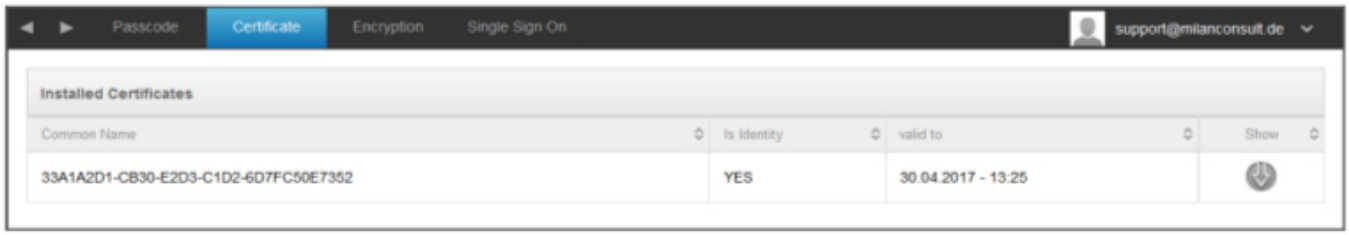
Qui puoi stabilire le impostazioni della password del dispositivo

Disattivazione del codice consentita	Quando questa impostazione è attivata, non viene richiesta l'immissione di una password. Una volta stabilita la password, questa non può essere disattivata.
Consenti un valore semplice	Consenti all'utente di utilizzare stringhe di numeri uguali, crescenti e decrescenti (es. 1234, 1111).
Richiedi un valore alfanumerico	Le password devono contenere almeno una lettera
Lunghezza minima del codice di accesso	Lunghezza minima della password
Numero minimo di caratteri complessi	Numero minimo di simboli alfanumerici nella password
Età massima del codice di accesso	Numero di giorni dopo i quali la password deve essere cambiata
Blocco automatico massimo	Tempo massimo dopo il quale il dispositivo viene bloccato
Periodo massimo di tolleranza per il blocco del dispositivo	Tempo, dopo il quale il dispositivo entra in Stand-By bloccato.
Numero massimo di tentativi falliti	Stabilisce quante volte una password può essere inserita in modo errato prima che venga eseguita una cancellazione completa del dispositivo.
Età massima del passcode (1-730 giorni)	Età massima della password
Cronologia dei codici (1-50 codici)	L'uso di una vecchia password è consentito dopo questo numero

Facendo clic sul cestino, si apre la finestra di dialogo Password-Reset, con la quale è possibile cancellare la password del dispositivo dimenticata.

Certificato (solo a livello di dispositivo)

Visualizza i certificati disponibili sul 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

Crittografia

Richiedi la crittografia dello storage	Attiva la funzione di crittografia del dispositivo installato

Single Sign-On

Al punto "Single Sign-On", puoi configurare l'autenticazione Kerberos.

Qui si stabiliscono le credenziali di accesso e i rispettivi URL/app che possono utilizzare i token Kerberos.

Disponibile in modalità supervisionata	
Nome del conto	Nome del conto
Nome principale	Identità unica a cui distribuire i biglietti Kerberos
Regno	Il tuo Realm Kerberos da utilizzare (es. il tuo dominio)

Con il Simbolo puoi creare altri URL.

Modello di URL utilizzato per limitare questo account	URL da determinare, a cui possono essere distribuiti i Ticket Kerberos

Con il Simbolo puoi creare altre App.

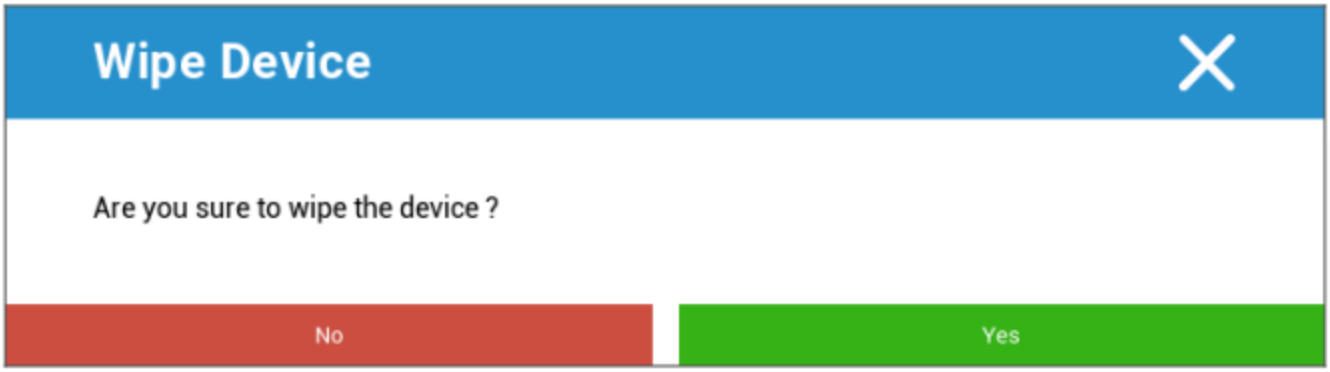
Applicazioni per limitare questo account	App da determinare, a cui possono essere distribuiti i ticket Kerberos

Fine vita (solo a livello di dispositivo)

Pulisci (solo a livello di dispositivo)

Alla voce "Wipe", puoi ripristinare le impostazioni di fabbrica del dispositivo. In questo caso i dati aziendali e privati verranno eliminati sul dispositivo dell'utente finale.

Cliccando sul "simbolo del meno" riceverai il seguente messaggio



Con "Sì" puoi eseguire la pulizia.

In "Wipe Report" possono essere visualizzati i seguenti elementi

Cancellata da	Storia di chi ha eseguito la pulizia
Data	Data
Stato	Stato (ad esempio, se il Wipe è stato eseguito con successo)

Impostazioni di restrizione

Funzionalità del dispositivo

Qui puoi bloccare le funzionalità dei singoli dispositivi dell'utente finale

Consenti l'installazione di app	Consentire l'installazione di applicazioni
Consenti alla fotocamera	Consenti l'uso della fotocamera
Consenti FaceTime	Consenti FaceTime
Consenti la cattura dello schermo	Consenti la cattura dello schermo
Consenti la sincronizzazione automatica durante il roaming	Consenti la sincronizzazione automatica durante il roaming
Consenti a Siri	Consenti a Siri
Consenti la composizione vocale	Consenti la composizione vocale
Consenti l'acquisto in-app	Consenti l'acquisto in-app
Richiedi la password di iTunes Store per tutti gli acquisti	Richiedi la password di iTunes Store per tutti gli acquisti
Consentire il gioco in multiplayer	Consentire il gioco in multiplayer
Consente di aggiungere amici a Game Center	Consente di aggiungere amici a Game Center
Consenti l'apertura da gestito a non gestito	Consenti l'apertura dei contenuti delle app gestite nelle app non gestite
Consenti l'apertura da non gestito a gestito	Consentire l'apertura di contenuti di app non gestite in app gestite
Consenti la visualizzazione di oggi nella schermata di blocco	Quando questa impostazione è attiva, la vista "Oggi" verrà visualizzata nel Centro notifiche della schermata di blocco.
Consenti il centro di controllo nella schermata di blocco	Consenti il Centro di Controllo sulla schermata di blocco
Consenti TouchID	Consenti TouchID
Consenti gli aggiornamenti PKI over-the-air	Consenti gli aggiornamenti PKI over-the-air

Consenti il passbook quando è bloccato	Consenti il passbook quando il dispositivo è bloccato
Limitare il tracciamento degli annunci	Questa funzione disattiva l'Ad Tracking (ad esempio, gli inserzionisti non possono utilizzare l'Ad Tracking per distribuire annunci personalizzati).
Consenti Handoff	Consenti Handoff
Consenti i risultati di internet in primo piano	Consenti i risultati di internet in spotlight (ad esempio Bing o Wikipedia)
Richiedi un codice di accesso al primo accoppiamento AirPlay	Richiedi un codice di accesso al primo accoppiamento AirPlay
Protezione da polso per orologi Force	Se attivato, l'Apple Watch è costretto a utilizzare la "Protezione del polso" (riconoscimento del polso).
Consenti la Libreria foto di iCloud	Consente di utilizzare la Libreria foto di iCloud. Se non è consentito, tutte le immagini che non sono state scaricate completamente da iCloud verranno cancellate dalla memoria locale.
Disponibile in modalità supervisionata	
Consenti la modifica dell'account	Consenti la modifica di "posta, contatti, calendario".
Consenti AirDrop	Consenti AirDrop
Consenti la modifica cellulare dell'app	Questa impostazione blocca l'impostazione di quali applicazioni sono autorizzate a utilizzare i dati mobili. Questa impostazione può, ad esempio, essere impostata manualmente sul dispositivo dell'utente finale e quindi questa restrizione può essere attivata.
Permetti a Siri di interrogare i contenuti generati dagli utenti sul web	La ricerca su alcuni siti web è bloccata, ad esempio. Wikipedia, perché tutti possono apportare modifiche a proprio piacimento.
Attiva il filtro per le bestemmie di Siri	Le bestemmie rivolte a Siri vengono censurate.
Consenti iBook Store	Consenti iBook Store
Consenti a iBook Store Erotica	Consenti a iBook Store Erotica
Consente di modificare le impostazioni di Trova i miei amici	Consente di modificare le impostazioni di Trova i miei amici

Consenti Game Center	Consenti Game Center
Consenti l'accoppiamento dell'host	Accoppiamento del computer di controllo
Consente l'installazione di profili di configurazione	Consente l'installazione di profili di configurazione
Consenti di rimuovere l'applicazione	Rimozione delle app di controllo
Consenti iMessage	Consenti iMessage
Consente di cancellare tutti i contenuti e le impostazioni	Consente di cancellare tutti i contenuti e le impostazioni
Consente di configurare le restrizioni	Consente di configurare le restrizioni
Consenti il Podcast	Consenti il Podcast
Consenti la ricerca delle definizioni	Consenti la ricerca delle definizioni
Consenti la tastiera predittiva	Consenti la tastiera predittiva
Consenti la correzione automatica	Consenti la correzione automatica
Consenti l'installazione di app UI	Se è disattivato, non è possibile installare applicazioni dall'AppStore pubblico (l'icona non sarà più visualizzata). Tuttavia, le app possono ancora essere installate tramite iTunes e il Configuratore.
Consenti le scorciatoie da tastiera	Consenti le scorciatoie da tastiera, se il dispositivo è collegato a una tastiera fisica
Consenti l'accoppiamento dell'Apple Watch	Impedisce l'accoppiamento tra il dispositivo e l'Apple Watch; le connessioni esistenti verranno interrotte.
Consenti la modifica del codice di accesso	Se non è consentito, nessuna password del dispositivo può essere aggiunta, modificata o rimossa.
Consenti la modifica del nome del dispositivo	Linee guida per determinare se il nome del dispositivo può essere cambiato
Consenti la modifica dello sfondo	Linee guida per determinare se la carta da parati può essere cambiata
Consenti il download automatico delle app	Se disattivata, un'app acquistata non verrà installata automaticamente su altri dispositivi. Non si applica agli aggiornamenti per le app esistenti

Consenti le notizie	Consenti le notizie sul dispositivo iOS
Consenti la fiducia nelle app aziendali	Se impostato su false, impedisce di fidarsi delle applicazioni aziendali.

iCloud

Blocca alcune funzionalità durante l'accoppiamento con iCloud

Consenti il backup	Consenti il backup
Consenti la sincronizzazione dei documenti	Consenti la sincronizzazione dei documenti
Consenti il flusso di foto	Consenti il flusso di foto
Consenti lo streaming di foto condivise	Consenti lo streaming di foto condivise
Consenti la sincronizzazione del portachiavi nel cloud	Consenti la sincronizzazione del portachiavi nel cloud
Consenti alle app gestite di memorizzare i dati	Consenti alle app gestite di memorizzare i dati
Consenti la sincronizzazione delle note e delle evidenziazioni per i libri aziendali	Consenti la sincronizzazione delle note e delle evidenziazioni per i libri aziendali
Consente il backup dei libri aziendali	Consente il backup dei libri aziendali

Sicurezza e privacy

Blocca queste funzionalità associate ai dati diagnostici

Consente l'invio di dati diagnostici ad Apple	Consentire l'invio di dati diagnostici ad Apple
Consenti all'utente di accettare certificati TLS non attendibili	Consenti all'utente di accettare certificati TLS non attendibili
Forza i backup criptati	Forza i backup criptati

BYOD

Sicurezza iOS integrata (contenitore)

iOS è sempre stato in grado di fare la differenza tra gestito (business) e non gestito (privato). Tutto ciò che proviene dal sistema MDM viene trattato come gestito. Ad esempio, se installi un'app tramite MDM o configuri un account Exchange, questo verrà trattato come gestito da iOS.

Tutto il resto che viene configurato/installato manualmente sul dispositivo sarà trattato come non gestito. Ad esempio se l'utente installa WhatsApp da solo o se aggiunge un account Exchange. Tuttavia questa separazione non ha mai influito sui contatti. Ma da iOS 11.3 (e successivi) questa funzione è stata aggiunta anche per i contatti.

Poiché si tratta di una funzionalità di base del sistema operativo, non è necessario installare qualcosa o configurare un contenitore speciale.

Attiva la funzione integrata per separare le applicazioni/informazioni/file private da quelle aziendali. Questa impostazione disabilita anche alcune altre funzioni, che potrebbero altrimenti disattivare per errore alcune parti di questa separazione.

Attivazione

Attiva le soluzioni-contenitore supportate da AppTec360

Abilita il contenitore Google Divide	Abilita il contenitore Google Divide
Abilita il contenitore SecurePIM	Abilita il contenitore SecurePIM

Se hai attivato il SecurePIM Container, troverai anche il seguente punto alla voce "Attivazione". Inoltre, si apriranno subito altre quattro schede, descritte di seguito.

Indirizzo e-mail dell'assistenza	Indirizzo e-mail di supporto a cui l'utente può rivolgersi in caso di problemi

Password SecurePIM

In "Password SecurePIM" puoi stabilire le linee guida per la sicurezza della password.

Timeout della sessione	Qui puoi stabilire dopo quanti minuti deve essere inserita una nuova password, una volta che SecurePIM viene eseguito in background.
Lunghezza della password	Lunghezza della password per l'accesso al SecurePIM Container
Caratteri maiuscoli	Caratteri maiuscoli minimi
Caratteri minuscoli	Caratteri minuscoli minimi
Caratteri speciali	Caratteri speciali minimi
Cifre	Cifre minime
Applicazione della salvietta	Numero di volte in cui una password può essere inserita in modo errato, prima che il contenuto di SecurePIM venga cancellato. (L'applicazione rimane comunque sul dispositivo dell'utente finale).

Sicurezza SecurePIM

In "Sicurezza SecurePIM" puoi stabilire una serie di impostazioni di sicurezza.

Rileva i dispositivi jailbroken	Se questa impostazione è attivata, l'accesso al SecurePIM Container verrà bloccato non appena il dispositivo verrà riconosciuto come jailbroken.
Campi di testo sicuri	Il contenuto dei campi di invio sarà criptato e nessuna informazione raggiungerà il sistema operativo (iOS). Nota: finché questa impostazione è attiva, la correzione automatica non è più disponibile.
Esporta i dati dei contatti sul dispositivo	Se questa impostazione è attivata, l'utente può esportare i contatti di Exchange sul proprio dispositivo locale. Nota: vengono esportati solo il nome e il numero di telefono.
Luogo dell'evento	Se questa impostazione è attivata, la posizione dei prossimi eventi sarà visualizzata nella barra delle notifiche.
Mostra il titolo dell'evento	Se questa impostazione è attivata, la posizione del titolo dell'evento imminente verrà visualizzata nella barra delle notifiche.

Browser SecurePIM

Qui puoi configurare il browser di SecurePIM.

Con il simbolo puoi definire un nuovo URL.

Con il simbolo, puoi rimuovere nuovamente un URL definito.

Gli "URL whitelisted" sono URL che possono essere caricati.

Gli "URL in lista nera" sono URL che non possono essere caricati e quindi bloccati.

Tieni presente che le voci della Whitelist hanno una priorità maggiore rispetto alle voci della Blacklist. Alla voce "Titolo del segnalibro" puoi inserire un titolo. Con "Bookmark URL" puoi associare l'indirizzo URL al titolo del segnalibro: in questo modo potrai distribuire segnalibri personalizzati ai rispettivi utenti.

Scambio

Alla voce "Exchange" puoi configurare un account Exchange.

Indirizzo e-mail di ActiveSync	Indirizzo di posta elettronica di Exchange (fare attenzione ai "segnaposto")
Accesso a ActiveSync Exchange	Nomi degli utenti di Exchange (notare i "segnaposto")
ActiveSync Exchange Server	Indirizzo del server di Exchange (FQDN)
Dominio ActiveSync Exchange	Indirizzo di dominio di Exchange
Certificato utente	Certificato utente
Autenticazione basata su certificati	L'utente si autentica con un certificato
Consenti la crittografia S/MIME	Permette all'utente di crittografare la propria posta elettronica
Consenti la firma S/MIME	Permette all'utente di firmare la propria posta
Controllo CRL	Se attivo, il certificato privato verrà confrontato con la CRL (Certificate Revocation List).

Gestione delle connessioni

Wi-Fi

Identificatore del set di servizi (SSID)	SSID della rete da collegare
Auto Join	Attiva l'adesione automatica quando ti unisci a una rete
Rete nascosta	Attiva, nel caso in cui l'AP non trasmetta il SSID

Configurazione del proxy

Configurazione di un proxy per ogni punto di accesso

Nessuno	Non stabilire un Proxy
Manuale	Stabilire un Proxy manuale
URL del server proxy	Indirizzo per accedere alle impostazioni del proxy
Porto	Stabilisci la porta per il Proxy
Autenticazione	Nome utente per l'autenticazione sul Proxy
Password	Password per l'autenticazione sul Proxy
Automatico	Stabilisci automaticamente un Proxy
URL del server proxy	URL per accedere alle impostazioni del Proxy

Tipo di sicurezza

Stabilire il tipo di sicurezza per l'AP

WEP	
Password	Password per l'AP

WPA/WPA2	
Password	Password per l'AP

WEP Impresa - WPA / WPA2 Impresa - Qualsiasi Impresa			
	Protocolli		
	TLS	Attiva/Disattiva	
	TTLS	Attiva/Disattiva	
	LEAP	Attiva/Disattiva	
	PEAP	Attiva/Disattiva	
	EAP-FAST	Attiva/Disattiva	
	EAP-SIM	Attiva/Disattiva	
	Usa il PAC		Uso del PAC (Controllo dell'accesso protetto)
	Provvedimento PAC	Configurazione di Provision PAC	
	Fornitura di PAC in forma anonima	Fornitura anonima di PAC	
	Autenticazioni interne	Protocollo di autenticazione da utilizzare: PAP, CHAP, MSCHAP, MSCHAPv2	
	Nome utente	Nome utente di autenticazione	
	Non usare la password per la connessione	Non usare la password per la connessione	
	Certificato di identità	Carica/seleziona il certificato di autenticazione	
	Identità esterna	Identità visibile all'esterno	
	Fiducia		
	Certificato di fiducia 1	Carica il primo certificato attendibile	
	Certificato di fiducia 2	Carica il secondo certificato attendibile	
	Certificato di fiducia 3	Carica un terzo certificato attendibile	
	Nomi dei certificati dei server affidabili	I nomi dei certificati del server previsti (in un elenco separato da virgole)	

Nessuno	Non stabilire alcuna sicurezza

VPN

Nome della connessione	Nome del profilo VPN

Tipo di VPN

VPN

Tutto il traffico di rete del dispositivo sarà instradato attraverso una connessione VPN.

Tipo di connessione	Stabilisci il tipo di connessione VPN
IPsec (cisco)	Protocollo IPsec di cisco
PPTP	Protocollo PPTP
L2TP	Protocollo L2TP
Cisco AnyConnect	Protocollo AnyConnect
Juniper SSL	Protocollo SSL Juniper
F5 SSL	Protocollo SSL F5
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protocollo VIA di Aruba
SSL personalizzato	Connessione tramite SSL personalizzato
OpenVPN	Protocollo OpenVPN

VPN per app

Quando si apre una determinata applicazione, viene stabilita una connessione VPN.

Avvia automaticamente la connessione VPN per app		Avvia automaticamente la connessione VPN per app
Tipo di connessione		Stabilisci il tipo di connessione VPN
	Cisco AnyConnect	Protocollo AnyConnect
	Juniper SSL	Protocollo SSL Juniper
	F5 SSL	Protocollo SSL F5
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protocollo VIA di Aruba
	SSL personalizzato	Connessione tramite SSL personalizzato
	OpenVPN	Protocollo OpenVPN

Configurazione del proxy

Configurazione di un Proxy per la connessione VPN

Nessuno	Non stabilire un Proxy
Manuale	Stabilire manualmente un Proxy
URL del server proxy	Indirizzo per accedere alle impostazioni del proxy
Porto	Stabilisci la porta per il Proxy
Autenticazione	Nome utente per l'autenticazione al Proxy
Password	Password per l'autenticazione al Proxy
Automatico	Stabilisci automaticamente un Proxy
URL del server proxy	URL per accedere alle impostazioni del Proxy

Mostra segnaposto	Visualizza tutte le variabili-utente disponibili che AppTec360 può utilizzare.

APN

Nome del punto di accesso	Nome del punto di accesso
Nome utente del punto di accesso	Nome utente dell'Access Point
Password del punto di accesso	Password del punto di accesso
Server Proxy	Indirizzo del server proxy
Porto	La rispettiva porta Proxy

Cellulare

Abilita il roaming dati	Abilita il roaming dati
Abilita il roaming vocale	Abilita il roaming vocale
Abilita l'hotspot	Abilita l'hotspot

Proxy HTTP

Tipo di proxy	
Manuale	Stabilisci un Proxy manualmente
URL del server proxy	Indirizzo per accedere alle impostazioni del Proxy
Porto	Stabilisci la porta Proxy
Autenticazione	Nome utente per l'autenticazione al Proxy
Password	Password per l'autenticazione al Proxy
Automatico	Stabilisci automaticamente un Proxy
URL PAC proxy	URL PAC proxy
Consenti la connessione diretta se il PAC non è raggiungibile	Consenti la connessione diretta (senza VPN), se il PAC non è raggiungibile
Consente di bypassare il proxy per accedere a reti riservate	Consente di bypassare il proxy per accedere a reti interne vincolate

AirPrint

Indirizzo IP	Indirizzo IP della stampante
Percorso delle risorse	Percorso definito per il dispositivo AirPrint

AirPlay

Nome del dispositivo	Nome del dispositivo
Password	Password di accoppiamento
Whitelist	Definisci un elenco di dispositivi con cui il dispositivo può accoppiarsi in modo esclusivo

Gestione del PIM

Sincronizzazione attiva di Exchange

Nome del conto	Nome dell'account e-mail
Host di Exchange ActiveSync	Indirizzo/FQDN del server
Consenti lo spostamento	Consentire lo spostamento delle e-mail
Utilizza solo per la posta	Le interazioni possono avvenire solo sull'app nativa Mail
Usa l'SSL	Usa la crittografia SSL
Dominio	Dominio del server
Utente	Nome utente
Indirizzo e-mail	indirizzo e-mail (solo a livello di dispositivo)
Password (solo a livello di dispositivo)	Password utente
Certificato di identità	Seleziona il rispettivo certificato per l'autenticazione sul server.
Giorni passati di Mail to Sync	Numero di giorni fino a quando le e-mail devono essere sincronizzate. Nessun limite = illimitato
Abilita S/MIME	Abilita la crittografia S/MIME
Certificato di firma	Carica il rispettivo certificato di firma
Certificato di crittografia	Carica il rispettivo certificato di crittografia

eMail

Configurazione di account POP3 / IMAP sul dispositivo dell'utente finale

Descrizione dell'account	Nome degli account e-mail		
Tipo di conto	IMAP	Prefisso del percorso	Il prefisso di percorso per le cartelle speciali
	POP		
Nome visualizzato dall'utente	Nome utente visualizzato		
Indirizzo e-mail	Indirizzo e-mail dell'utente		
Consenti lo spostamento	Consentire lo spostamento delle e-mail		
Abilita S/MIME	Abilita la crittografia S/MIME		
Certificato di firma	Carica il rispettivo certificato di firma		
Certificato di crittografia	Carica il rispettivo certificato di crittografia		

Posta in arrivo

Impostazioni del server in entrata

Indirizzo del server di posta	Indirizzo del server di posta
Porta del server di posta	Porta del server di posta
Nome utente	Nome utente rispettivo
Tipo di autenticazione	Tipo di autenticazione
Nessuno	Nessun tipo di autenticazione
Password (solo a livello di dispositivo)	Richiesta di password
Sfida-Risposta MDM	
NTLM	Autenticazione NTLM
Digest MD5 HTTP	
Usa l'SSL	Usa l'SSL, se necessario

Posta in uscita

Impostazioni del server in uscita

Indirizzo del server di posta	Indirizzo del server di posta
Porta del server di posta	Porta del server di posta
Nome utente	Nome utente rispettivo
Tipo di autenticazione	
Nessuno	Nessun metodo di autenticazione
Password (solo a livello di dispositivo)	Richiesta di password
Sfida-Risposta MDM	
NTLM	Autenticazione NTLM
Digest MD5 HTTP	
Usa l'SSL	Usa l'SSL, se necessario
La password in uscita è la stessa di quella in entrata	La password in uscita è la stessa di quella in entrata
Utilizzare solo per la posta	Attiva, se tutte le e-mail in uscita devono essere inviate tramite la Mail-App

CalDav

Configura la configurazione e la distribuzione di un account CalDav

Descrizione dell'account	Nome visualizzato dell'account
Nome host	Nome host e/o indirizzo IP
Porto	Porta dell'account CalDav
URL principale	URL principale dell'account
Nome utente	Nome utente CalDav corrispondente
Password (solo a livello di dispositivo)	La rispettiva password CalDav
Usa l'SSL	Usa l'SSL, se necessario

Calendari sottoscritti

Impostazione e distribuzione dei calendari sottoscritti

Descrizione	Nome visualizzato dell'account
URL	URL del database del calendario
Nome utente	Nome utente dell'abbonamento al calendario
Password (solo a livello di dispositivo)	Password dell'abbonamento al calendario
Usa l'SSL	Usa l'SSL, se necessario

LDAP

In quest'area, imposta una connessione LDAP per consentire lo scambio dinamico di certificati tra il dispositivo dell'utente finale e Active Directory.

Ricorda che l'utente selezionato deve avere i rispettivi permessi di lettura.

Descrizione dell'account	Descrizione dell'account
Nome utente dell'account	Utente per l'accesso a LDAP
Password dell'account	Password per l'accesso a LDAP
Nome host dell'account	Nome host/indirizzo IP del server LDAP
Usa l'SSL	Usa l'SSL, se necessario

Nella seconda parte, puoi definire dei filtri individuali per la ricerca nel registro LDAP.

Descrizione	Ambito di applicazione	Base di ricerca
Descrizione del filtro	Livello di ricerca nel registro LDAP	Definisci il filtro individuale

Gestione del web

Webclips

In questa posizione si definiscono i segnalibri, con link a pagine web, portali intranet ecc. che saranno visibili come applicazione sul dispositivo dell'utente finale.

Etichetta	Nome della connessione sul dispositivo dell'utente finale
URL	Link al rispettivo sito web
Rimovibile	Se attivato, l'utente può rimuovere il webclip
Icona	Tramite questo dialogo, carica un logo per la connessione: Dimensioni 180x180, formato png
Icona Precomposta	Se attivata, non verranno visualizzati effetti aggiuntivi (ombra, riflesso) sull'icona.
Schermo intero	Quando si aprono i webclip, il browser si apre in modalità a schermo intero

Filtro dei contenuti web

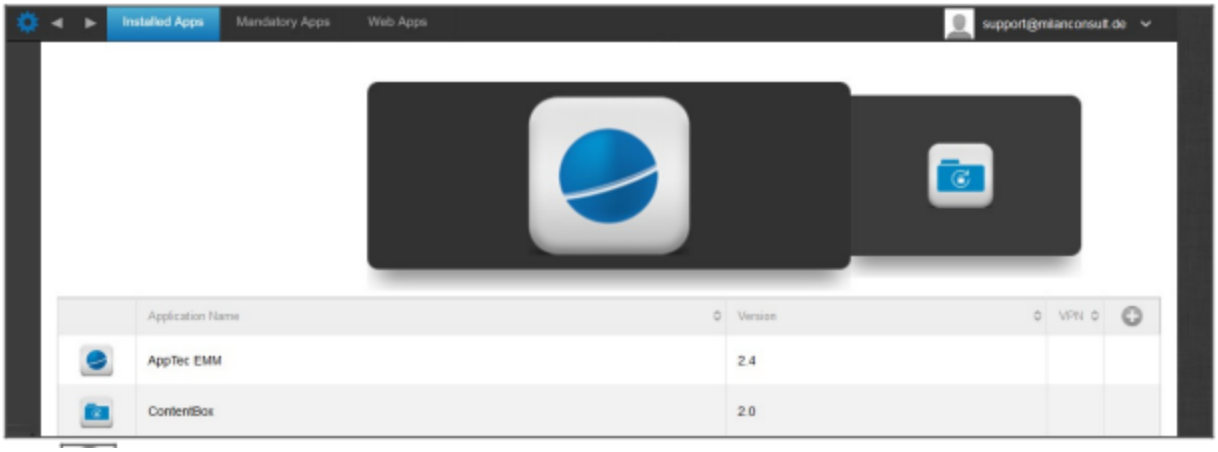
Il filtro dei contenuti web consente di limitare l'accesso a pagine internet specifiche.

Siti web consentiti	
Limita i contenuti per adulti	Il filtro web viene applicato automaticamente per i contenuti per adulti
URL consentiti	Con il simbolo + aggiungi le pagine consentite
URL nella lista nera	Con il simbolo + aggiungi le pagine bloccate
Solo siti web specifici	È possibile visualizzare solo contenuti specifici, che puoi aggiungere con il simbolo +.

Gestione delle app

Enterprise App Manager

Applicazioni installate (solo a livello di dispositivo)



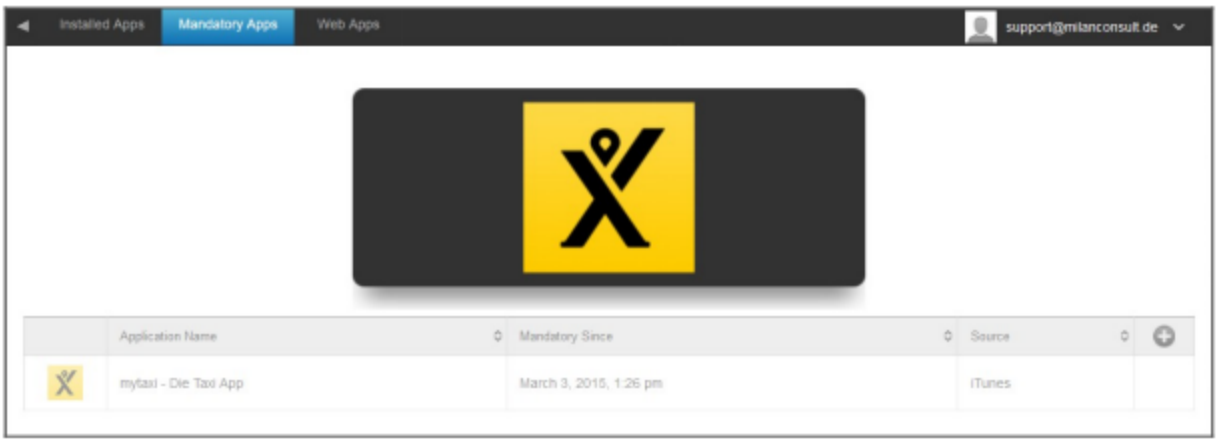
Qui puoi vedere le applicazioni attualmente installate sul dispositivo.

Applicazioni obbligatorie

Sotto la voce Applicazioni obbligatorie, puoi imporre le applicazioni necessarie.

All'utente verrà continuamente ricordato di installare questa applicazione.

Tramite l'opzione , è possibile definire l'App obbligatoria.



Può trattarsi di un'applicazione dell'App Store di Apple, ma anche di un'applicazione interna.

Se si tratta di un dispositivo supervisionato, l'applicazione verrà installata automaticamente.

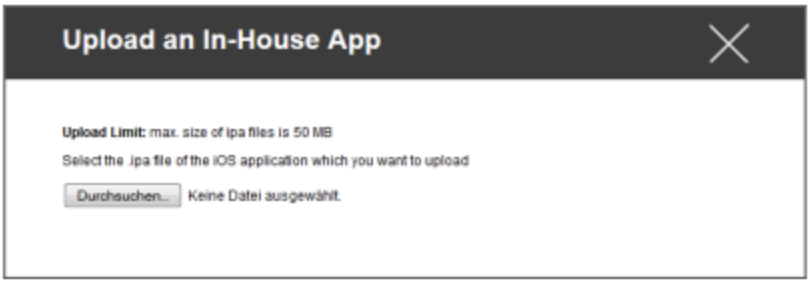
Puoi installare sul dispositivo un'applicazione "Apple AppStore" dall'AppStore pubblico, così come un'applicazione interna sviluppata internamente.

Oppure puoi selezionare la categoria "App in-house iOS" e scegliere un'app in-house che hai caricato nelle Impostazioni generali.

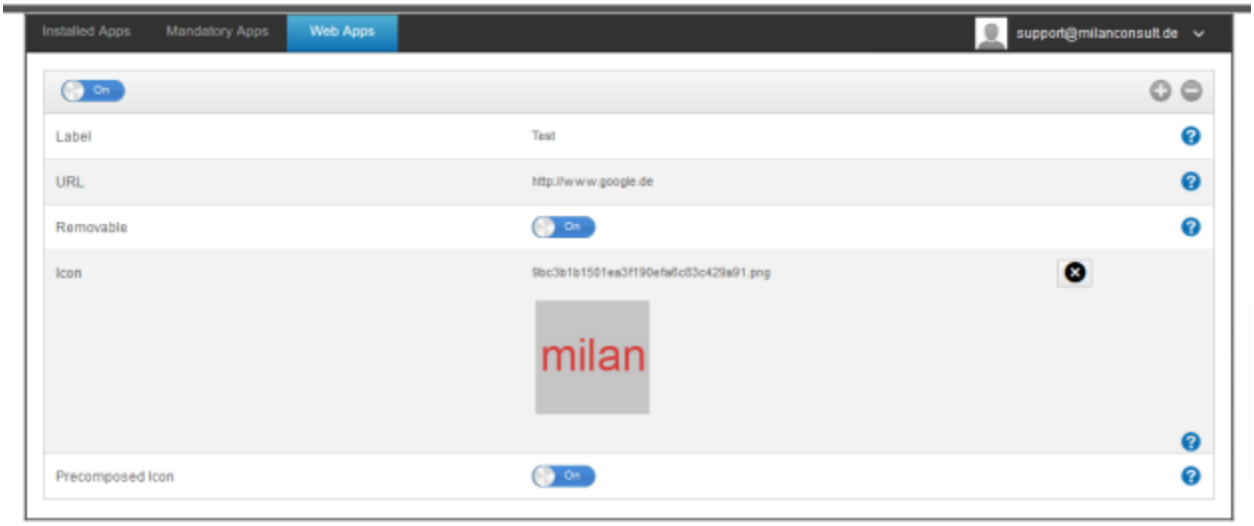
Opzioni di installazione

Mantenere l'aggiornamento (supportato solo per VPP per dispositivo)	Una volta alla settimana, verrà stabilito se c'è un aggiornamento per l'applicazione. Se sì, l'aggiornamento verrà installato Per le applicazioni in-house, il target di aggiornamento configurato nelle Impostazioni generali verrà utilizzato per il processo di aggiornamento.
Superare quando non è gestito	Se l'app è già installata, l'MDM prenderà in carico l'app e la gestirà.
Rimuovi l'app quando il profilo MDM viene rimosso	In caso di rimozione della gestione del dispositivo, l'app verrà disinstallata.
Impedisci il backup dei dati delle app	Non verrà creato un backup dei dati specifici dell'applicazione.
Impostazione dell'app	In "Impostazioni app", puoi assegnare all'app determinati valori in primo piano (a patto che l'app lo supporti, se necessario chiedi allo sviluppatore dell'app).

Puoi anche selezionare e caricare direttamente un file ipa, tramite "Upload In-House App".



Applicazioni web



Sotto il punto "Web Apps", puoi, analogamente a quanto avviene con le "Web Clips", inviare pagine internet o portali intranet come applicazione sul dispositivo dell'utente finale, nell'area della Gestione Web. Come impostazione predefinita, le applicazioni web vengono visualizzate in modalità a schermo intero, che può essere configurata in Webclips.

Etichetta	Nome della connessione sul dispositivo dell'utente finale
URL	Link al rispettivo sito web
Rimovibile	Se attivato, l'utente può rimuovere il Webclip
Icona	Tramite questo dialogo, carica un logo per la connessione: Dimensioni 180x180, formato png
Icona Precomposta	Se attivata, non verranno visualizzati effetti aggiuntivi (ombra, riflesso) sull'icona.

Restrizioni e impostazioni

Applicazioni nella lista nera/bianca

Qui puoi impostare le app che vengono bloccate (o consentite) a seconda delle tue impostazioni in "Impostazioni generali". Facendo clic su di esso, si aprirà la ricerca delle app conosciute. Da qui puoi cercare le app che vuoi aggiungere.

Si noti che per questa funzione è necessario un dispositivo supervisionato.

Restrizioni della SysApp

Blocca applicazioni o funzioni specifiche del tuo dispositivo

Consenti l'uso di YouTube	Consenti l'uso di YouTube
Consenti l'uso di iTunes Store	Consenti l'uso di iTunes Store
Consenti l'uso di Safari	Consenti l'uso di Safari
Abilita l'autofill	Permette il riempimento automatico
Avviso di frode della Forza Armata	Forza l'avviso di frode
Abilita JavScript	Abilita l'uso di JavaScript
Blocca i pop-up	Blocca tutti i tipi di pupazzi
Consenti i cookie	Scegli quando Safari accetterà i cookie

App-VPN

Tramite il simbolo, puoi definire le applicazioni che avvieranno automaticamente la connessione VPN selezionata all'avvio.

Impostazioni dell’app

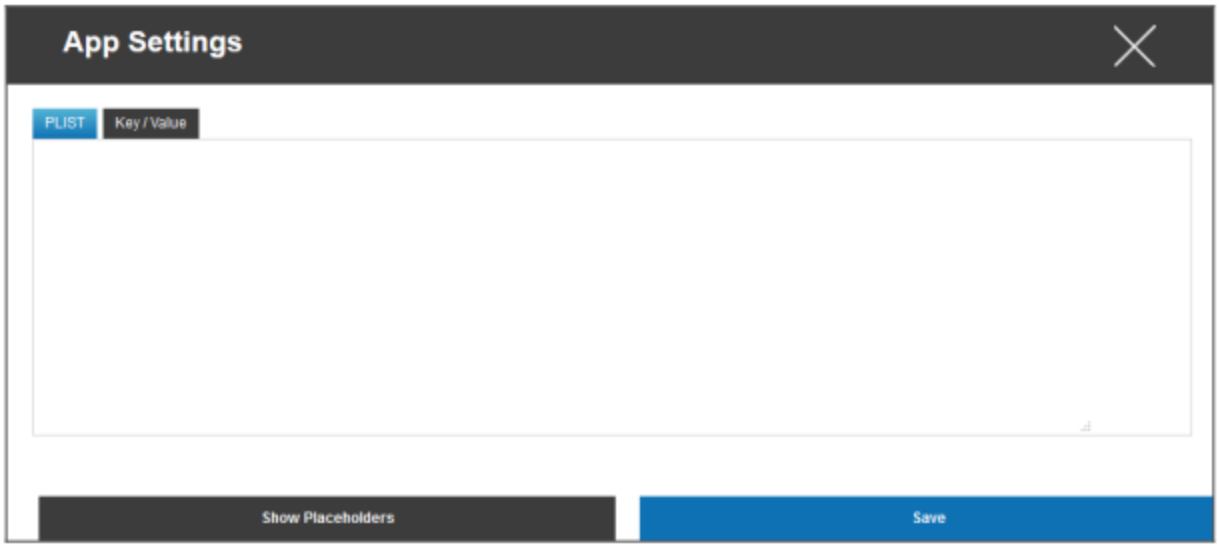
In "Impostazioni app", puoi assegnare all'app determinati valori in primo piano (a patto che l'app lo supporti, se necessario chiedi allo sviluppatore dell'app).

Tramite il simbolo, aggiungi un'applicazione (aggiuntiva). Troverai ancora una volta la familiare rappresentazione di AppTec360 di un'importazione di app.

Cerca qui l'applicazione che desideri configurare e selezionala. Le impostazioni si applicano solo alle app gestite.

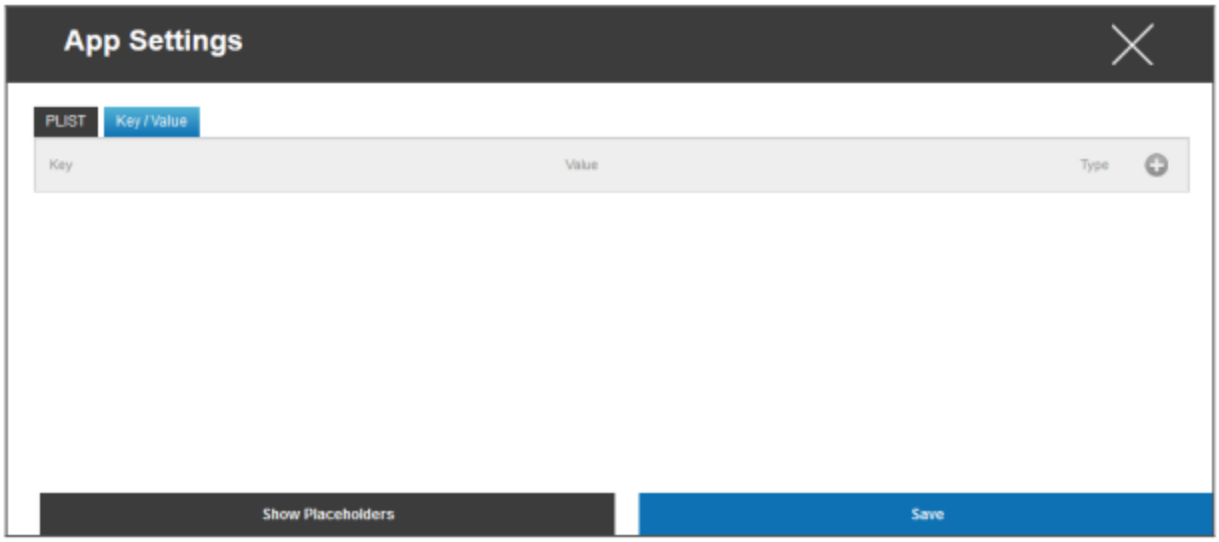
Se l'importazione è andata a buon fine, vedrai la seguente schermata:

Ora, con un clic su , puoi eseguire una serie di configurazioni. Riceverai quindi la seguente panoramica:

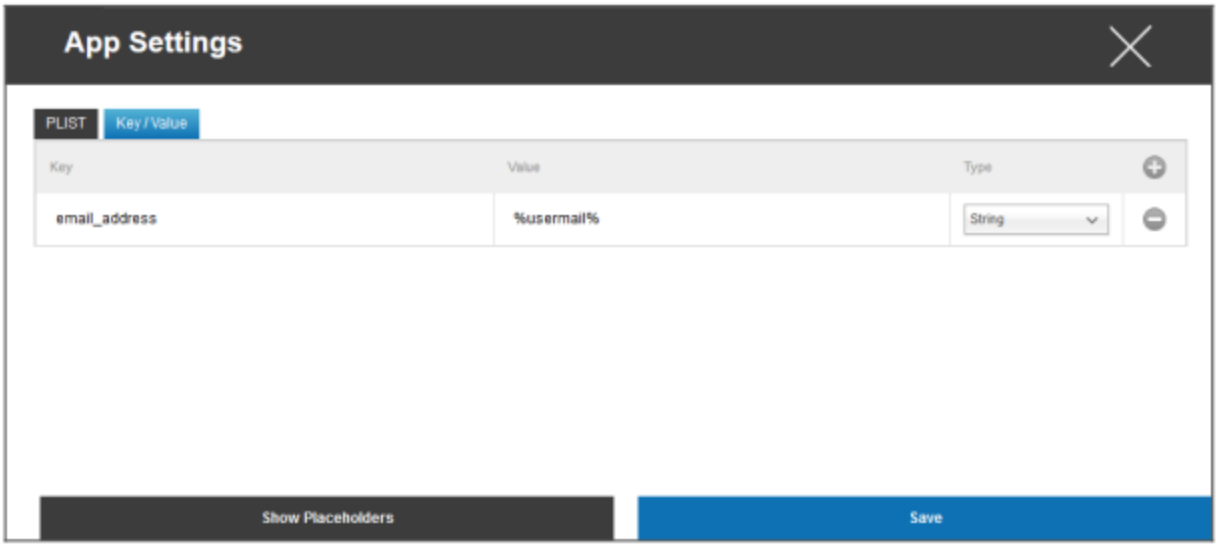


Se hai già una PLIST (testo sorgente della configurazione), puoi aggiungerla qui e salvare il tutto con "Salva".

Sotto la voce "Chiave/Valore", puoi allegare configurazioni specifiche all'App



Qui puoi stabilire una nuova chiave e il suo valore con il simbolo.



Ovviamente, tutti i segnaposto di AppTec sono a tua disposizione

Spiegazione "Tipo":

Stringa	Testo
Booleano	Vero/Falso
Numero	Numero

Con il simbolo puoi rimuovere nuovamente un'applicazione.

App Store aziendale

Applicazioni iTunes

A questo punto, puoi distribuire applicazioni opzionali per il tuo utente.

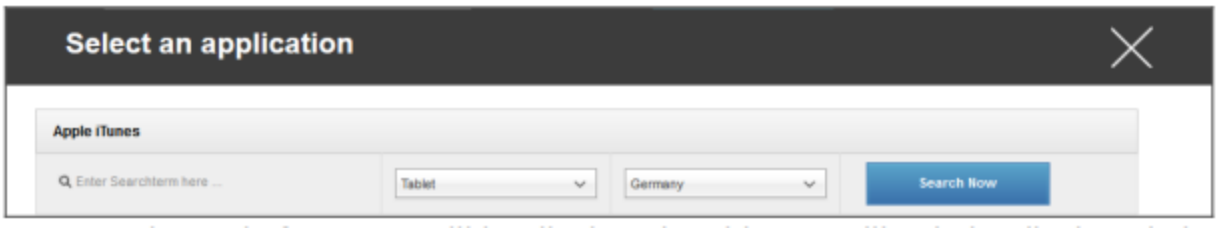
Nel caso in cui sia presente un'app, questa verrà installata automaticamente sul dispositivo dell'utente finale dell'AppTec360 Store.

Si tratta semplicemente di link all'App Store ufficiale di Apple. Per questo motivo, ogni dispositivo dell'utente finale deve essere dotato di un ID Apple.

A questo punto, consigliamo che ogni utente abbia un proprio ID Apple.

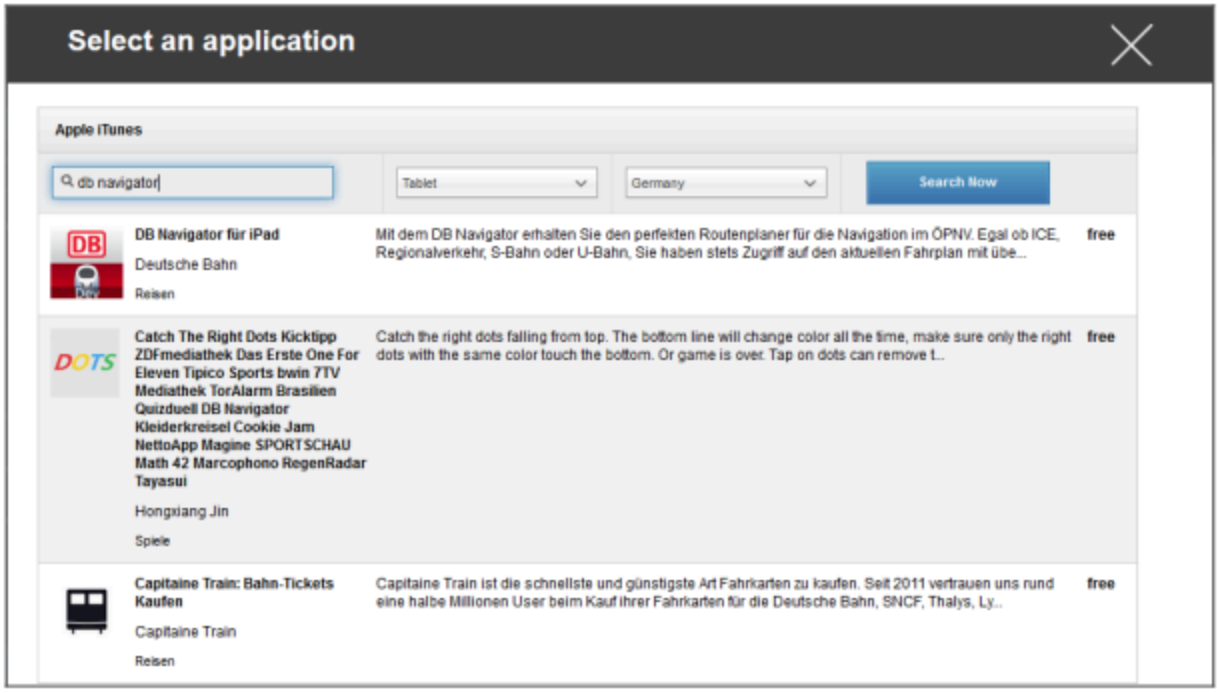
Con il simbolo puoi aggiungere altre applicazioni.

Dopodiché si aprirà una finestra con la seguente panoramica.



Tieni presente che verranno visualizzate solo le app gratuite, mentre quelle a pagamento verranno visualizzate solo tramite VPN.

Alla voce "Inserisci un termine di ricerca qui...", puoi cercare un'applicazione presente nell'App Store di Apple.



Una volta cliccato sull'icona o sul nome dell'applicazione, ti verrà chiesto di eseguire ulteriori configurazioni.

Tieniti aggiornato	Una volta alla settimana, verrà stabilito se c'è un aggiornamento per l'applicazione. Se sì, l'aggiornamento verrà installato
Rimuovi l'app quando il profilo MDM viene rimosso	In caso di rimozione della gestione del dispositivo, l'app verrà disinstallata.
Impedisci il backup dei dati delle app	Non verrà creato un backup dei dati specifici dell'applicazione.
App-VPN	Seleziona una connessione VPN, che verrà avviata all'apertura dell'app.

Dopo aver cliccato su "Installa", l'applicazione verrà aggiunta all'Enterprise App Store e potrà essere installata sul dispositivo dell'utente finale, tramite l'AppStore di AppTec360.

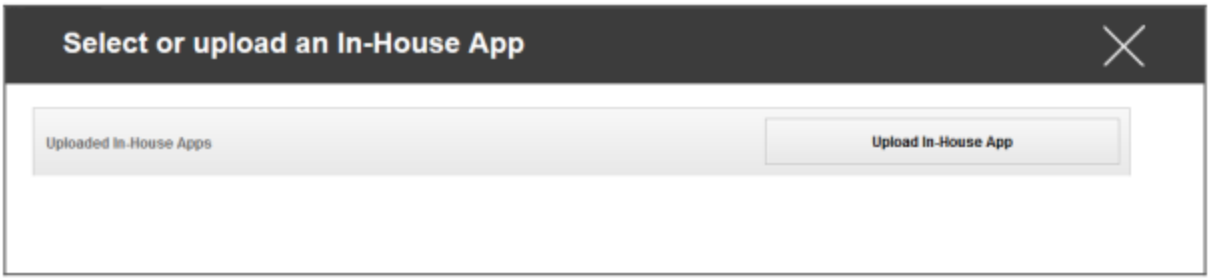
Se l'importazione dell'App-Store è andata a buon fine, riceverai la seguente panoramica:

In-house

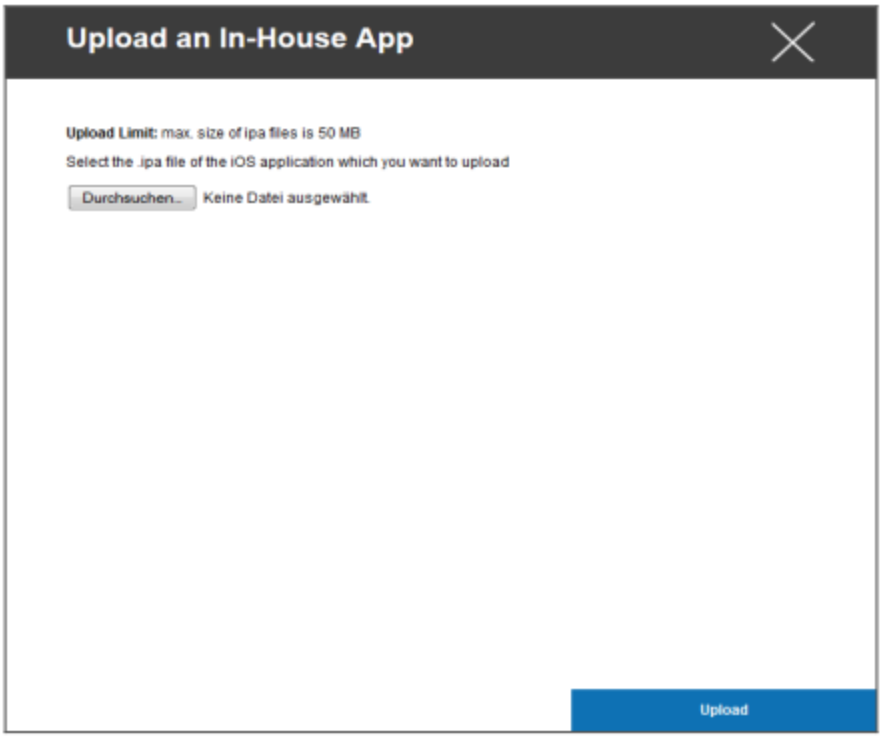
Al punto "In-House", puoi caricare le App sviluppate internamente e distribuirle.

Con il simbolo puoi distribuire altre App In-House.

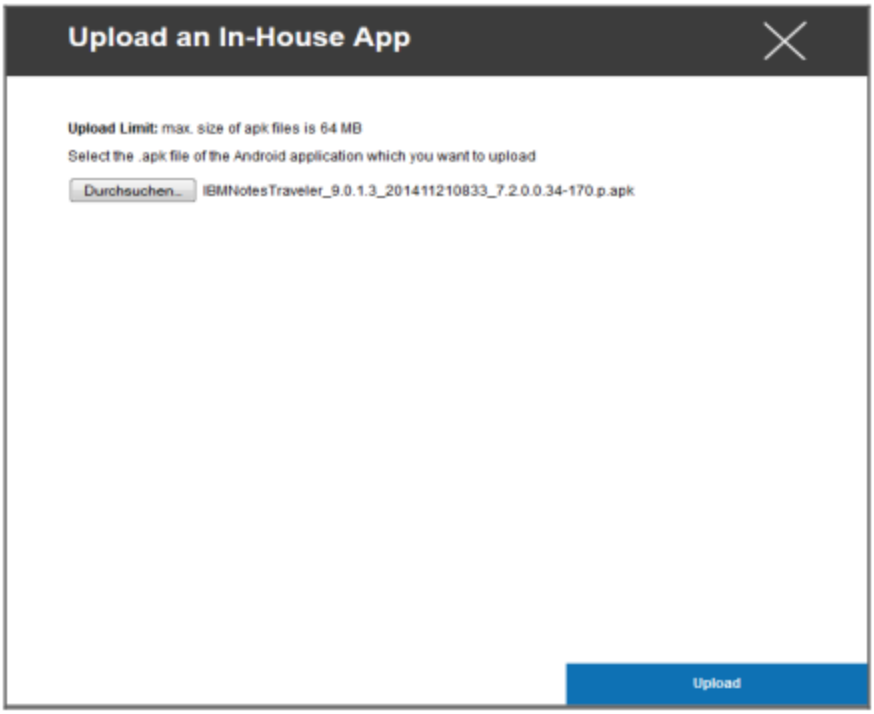
Se non hai mai distribuito App In-House, riceverai la seguente panoramica:



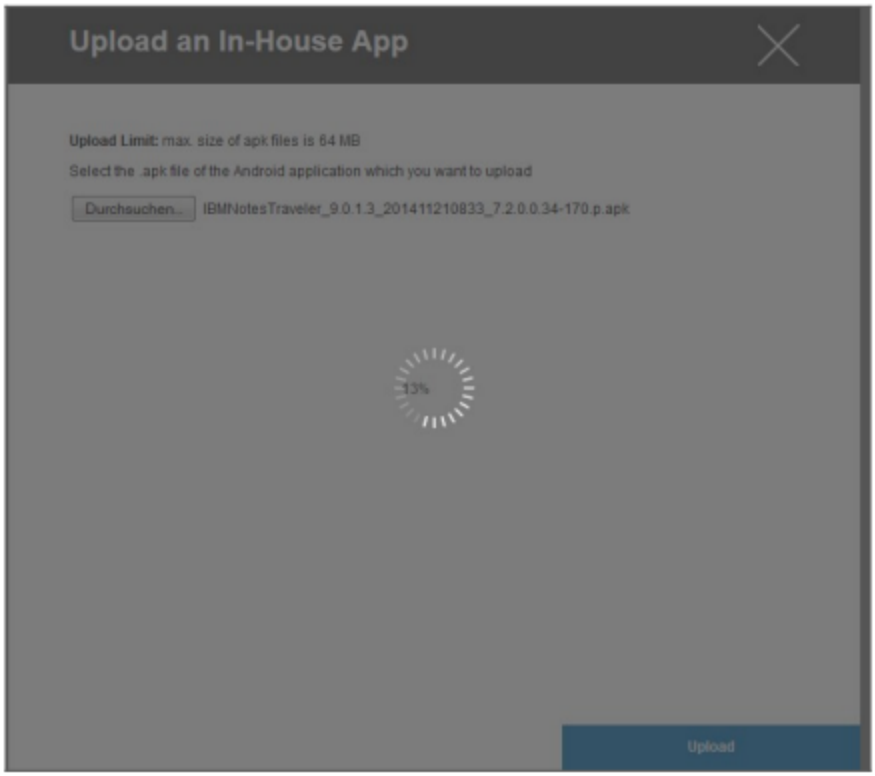
A tal fine, clicca su "Upload In-House App" e riceverai la seguente panoramica:



Ora seleziona con "Cerca..." un file .ipa e poi clicca su "Carica".



La tua App sarà ora caricata. Al centro del cerchio, puoi vedere la percentuale di quanto la tua App è già stata caricata.



Se il caricamento dell'App In-House è andato a buon fine, vedrai l'applicazione appena caricata nel tuo Catalogo delle App.

L'utente ha ora la possibilità di vedere e installare questa applicazione nell'AppTec360 Store sul dispositivo dell'utente finale, sotto la categoria "In-House".

Poiché non si tratta di un'applicazione pubblica dell'AppStore di Apple, l'utente non ha bisogno di un ID Apple memorizzato sul dispositivo dell'utente finale.

Modalità chiosco

La modalità chiosco di iOS è disponibile solo in modalità supervisionata.

La modalità Kiosk ti permette di predefinire un'applicazione o un URL, in modo che sia possibile eseguire/visitare esclusivamente questa applicazione/URL.

Inoltre, puoi disattivare diversi pulsanti hardware nella modalità Kiosk.

Tipo di applicazione

Pacchetto

Se vuoi lanciare l'applicazione in modalità Kiosk, seleziona "Pacchetto" sotto "Tipo di applicazione".

Applicazione chiosco	Clicca qui per selezionare un'applicazione che deve essere avviata in modalità Kiosk. Troverai la panoramica attuale della Gestione delle App Puoi scegliere tra "App Apple iTunes" e "App iOS In-House".

URL

Se vuoi lanciare un URL nella modalità Kiosk, seleziona "URL" alla voce "Tipo di applicazione".

URL	Ora, definisci l'indirizzo URL desiderato
Politica della stessa origine	Se questa funzione è attiva, l'utente può navigare solo nelle sottopagine dell'URL predefinito. Ad esempio, se hai definito il seguente URL: www.mypage.com, allora l'utente potrà navigare su www.mypage.com/subpage
URL inseriti nella whitelist	Qui puoi mantenere una Whitelist, tutti i seguenti URL sono consentiti Massimo 1 URL per riga Un URL deve iniziare con http:/ o https://
URL nella lista nera	Qui è possibile mantenere una Blacklist, tutti questi URL non sono consentiti Massimo 1 URL per riga Un URL deve iniziare con http:/ o https://
Cancella il browser dopo l'inattività	Dopo l'inattività, la cache del browser verrà svuotata.
Password di uscita abilitata	Se attivi questa funzione, l'utente ha la possibilità di terminare la modalità Kiosk con una password predefinita dall'utente.
Password di uscita	Questa è la password che è stata predefinita dall'utente.

Impostazioni della modalità Kiosk

Modalità chiosco programmata	In base all'ora del giorno, puoi impostare la modalità Kiosk, in modo che venga avviata e conclusa automaticamente a un'ora prestabilita.
Ora di inizio	Ora di inizio
Tempo in minuti	Tempo in minuti, dopo il quale la modalità Kiosk deve essere terminata di nuovo.
Disabilita il touch	Se attivato, il touchscreen è disattivato
Disabilita la rotazione del dispositivo	Se attivato, l'adattamento automatico dello schermo è disattivato.
Disattiva l'interruttore della suoneria	Se attivato, l'interruttore della suoneria si disattiva. Da quel momento in poi, il comportamento dipende dalla funzione impostata in precedenza
Disabilita i pulsanti del volume	Se attivato, i pulsanti del volume saranno disattivati.
Disabilita il pulsante di sveglia e riposo	Se attivato, l'interruttore di accensione/spegnimento sarà disattivato.
Disabilita il blocco automatico	Se attivato, il dispositivo non verrà messo in standby.
Abilita il Voice Over	Se attivato, verrà attivato l'assistente vocale.
Abilita lo zoom	Se attivato, lo zoom verrà attivato
Abilita l'inversione dei colori	Se attivata, verrà attivata la modalità di visualizzazione invertita.
Abilita il tocco assistivo	Se attivato, l'AssistiveTouch sarà attivato
Abilita la selezione del parlato	Se attivata, verrà attivata la selezione del parlato
Abilita l'audio mono	Se attivato, l'audio mono sarà attivato
VoiceOver	Se attivato, l'utente può attivare VoiceOver
Zoom	Se attivato, l'utente può abilitare lo Zoom
Invertire i colori	Se attivato, l'utente può attivare i colori invertiti
Tocco Assistibile	Se attivato, l'utente può abilitare il tocco assistivo

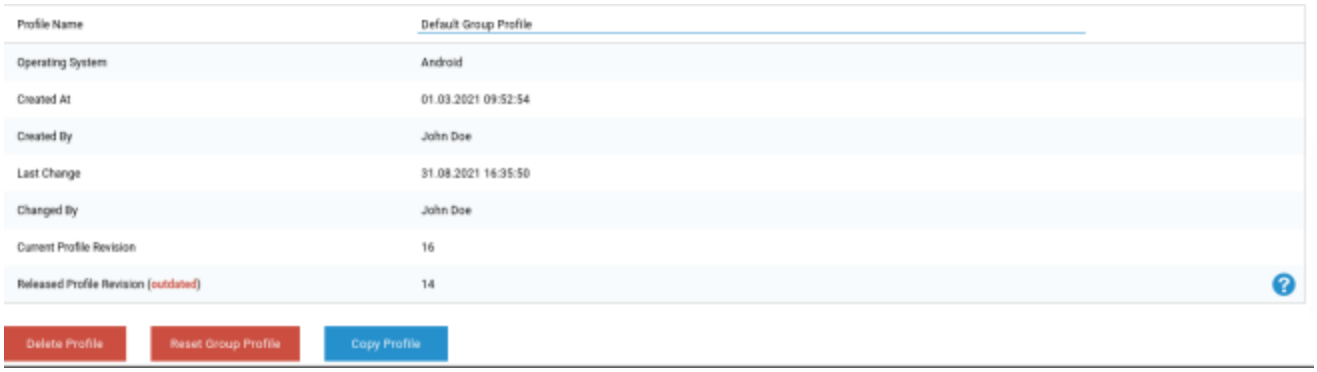
Android Enterprise – Configurazione dei dispositivi completamente gestita

A seconda che tu abbia selezionato un profilo di gruppo o un dispositivo, la panoramica e i suoi punti secondari sono diversi: ti preghiamo di considerare attentamente questo aspetto!

Generale

Panoramica del profilo del gruppo (solo a livello di gruppo)

Quando apri il profilo di un gruppo, otterrai una rapida panoramica del profilo.



Nome del profilo	Nome del profilo (può essere modificato qui)
Sistema operativo	Sistema operativo per cui è stato creato il profilo
Creato a	Tempo della creazione
Creato da	Il creatore del profilo
Ultimo cambiamento	Ora dell'ultima modifica al profilo
Modificato da	Account che ha apportato le ultime modifiche
Revisione del profilo attuale	Revisione dello stato del profilo salvato
Revisione del profilo rilasciata	Revisione del profilo assegnata ("Assegna ora"). Se l'etichetta mostra " (outdated)" dietro il testo, significa che hai salvato il profilo ma non l'hai ancora assegnato, quindi i dispositivi riceveranno ancora la versione più vecchia.

Panoramica del dispositivo (solo a livello di dispositivo)

Se ti trovi su un dispositivo, riceverai un riepilogo del dispositivo selezionato:

Nome del dispositivo	Nome del dispositivo
Posizione	Coordinate della posizione
Numero di telefono	Numero di telefono
Applicazioni obbligatorie assegnate	Numero di applicazioni obbligatorie assegnate
Versione OS	Versione del sistema operativo del dispositivo
Sistema operativo	Sistema operativo (Android Enterprise)
Numero di serie	Numero di serie del dispositivo
Proprietà del dispositivo	Dispositivo aziendale o privato
Tipo di dispositivo	Dispositivo gestito da AE Work
Radicati	Stato, che indica se il dispositivo è stato sottoposto a rooting
Conforme	Conformi alle linee guida
Indirizzo IP	Indirizzo IP del dispositivo
Ultimo visto	Momento in cui il dispositivo si è connesso per l'ultima volta ad AppTec.
Ultima spinta	Momento in cui è stato inviato l'ultimo push al dispositivo.
Modalità proprietario dispositivo AE	Sì
Assegnazione dell'utente	L'utente o il gruppo a cui è assegnato questo dispositivo

Revisione della configurazione (solo a livello di dispositivo)

Qui puoi vedere quale profilo di gruppo è assegnato al dispositivo.

Se clicchi sul profilo del gruppo, avrai accesso diretto a questo profilo e potrai eseguire le impostazioni.

Con questo simbolo puoi riportare le applicazioni distribuite alle impostazioni del profilo del gruppo.

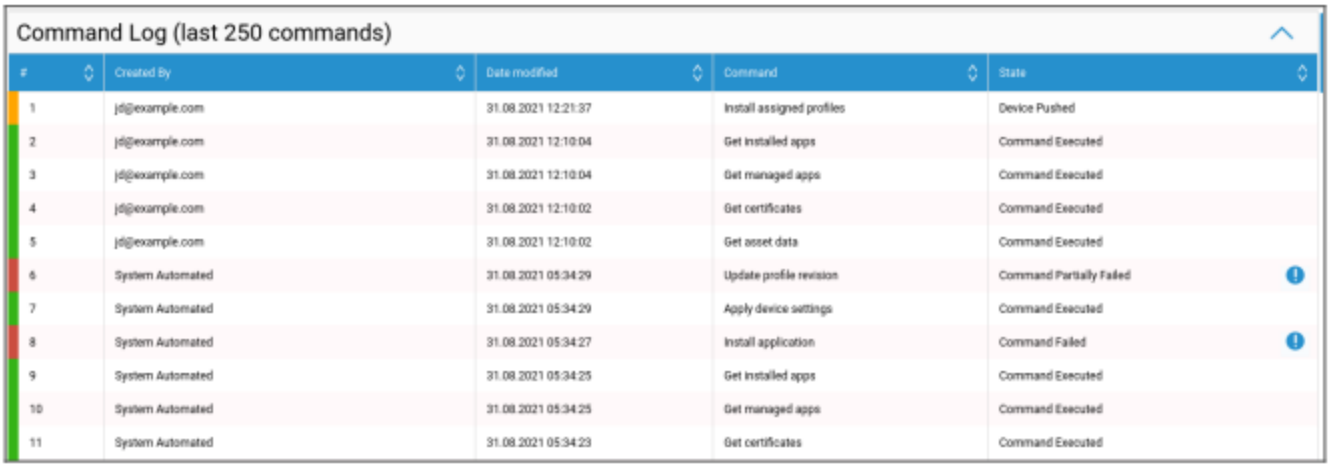
Con questo simbolo puoi riportare tutte le app utilizzate alle impostazioni del profilo del gruppo.

L'indicazione "Revisione più recente disponibile" indica che il profilo del gruppo è stato modificato e salvato ma non assegnato. Il profilo del gruppo deve essere assegnato con "Assegna ora" a livello di gruppo per applicare le modifiche ai dispositivi.

Registro del dispositivo (solo a livello di dispositivo)

Registro dei comandi

Qui puoi vedere quali comandi sono stati emessi per il dispositivo e qual è il loro stato.



I comandi creati da "Sistema automatico" vengono creati automaticamente dal sistema.

Possibili stati del comando

Dispositivo spinto	È stata inviata una richiesta push al servizio push (ad esempio APNS) per indicare al dispositivo di connettersi nuovamente al server EMM.
Comando creato	Il comando è stato creato nel sistema.
Comando inviato	Il comando è stato inviato al dispositivo dopo la connessione al server.
Comando eseguito	Il comando è stato eseguito con successo.
Comando fallito	Il comando è fallito. *
Comando parzialmente fallito	A seconda del sistema operativo del dispositivo, alcuni comandi possono essere raggruppati. In questo caso alcune parti di questo gruppo di comandi sono fallite. *
Comando eseguito, alla fine fallito	Il comando è stato eseguito ma forse non lo è stato.
Comando Riportato	Il comando è stato ripreso da un utente.
Scartato	Il comando è stato scartato. Ad esempio perché è stato sostituito da un altro comando o perché il dispositivo è stato reinserito e i vecchi comandi sono stati rimossi.

Se dietro il messaggio c'è un punto esclamativo, puoi ottenere maggiori informazioni passando il cursore sull'icona.

Impostazioni del dispositivo

Configurazione del cliente

Qui puoi eseguire le seguenti configurazioni sul tuo dispositivo Android:

Tempo di non conformità	Il limite di timeout di risposta dell'utente dopo il quale viene applicata l'azione di applicazione.
Azione esecutiva dopo il timeout di conformità	Azione di controllo quando un utente non esegue azioni che portano a uno stato di conformità del dispositivo.
Frequenza di raccolta dei dati	Frequenza con cui raccogliere le informazioni sul dispositivo/GPS
Frequenza del battito cardiaco del dispositivo	Intervallo di tempo in cui il dispositivo deve contattare il server AppTec360 Min. 1 minuto Max. 24 ore
Abilita gli aggiornamenti della posizione	Se attivato, il dispositivo invia aggiornamenti sulla posizione al server AppTec360.
Posizione Ora di aggiornamento	Determina gli intervalli di tempo in cui il dispositivo invia gli aggiornamenti sulla posizione ad AppTec360.
Usa Google Location Accuracy per l'aggiornamento della posizione	Se attivata, la posizione di rete verrà utilizzata per gli aggiornamenti della posizione (se è stata disattivata in "Restrizioni", questa impostazione non avrà alcun effetto).
Usa la posizione GPS per l'aggiornamento della posizione	Se attivato, il GPS verrà utilizzato per gli aggiornamenti sulla posizione.
Consenti le posizioni fittizie (false)	Consente di falsificare le informazioni sulla posizione tramite applicazioni di terze parti
Azione di perdita della connessione	Se abilitata, puoi specificare un'azione nel caso in cui un dispositivo non si connetta al server MDM nell'intervallo di heartbeat. Ad esempio, se il dispositivo ha un tempo di battito cardiaco di 5 minuti, si connette al server alle 10:35 del mattino. Dopodiché il dispositivo esce dal raggio d'azione del Wi-Fi. Il prossimo battito cardiaco delle 10:40 fallirà e verrà eseguita l'azione specificata.
Azione	L'azione da intraprendere non appena un dispositivo diventa non conforme.

	• Dispositivo di blocco = dispositivo di blocco • Wipe Device = il dispositivo verrà ripristinato alle impostazioni di fabbrica. • Wipe Device & SD Card = il dispositivo verrà ripristinato alle impostazioni di fabbrica e la memoria della scheda SD verrà cancellata.
Soglia	Puoi specificare una soglia di battiti cardiaci non riusciti necessari per attivare l'azione specificata.

Modalità di applicazione dei criteri	Predefinito:	Agli utenti verrà richiesto periodicamente di eseguire le azioni in sospeso.
	Applicazione pigra dei criteri:	Agli utenti non verrà mai richiesto di eseguire azioni in sospeso. Tutte le azioni aperte saranno visualizzate nel client AppTec360
	Applicazione aggressiva dei criteri:	Agli utenti verrà richiesto senza sosta di eseguire le azioni in sospeso.
Blocco della versione di AppTec360	Se abilitato, è possibile specificare un codice di versione per AppTec360 MDM Client. Il client AppTec360 si aggiornerà solo alla versione specificata. Le versioni più recenti saranno ignorate. Non è possibile effettuare un downgrade.	
Codice versione	Codice della versione del client MDM di AppTec360 da bloccare.	
Disattivare la notifica di AppTec360	Se disattivato, il client AppTec360 non mostrerà alcuna notifica nella barra delle notifiche. In questo modo gli utenti possono chiudere il client AppTec360 tramite il task manager. Se il client di AppTec360 è chiuso, diverse funzioni, tra cui la modalità Kiosk e la lista nera/bianca delle app, non funzioneranno correttamente. I dispositivi Samsung offrono un meccanismo di protezione per il client AppTec360. La notifica è disattivata per impostazione predefinita sui dispositivi Samsung che supportano le API KNOX. La notifica non dovrebbe essere disabilitata sui dispositivi con Android 8.0 o superiore.	

Carta da parati

Imposta uno sfondo personalizzato	Abilita/Disabilita lo sfondo personalizzato
Carta da parati	Imposta la modalità di sfondo per utilizzare un codice colore o un'immagine.
Specifica un colore	Specifica un colore di fondo come valore esadecimale, ad esempio #000000 per il nero o #ffffff per il bianco.
Imposta l'immagine come sfondo	Carica il file dell'immagine che vuoi utilizzare come sfondo

Gestione delle risorse (solo a livello di dispositivo)

Info sul dispositivo

Modello	Denominazione del modello del dispositivo
Sistema operativo	OS
Versione OS	Versione del sistema operativo
Numero di serie	Numero di serie
Nome del dispositivo	Nome del dispositivo
Stato della batteria	Stato della batteria
Memoria libera / totale	Memoria libera / Totale
Samsung Safe	Interfaccia Samsung SAFE, necessaria per una serie di opzioni di impostazione
Scheda SD disponibile	Scheda SD disponibile
Scheda SD emulata	Scheda SD emulata
Scheda SD rimovibile	Scheda SD rimovibile
SD Memoria libera / Memoria totale	SD Libera / Memoria totale della scheda SD

Wi-Fi

Indirizzo IP	Indirizzo IP del dispositivo
WiFi MAC	Indirizzo MAC WiFi

Cellulare

Stato	Stato (scheda SIM installata)
Numero di telefono	Numero di telefono
Roaming (voce/dati)	Roaming per voce/dati
Stato del roaming	Stato attuale del roaming
Indirizzo IP	Indirizzo IP
Operatore/Vettore	Operatore/Vettore
Tecnologia cellulare	Tecnologia cellulare
IMEI	Numero IMEI
ICCID	Si tratta dell'ID della carta SIM, spesso anche Smartcard o Carta a Circuito Integrato (ICC).
IMSI	L'International Mobile Subscriber Identity (IMSI) fornisce nelle reti mobili GSM e UMTS un'identificazione precisa degli utenti della rete. L'IMSI è composto da un massimo di 15 cifre e viene configurato nel modo seguente: • Codice paese mobile (MCC), 3 cifre • Codice di rete mobile (MNC), 2 o 3 cifre • Numero di identificazione dell'abbonato mobile (MSIN), da 1 a 10 cifre
Attuale MCC/MNC	Vedere "SIM MCC/MNC"
SIM MCC/MNC	Il codice del paese mobile è un identificativo del paese stabilito dall'ITU secondo la norma E.212. Standard. Questo funziona insieme al Mobile Network Code (MNC) per l'identificazione della rete mobile. Ovvero il codice di rete nazionale/mobile della carta SIM. Se fai il roaming su un'altra rete mobile, logicamente il "Current MCC/MNC" e il "SIM MCC/MNC" saranno diversi.

Bluetooth

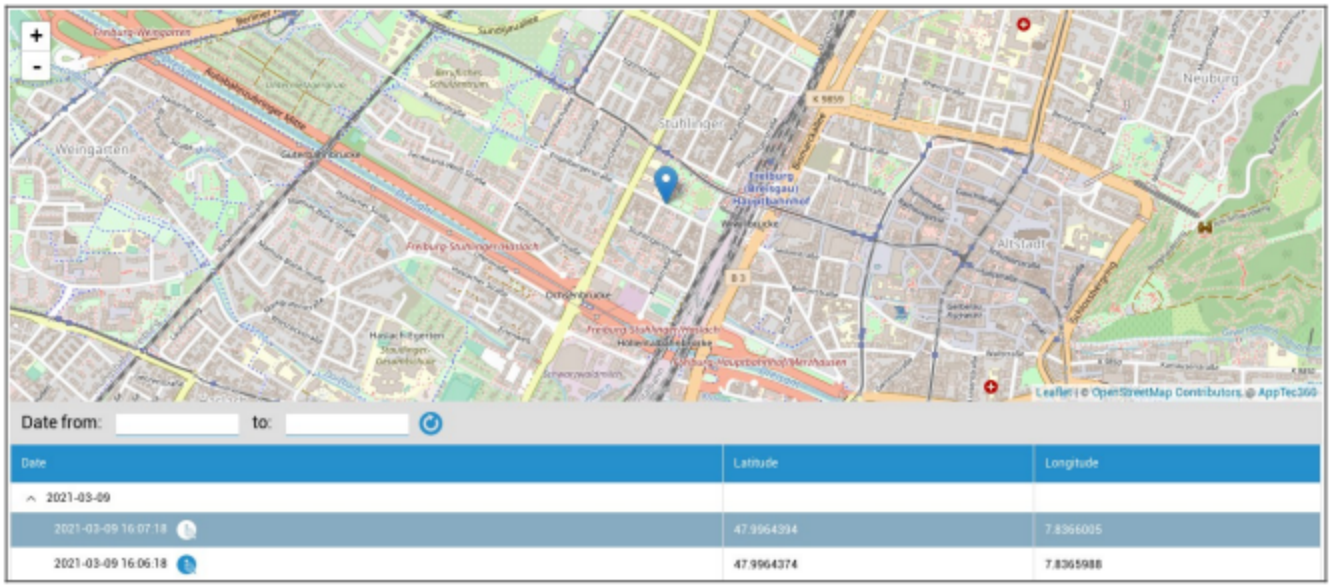
MAC Bluetooth	Indirizzo MAC Bluetooth

Gestione della sicurezza

Antifurto (solo a livello di dispositivo)

Informazioni GPS (solo a livello di dispositivo)

Qui puoi stabilire la posizione attuale/ultima del dispositivo. La localizzazione può essere protetta con una o anche due password - Vedi: Impostazioni generali - Privacy - Accesso GPS



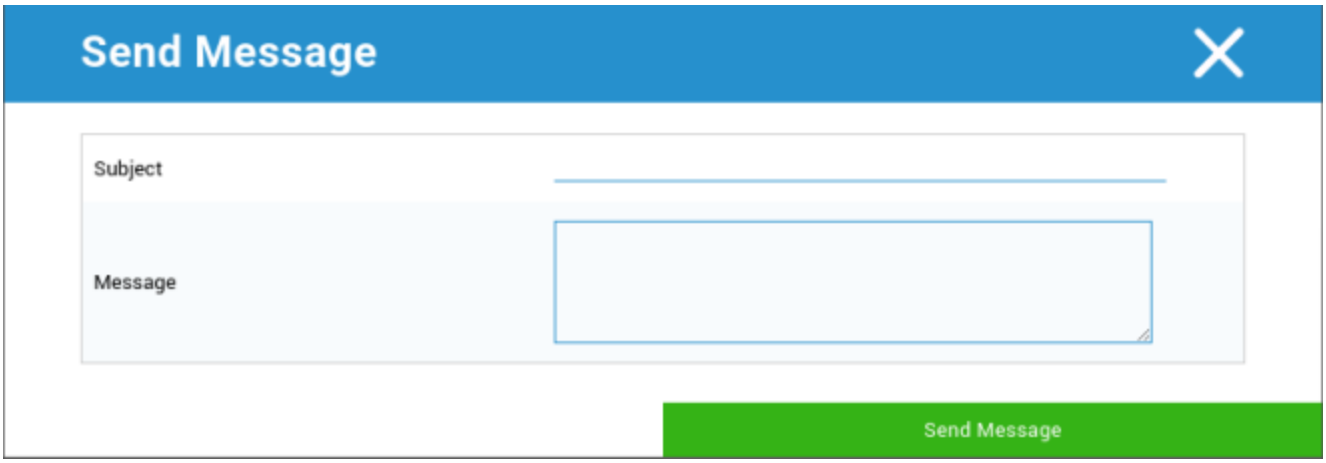
Pulisci e blocca (solo a livello di dispositivo)

Alla voce "Pulisci e blocca", puoi eseguire le seguenti tre azioni:

Pulizia completa	Il dispositivo viene riportato alle impostazioni di fabbrica (i dati aziendali e quelli personali vengono cancellati).
Pulizia aziendale	Solo i dati aziendali vengono rimossi dal dispositivo dell'utente finale (tutte le applicazioni, i dati, ecc. forniti da AppTec360).
Schermata di blocco	Il blocco dello schermo è attivato, è sufficiente sbloccare il dispositivo con la password/PIN del dispositivo.

Messaggio (solo a livello di dispositivo)

Qui puoi inserire l'oggetto e un messaggio e inviarlo a un dispositivo dell'utente finale.



Configurazione della sicurezza

Codice di accesso al dispositivo

Alla voce "Codice di accesso" puoi assegnare una password al dispositivo; sono disponibili le seguenti opzioni di impostazione

Lunghezza minima della password	Stabilisce il numero minimo di simboli che una password deve contenere	
Qualità della password	Non specificato	Questa politica non prevede requisiti per la password.
	Biometrico debole	Questa politica consente una tecnologia di riconoscimento biometrico a bassa sicurezza. Questo implica tecnologie in grado di riconoscere l'identità di un individuo fino a circa un PIN di 3 cifre (il rilevamento di falsi è inferiore a 1 su 1.000).
	Qualcosa	Questo criterio richiede l'impostazione di un qualche tipo di password o modello, ma non applica alcuna regola specifica.
	Alfabetico	L'utente deve aver inserito una password contenente almeno caratteri alfabetici (o altri simboli).
	Alfanumerico	L'utente deve aver inserito una password contenente almeno due caratteri numerici e alfabetici (o altri simboli).
	Complesso	L'utente deve aver inserito una password contenente almeno una lettera, una cifra numerica e un simbolo speciale, per impostazione predefinita. Con questa qualità di password, le password possono essere limitate a contenere vari set di caratteri, come almeno una lettera maiuscola, ecc.
Lunghezza minima della password	Imposta il numero di caratteri richiesto per la password. Ad esempio, puoi richiedere che il PIN o la password abbiano almeno sei caratteri.	
Cifre numeriche minime richieste nella password	Cifre numeriche minime richieste nella password	
Lettere minuscole minime richieste nella password	Lettere minuscole minime richieste nella password	

Lettere maiuscole minime richieste nella password	Lettere maiuscole minime richieste nella password
Caratteri non letterali minimi richiesti nella password	Caratteri non letterali minimi richiesti nella password
Simboli minimi richiesti nella password	Simboli minimi richiesti nella password

Blocco del tempo massimo di inattività	Inattività massima dell'utente fino al blocco temporale
Timeout di scadenza della password	Stabilisce, dopo quale intervallo di tempo la password scade e deve essere emessa una nuova password.
Limitazione della cronologia delle password	Numero di password precedentemente utilizzate che non sono consentite
Massimo di tentativi di password falliti	Stabilisce quante volte una password può essere inserita in modo errato prima che venga eseguita una cancellazione completa del dispositivo.
Consenti l'autenticazione biometrica	Consente l'autenticazione tramite impronta digitale o scansione dell'iride. Solo per Samsung KNOX 2.1 e successivi

AntiVirus

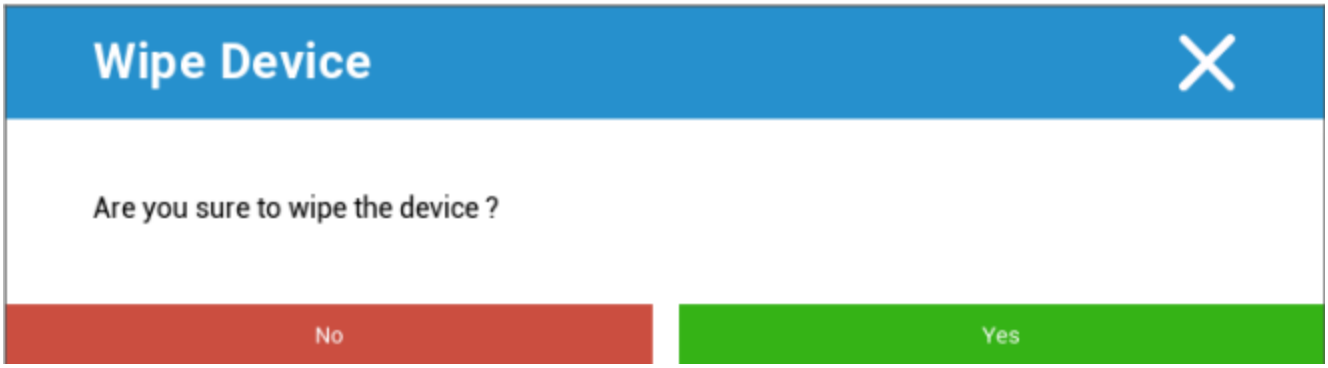
Scansione automatica	Abilita le scansioni automatiche periodiche
Intervallo di scansione	Intervallo per l'esame (Rapido / Completo)
Scansione automatica completa	Abilita le scansioni automatiche complete
Aggiornamenti automatici	Abilita gli aggiornamenti automatici
Intervallo di controllo dell'aggiornamento	Ogni quanto tempo l'app e il suo database devono essere aggiornati (virus/codice danneggiato)
Protezione delle app	Abilita la scansione automatica delle app
Protezione della scheda SD	Abilita la scansione automatica della scheda SD
Aggiornamento solo Wi-Fi	Se abilitato, gli aggiornamenti verranno applicati solo quando il dispositivo è connesso correttamente a una rete Wi-Fi.

Fine vita (solo a livello di dispositivo)

Pulisci (solo a livello di dispositivo)

Alla voce "Wipe", puoi ripristinare le impostazioni di fabbrica del dispositivo. In questo caso i dati aziendali e privati verranno eliminati sul dispositivo dell'utente finale.

Cliccando sul "simbolo del meno" riceverai il seguente messaggio:



Con "Sì" puoi eseguire la pulizia.

In "Wipe Report" possono essere visualizzati i seguenti elementi

Cancellata da	Storia di chi ha eseguito la pulizia
Data	Data
Stato	Stato (ad esempio, se il Wipe è stato eseguito con successo)

Impostazioni di restrizione

Restrizioni

Qui è possibile limitare e bloccare una serie di cose.

Abilita la telecamera	Consenti l'uso della fotocamera	
Forza la sincronizzazione automatica	Su	La sincronizzazione è attivata in modo permanente
	Spento	La sincronizzazione è disattivata in modo permanente
	Scelta dell'utente	Selezionato dall'utente
Forza Bluetooth	Su	Il Bluetooth è attivato in modo permanente
	Spento	Il Bluetooth è disattivato in modo permanente
	Scelta dell'utente	Selezionato dall'utente
Forza GPS	Su	Il GPS è attivato in modo permanente
	Spento	Il GPS è disattivato in modo permanente
	Scelta dell'utente	Selezionato dall'utente
Posizione della rete di forza	Su	Localizzazione permanente su internet
	Spento	Disattivazione permanente della localizzazione su internet
	Scelta dell'utente	Selezionato dall'utente

Sicurezza		
Disconoscimento della posizione della condivisione	Specifica se un utente non può attivare la condivisione della posizione.	
Disabilita l'avvio sicuro	Specifica se l'utente non può riavviare il dispositivo in modalità di avvio sicuro.	
Disabilita il reset della rete	Specifica se un utente non può ripristinare le impostazioni di rete dalle Impostazioni.	
Disabilita il reset di fabbrica	Specifica se un utente non può resettare il dispositivo.	
Abilita ADB	Consente la connessione a un PC tramite ADB	
Disabilita il Keyguard	Disattiva il Keyguard	
Informazioni sulla schermata di blocco del proprietario del dispositivo	Imposta le informazioni sul proprietario del dispositivo da mostrare nella schermata di blocco.	
Applicazione della conformità	Modalità Prompt Utente	All'utente verrà richiesto di eseguire le azioni necessarie.
	Modalità Contenitore di blocco	Nascondere tutte le app fino a quando non vengono soddisfatti tutti i requisiti

Gestione delle app	
Consenti il collegamento tra profili diversi delle app	Permette alle app del profilo padre di gestire i link web del profilo gestito.
Disabilita il controllo delle app	Specifica se un utente non può modificare le applicazioni nelle Impostazioni o nei lanciatori.
Disabilita l'installazione di app	Specifica se un utente non può installare applicazioni.
Disabilita le applicazioni da disinstallare	Specifica se un utente non può disinstallare le applicazioni.
Politica dei permessi di runtime	Specifica come verranno gestite le nuove richieste di autorizzazione da parte delle app.
Consenti fonti sconosciute	Se abilitata, gli utenti possono caricare le applicazioni in modalità sideload installando un file .apk.

Connettività	
Disabilita la configurazione della rete mobile	Specifica se un utente non può configurare le reti mobili.
Configurazione di Disallow Tethering	Specifica se un utente non può configurare il Tethering e gli hotspot portatili.
Disabilita la configurazione VPN	Specifica se un utente non può configurare una VPN.
Disabilita la configurazione Wifi	Specifica se un utente non può cambiare i punti di accesso WiFi.
Disconoscimento del raggio NFC in uscita	Specifica se l'utente non è autorizzato a utilizzare l'NFC per trasmettere dati dalle app.
Blocca la configurazione WiFi	Questa impostazione controlla se le configurazioni WiFi create da un'app Proprietario del dispositivo devono essere bloccate (cioè modificabili o rimovibili solo dall'app Proprietario del dispositivo, non anche dall'app Impostazioni).
Abilita il roaming dati	Attiva il roaming dati

Bluetooth	
Disabilita il Bluetooth	Specifica se il bluetooth non è consentito sul dispositivo. Richiede Android 8.0
Disabilita la condivisione Bluetooth	Specifica se la condivisione bluetooth in uscita non è consentita sul dispositivo. Richiede Android 8.0
Disabilita la configurazione Bluetooth	Specifica se un utente non può configurare il bluetooth.

Gestione degli account	
Disabilita l'aggiunta di un profilo gestito	Specifica se un utente non può aggiungere profili gestiti. Richiede Android 8.0
Disabilita l'aggiunta di utenti	Specifica se un utente non può aggiungere nuovi utenti.
Disallow Rimuovi il profilo gestito	Specifica se i profili gestiti di questo utente possono essere rimossi, se non dal proprietario del profilo. Richiede Android 8.0
Disconoscimento della modifica dell'account	Specifica se un utente non può aggiungere e rimuovere account, a meno che non siano aggiunti programmaticamente da Authenticator.

Telefonia	
Disabilita le chiamate in uscita	Specifica che l'utente non può effettuare chiamate in uscita.
Disabilita gli SMS	Specifica che l'utente non è autorizzato a inviare o ricevere messaggi SMS.

Sistema	
Disabilita la creazione di finestre	Specifica che le finestre diverse da quelle dell'applicazione non devono essere create.
Disabilita l'impostazione dell'icona Utente	Specifica se un utente non può cambiare la propria icona.
Disallow Set Wallpaper	Limitazione dell'utente per impedire l'impostazione di uno sfondo.
Disabilita la barra di stato	La disabilitazione della barra di stato blocca le notifiche, le impostazioni rapide e altre sovrapposizioni dello schermo che permettono di uscire da un dispositivo monouso.
Abilita il tempo automatico	Imposta l'ora automaticamente.
Abilita il fuso orario automatico	Imposta automaticamente il fuso orario.
Rimane acceso quando è collegato alla rete	Il dispositivo rimarrà attivo mentre è collegato a una fonte di alimentazione.

Immagazzinamento	
Disabilita la verifica delle app	Specifica se un utente non può disabilitare la verifica delle applicazioni.
Disallow Mount Physical Media	Specifica se un utente non può montare supporti fisici esterni.
Abilita il servizio di backup	Il servizio di backup gestisce tutti i meccanismi di backup e ripristino sul dispositivo. Impostando questo valore a false si impedisce il backup o il ripristino dei dati. Il servizio di backup è disattivato per impostazione predefinita. Richiede Android 8.0
Abilita l'archiviazione di massa USB	Abilita l'utilizzo della memoria di massa USB.

Tastiera	
Disabilita il riempimento automatico	Specifica se un utente non è autorizzato a utilizzare i servizi di riempimento automatico. Richiede Android 8.0
Disabilita il copia e incolla tra i profili	Specifica se ciò che viene copiato negli appunti di questo profilo può essere incollato nei profili correlati.

Suono	
Disconoscimento dell'adeguamento del volume	Specifica se un utente non può regolare il volume master.
Disabilita il microfono	Specifica se un utente non può regolare il volume del microfono.
Dispositivo Mute	Dispositivo di silenziamento.

Gestione dei certificati

Qui puoi distribuire Certificati di fiducia e Certificati di identità ai tuoi dispositivi.

Android 8 o superiore è necessario per distribuire Certificati di fiducia e Android 9 o superiore per distribuire Certificati di identità.

Con il "+" puoi aggiungere più certificati.

I certificati di fiducia devono essere in formato PEM.

I certificati di identità devono essere in formato PKCS12.

Gestione delle connessioni

Wifi

Per questa impostazione, esegui la preconfigurazione dei dispositivi dell'utente finale, per l'accesso all'Accesso interno
Punti

Identificatore del set di servizi (SSID)	SSID per la rete da collegare
Rete nascosta	Attiva, nel caso in cui l'AP non trasmetta il SSID

Tipo di sicurezza

Stabilire il tipo di sicurezza dell'AP

WEP

Password	Password per l'AP

WPA/WPA2

Password	Password per l'AP

802.1x EAP

Metodo EAP

PWD	Identità	Identità
	Password	Password

PEAP	Protocollo di autenticazione di fase 2	nessuno	Nessun protocollo aggiuntivo
		MSCHAPV2	Protocollo MSCHAPV2
		GTC	Protocollo GTC
	Certificato CA	Certificato CA	
	Identità	Identità	
	Identità anonima	Identità anonima	
	Password	Password	

TTLS	Protocollo di autenticazione di fase 2	nessuno	Nessun protocollo aggiuntivo
		PAP	Protocollo PAP
		MSCHAP	Protocollo MSCHAP
		MSCHAPV2	Protocollo MSCHAPV2
		GTC	Protocollo GTC
	Certificato CA	Certificato CA	
	Identità	Identità	
	Identità anonima	Identità anonima	
	Password	Password	

TLS	Certificato CA	Certificato CA
	Identità	Identità
	Password	Password

VPN

Nome della connessione	Nome della connessione VPN

Tipo di VPN

VPN

Client VPN

Cliente VPN AppTec360	
Configurazione del gateway	Seleziona la configurazione del Gateway VPN (vedi **Impostazioni generali > Gateway universale > Impostazioni VPN**).
VPN sempre attiva	Abilita il blocco nativo
Abilita il blocco di AppTec360	Abilita il blocco di AppTec360

Integrato (disponibile solo sui dispositivi Samsung)			
Tipo di connessione	PPTP	Server	Server
		Abilita la crittografia PPTP	Abilita la crittografia PPTP
	L2TP / IPSec PSK	Server	Server
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Abilita il segreto L2TP	Abilita il segreto L2TP
		Segreto L2TP	Segreto L2TP
	IPSec XAuth PSK	Server	Server
		Identificatore IPSec	Identificatore IPSec
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
Ricerca DNS Domini	Ricerca DNS Domini		
Impostazioni dell'esperto	Server DNS	Server DNS	
	Percorsi di inoltro	Percorsi di inoltro	

Aprire una VPN		
Server	Server	
Profilo OpenVPN	Profilo OpenVPN	
App OpenVPN	OpenVPN per Android (consigliato)	
	Connetti OpenVPN	
Impostazioni dell'esperto	Server DNS	Server DNS
	Percorsi di inoltro	Percorsi di inoltro

Samsung / Cigno forte			
Tipo di connessione	PPTP	Server	Server
		Nome utente	Nome utente
		Password	Password
		Abilita la crittografia PPTP	Abilita la crittografia PPTP
	L2TP / IPSec PSK	Server	Server
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
		Abilita il segreto L2TP	Segreto L2TP
	IPSec XAuth PSK	Server	Server
		Identificatore IPSec	Identificatore IPSec
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
Impostazioni dell'esperto	Server DNS	Server DNS	
	Percorsi di inoltro	Percorsi di inoltro	

Cisco Any Connect		
Server	Server	
Modalità certificato	Disabili	Disabili
	Automatico	Automatico
Impostazioni dell'esperto	Server DNS	Server DNS
	Percorsi di inoltro	Percorsi di inoltro

VPN per app

Client VPN

Cliente VPN AppTec360		
Configurazione del gateway	Seleziona la configurazione del Gateway VPN (vedi **Impostazioni generali > Gateway universale > Impostazioni VPN**).	
Applicazioni VPN	Applicazioni VPN	
VPN sempre attiva	Abilita il blocco nativo	VPN sempre attiva
Abilita il blocco di AppTec360	Abilita il blocco di AppTec360	

Samsung / Cigno forte			
Tipo di connessione	PPTP	Server	Server
		Applicazioni VPN	Applicazioni VPN
		Nome utente	Nome utente
		Password	Password
		Abilita la crittografia PPTP	Abilita la crittografia PPTP
	L2TP / IPSec PSK	Server	Server
		Applicazioni VPN	Applicazioni VPN
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
		Abilita il segreto L2TP	Segreto L2TP
	IPSec XAuth PSK	Server	Server
		Applicazioni VPN	Applicazioni VPN
		Identificatore IPSec	Identificatore IPSec
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
Impostazioni dell'esperto	Server DNS	Server DNS	
	Percorsi di inoltro	Percorsi di inoltro	

Restrizioni

Qui puoi impostare le restrizioni relative alla gestione delle connessioni.

Consenti il roaming dei dati	Consenti i dati mobili in roaming
Forza il roaming dei dati	Se attivato, il roaming per i dati mobili viene attivato in modo permanente (non è consigliato!). Questa impostazione sovrascrive l'impostazione "Consenti roaming dati"!
Le seguenti impostazioni sono disponibili solo su SAFE 2.x o superiore	
Consenti solo le chiamate di emergenza	Consenti solo le chiamate di emergenza
Consenti il WiFi	Consenti il WiFi
Livello minimo di sicurezza della rete WiFi	Livello minimo di sicurezza della rete WiFi Aperto = sono ammessi tutti i tipi di WiFi
Impedisci all'utente di aggiungere reti WiFi	L'utente non può aggiungere una rete WiFi da solo Questa impostazione è possibile solo se è stato definito un profilo WiFi in "Gestione connessioni".
Consenti SMS e MMS	Tutti = Tutto il traffico di SMS e MMS è consentito Solo SMS in entrata = Sono consentiti solo gli SMS in entrata. Solo SMS in uscita = Sono consentiti solo gli SMS in uscita. Nessuno = Non è consentito il traffico di SMS/MMS.
Consenti la sincronizzazione durante il roaming	Consenti la sincronizzazione durante il roaming On = attivato Off = disattivato Scelta dell'utente = scelta dell'utente
Consenti il roaming vocale	Consenti il roaming vocale On = attivato Off = disattivato Scelta dell'utente = scelta dell'utente
Usa il server proxy http del sistema	L'utilizzo di un server proxy HTTP, fornito dalle impostazioni del sistema nelle impostazioni, dipende dalla rete connessa (WiFi o APN).

Gestione del PIM

Scambio Gmail

Info: Questa configurazione verrà applicata all'applicazione Gmail. Quindi devi approvare e installare Gmail.

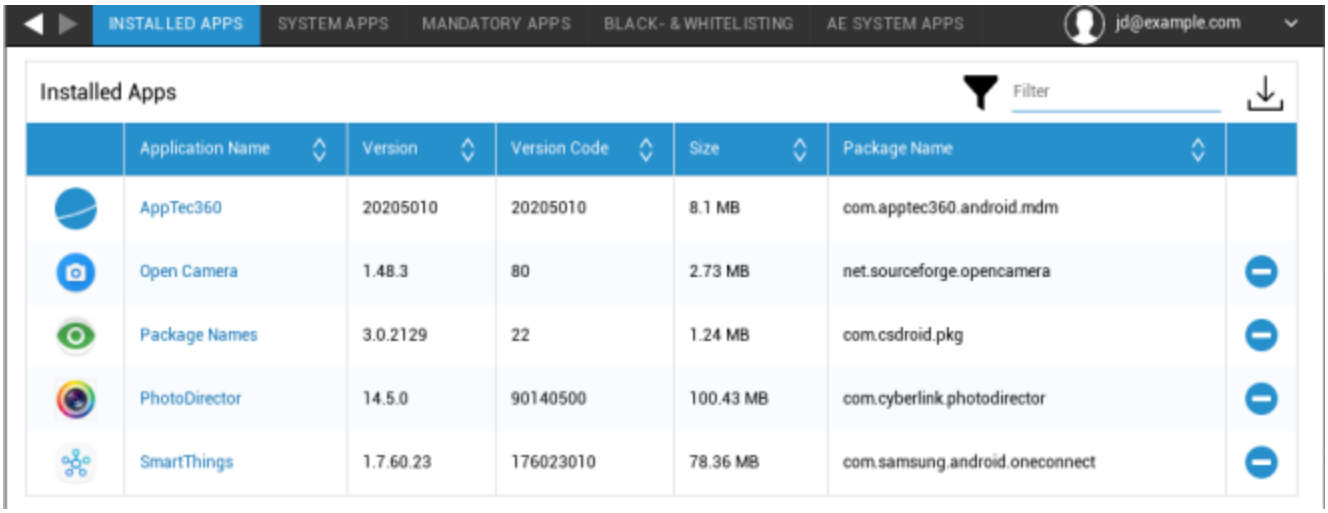
Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Con un clic potrai visualizzarle tu stesso
Nome host del server	Indirizzo del server di Exchange
Nome utente	Il nome di accesso per il rispettivo dispositivo dell'utente finale, si prega di notare anche i "Segnaposto qui".
Firma	È possibile allegare una firma (Suggerimento: alcuni dispositivi richiedono la formattazione HTML per la firma).
Numero di giorni precedenti da sincronizzare	Numero di giorni che determinano il momento in cui le email vengono sincronizzate di nuovo
Identificatore del dispositivo	Una stringa che contiene l'EAS DeviceID. Questo è un elemento del protocollo EAS e deve essere utilizzato in alcuni paesi.
Utilizza il Secure Sockets Layer (SSL)	Usa una connessione SSL
Accetta tutti i certificati	Sono accettati tutti i certificati. Seleziona questa opzione se il tuo Exchange Server utilizza un certificato autofirmato.

Gestione delle app

Enterprise App Manager

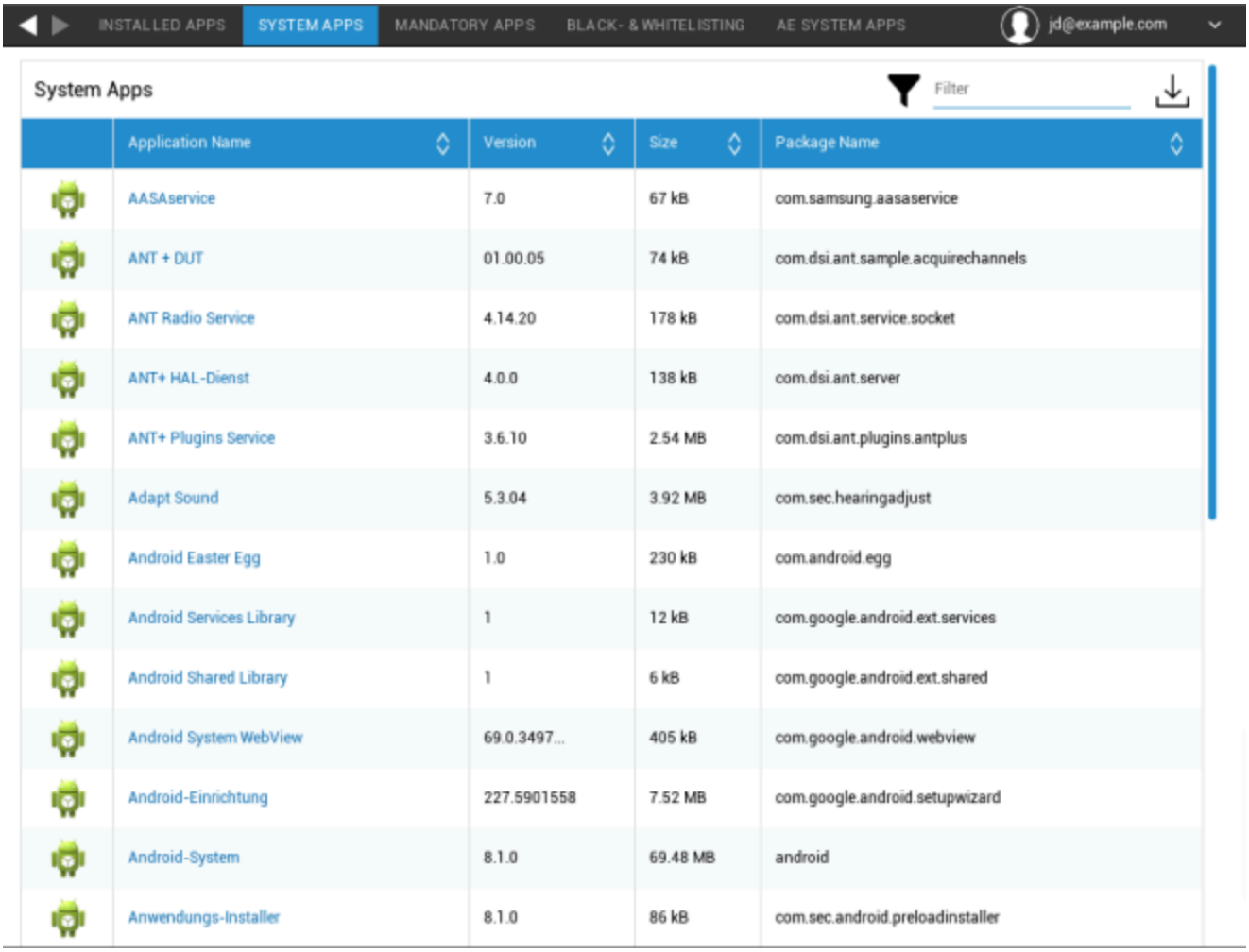
Applicazioni installate (solo a livello di dispositivo)

Qui verranno visualizzate tutte le app attualmente installate sul dispositivo dell'utente finale.



App di sistema (solo a livello di dispositivo)

Sotto la voce "App di sistema" sono elencate tutte le applicazioni e i servizi che sono già stati installati sul dispositivo dell'utente finale dal produttore del dispositivo.

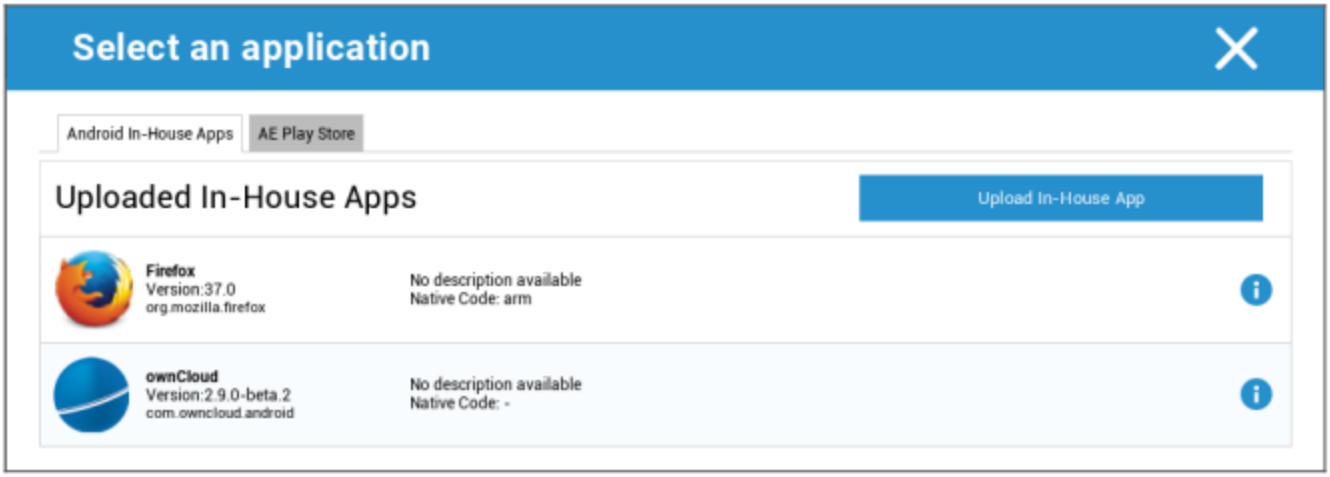


Applicazioni obbligatorie

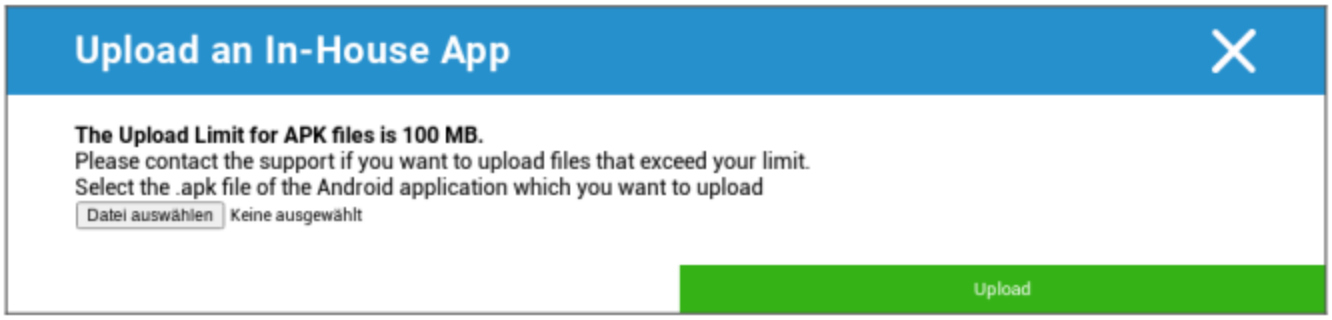
Nella sezione Applicazioni obbligatorie, puoi stabilire le applicazioni obbligatorie. All'utente verrà continuamente richiesto di installare l'applicazione designata.

Tramite l'opzione , è possibile definire l'applicazione obbligatoria.

Può trattarsi di un'applicazione interna tra le "Applicazioni interne Android" che hai caricato nelle Impostazioni generali.

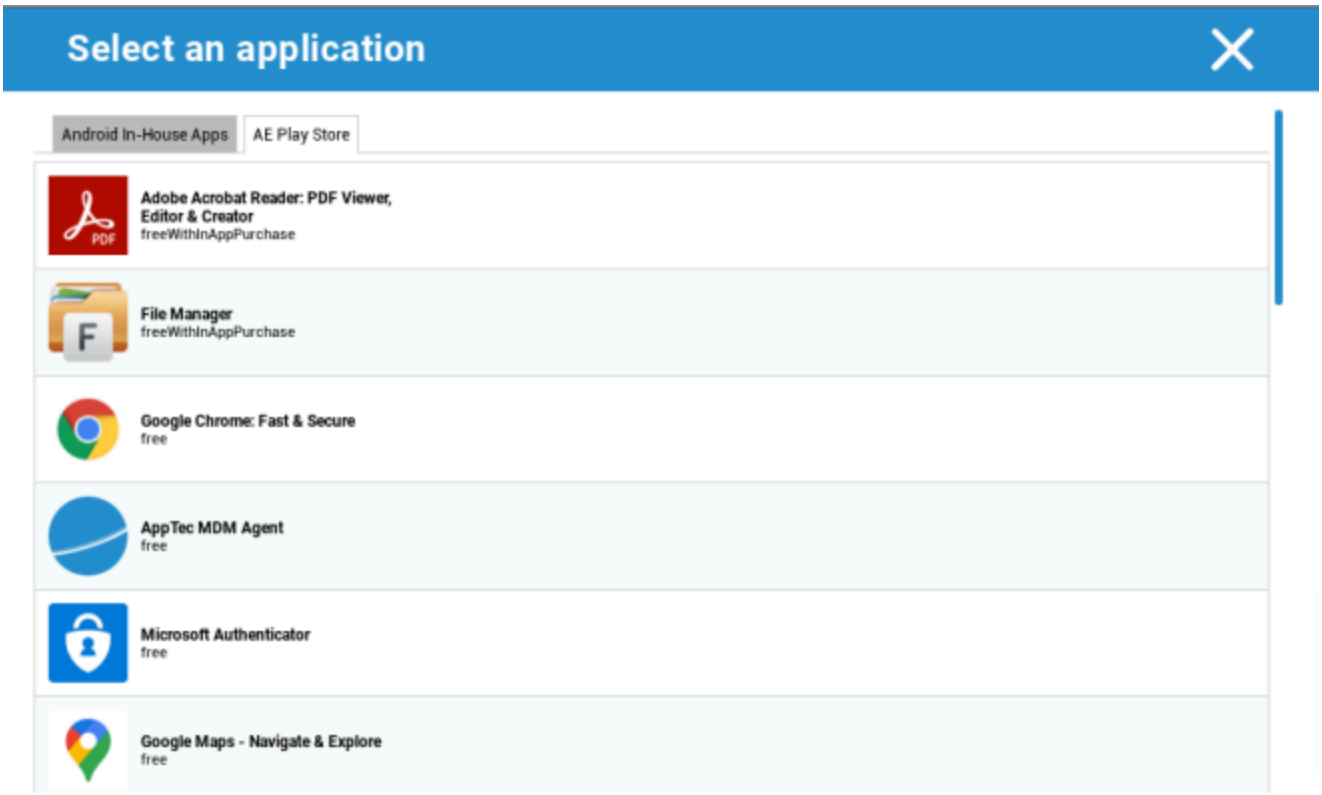


Puoi anche selezionare e caricare direttamente un file apk con "Upload In-House App".



Se stai installando un'App In-House, avrai la possibilità di attivare la funzione "Tieni aggiornato". Se l'opzione è attivata e hai definito una versione più recente nel DB delle app in-house, l'app verrà aggiornata sul dispositivo.

Oppure può essere un'applicazione "AE Play Store" dal Google Work Play Store.



In questa scheda verranno visualizzate solo le "App AE Play Store" approvate.

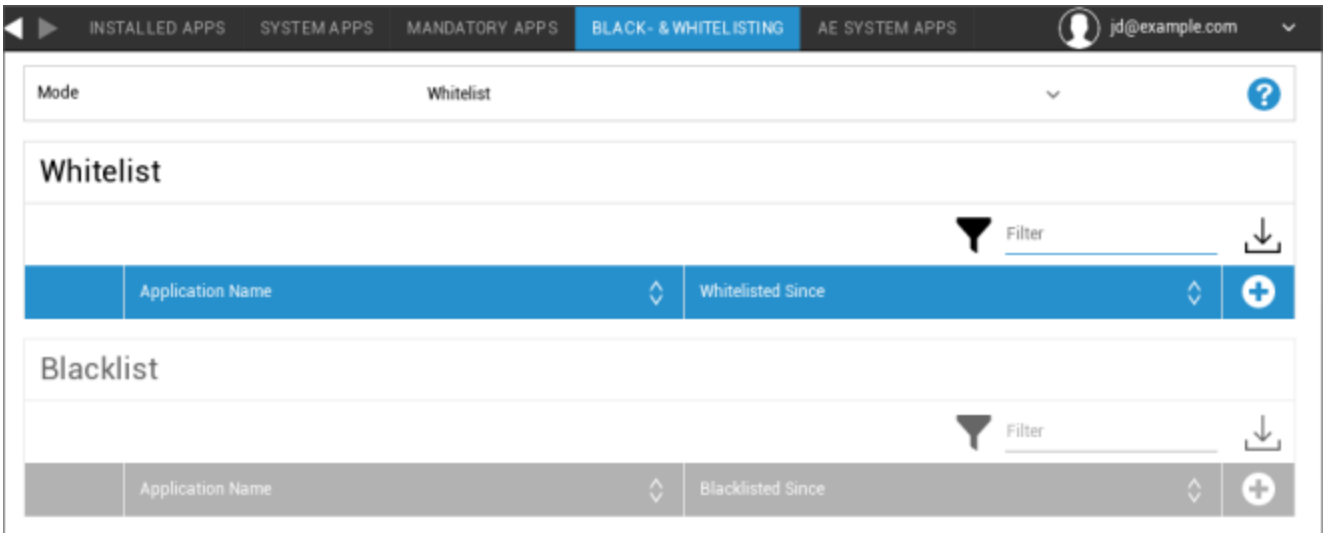
Per approvare un'applicazione "AE Play Store" vai in "Impostazioni generali" > "Gestione app" > "AE Play

Store" e aggiungi un'applicazione tramite il pulsante che ti reindirizzerà alla scheda "Applicazioni del Play Store" (oppure puoi
può andare direttamente alla scheda "App del Play Store").

Nella scheda "Play Store Apps" puoi cercare le applicazioni. Quando clicchi su un'applicazione, si apre la pagina dell'applicazione.
e qui puoi approvare l'applicazione cliccando su "Approva".

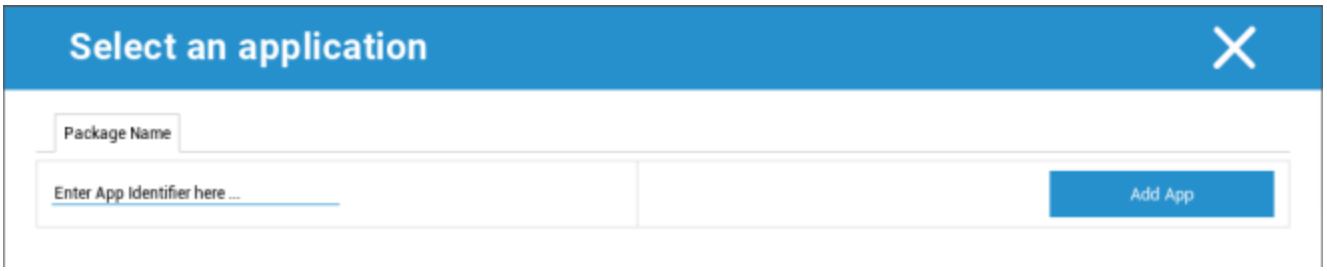
Black- e Whitelisting

In "Black- & Whitelisting", puoi scegliere tra la modalità "Whitelist" e la modalità "Blacklist".



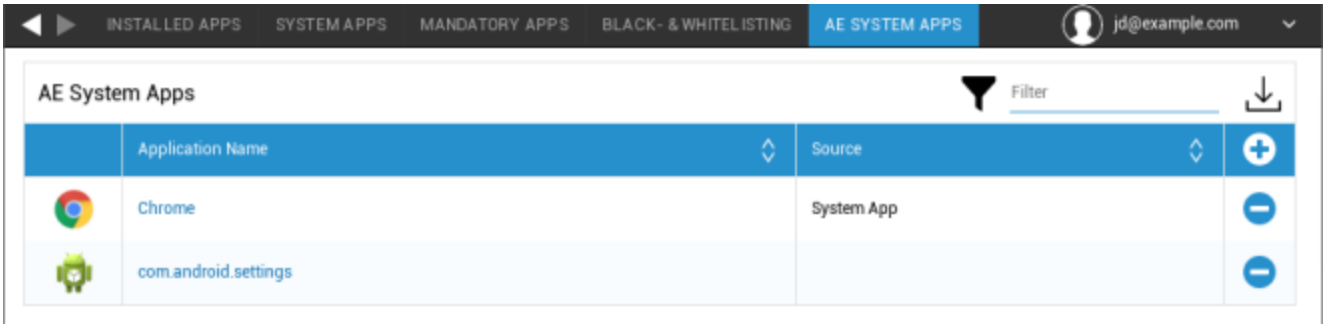
Whitelist	Solo le app e i servizi aggiunti all'elenco possono essere installati sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno attivati e impostati in modo che l'utente possa eseguirli.
	Tutte le altre app non aggiunte all'elenco non possono essere installate sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno disattivati e impostati in modo che l'utente non possa eseguirli.
Lista nera	Le app e i servizi aggiunti all'elenco non possono essere installati sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno disattivati e impostati in modo che l'utente non possa eseguirli.
	Tutte le altre app non aggiunte all'elenco possono essere installate sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno attivati e impostati in modo che l'utente possa eseguirli.

Tramite il pulsante , puoi aggiungere altre app o servizi all'elenco di quelli attualmente utilizzati.
Tramite il pulsante , puoi aggiungere altre applicazioni o servizi all'elenco attualmente inattivo.
Puoi definire un "nome del pacchetto":

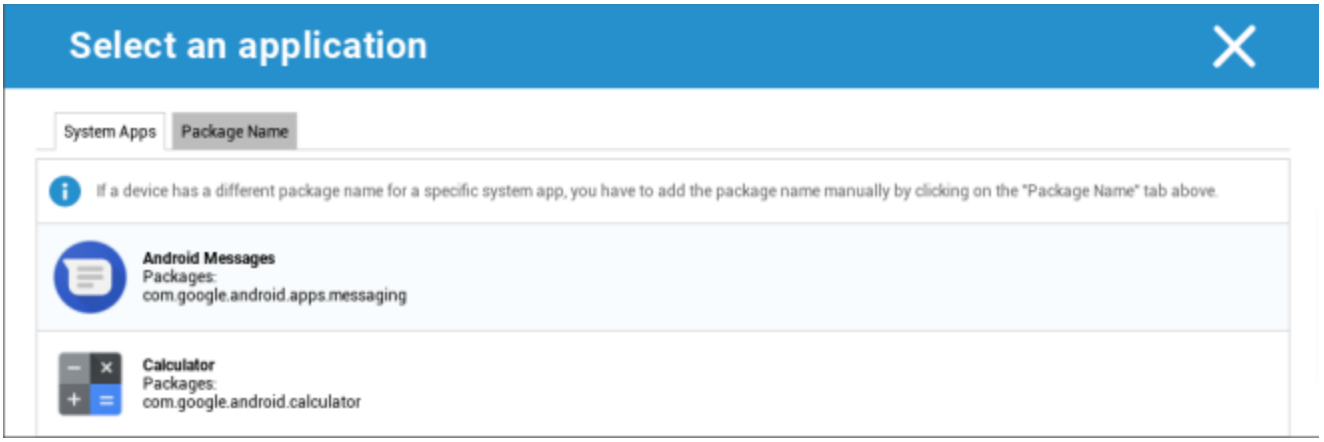

Select an application
Package Name
Enter App Identifier here ...
Add App

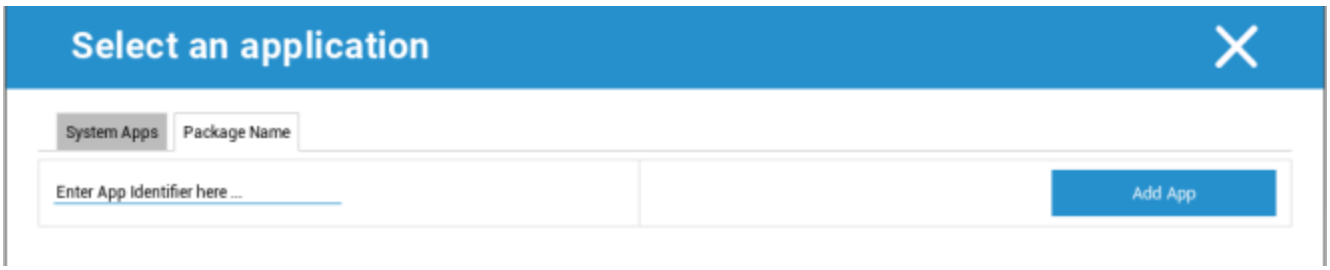
Applicazioni del sistema AE

Qui puoi definire un elenco contenente specifiche app di sistema che devono essere attivate sui dispositivi.



Se fai clic sul pulsante, puoi scegliere da un elenco di possibili app di sistema fornite da Google o inserire direttamente il nome del pacchetto di un'app di sistema da attivare.





Tieni presente che le app di sistema nell'elenco fornito da Google sono solo app che possono essere app di sistema, ma non devono necessariamente essere app di sistema sui tuoi dispositivi.

Tuttavia, questo elenco riguarda solo le app già preinstallate.

L'aggiunta di app che non sono preinstallate sui tuoi dispositivi non avrà alcun effetto sui tuoi dispositivi, indipendentemente dal fatto che l'app provenga dall'elenco fornito da Google o che il nome del pacchetto dell'app venga inserito direttamente.

Restrizioni e impostazioni

Impostazioni di gestione delle app

Qui puoi configurare il comportamento del dispositivo per quanto riguarda gli aggiornamenti delle app.

Frequenza di controllo degli aggiornamenti	Specifica in quale intervallo il client AppTec360 cercherà gli aggiornamenti delle applicazioni. Il valore predefinito è 24 ore.
Soglia Wi-Fi	Le app di dimensioni superiori a quelle specificate verranno scaricate tramite Wi-Fi. Se si seleziona "Solo Wi-Fi", tutte le app verranno scaricate tramite Wi-Fi.

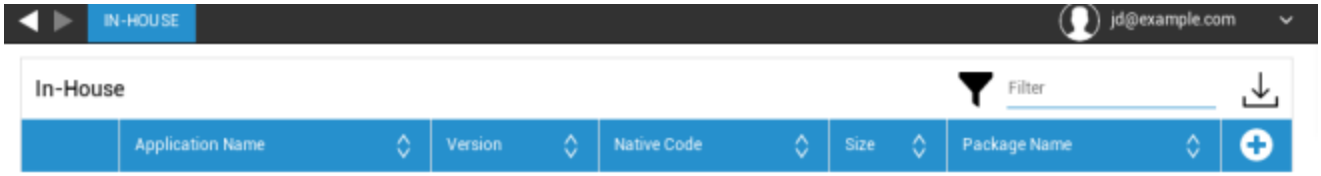
App Store aziendale

In-house

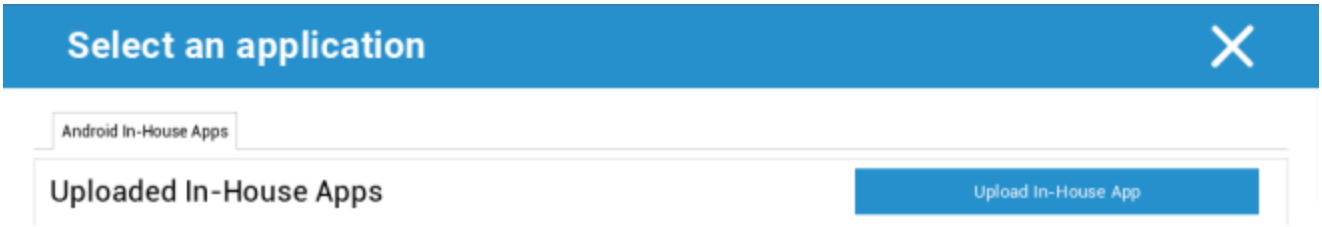
Al punto "In-House", puoi caricare e distribuire le app sviluppate internamente.

Con il simbolo puoi distribuire altre App In-House.

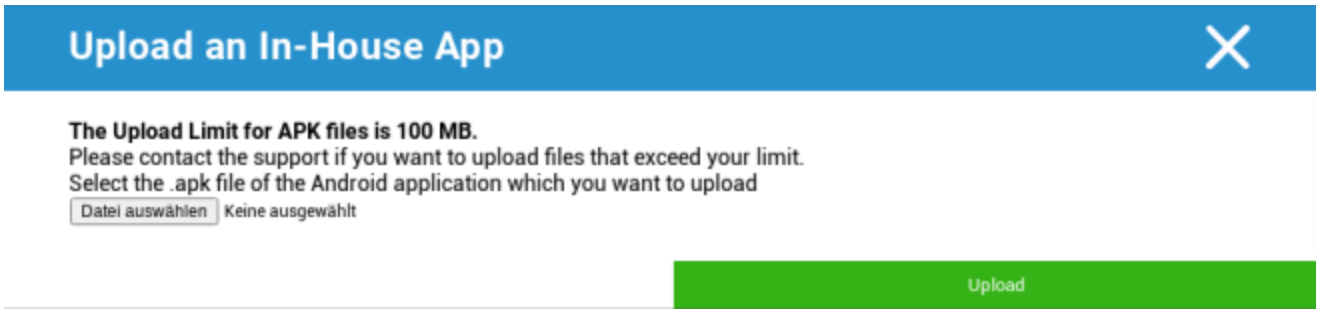
Se stai installando un'App In-House, avrai la possibilità di attivare la funzione "Tieni aggiornato". Se se l'applicazione è stata attivata e se hai definito una versione più recente nel DB delle applicazioni interne, l'applicazione sarà
aggiornato sul dispositivo.



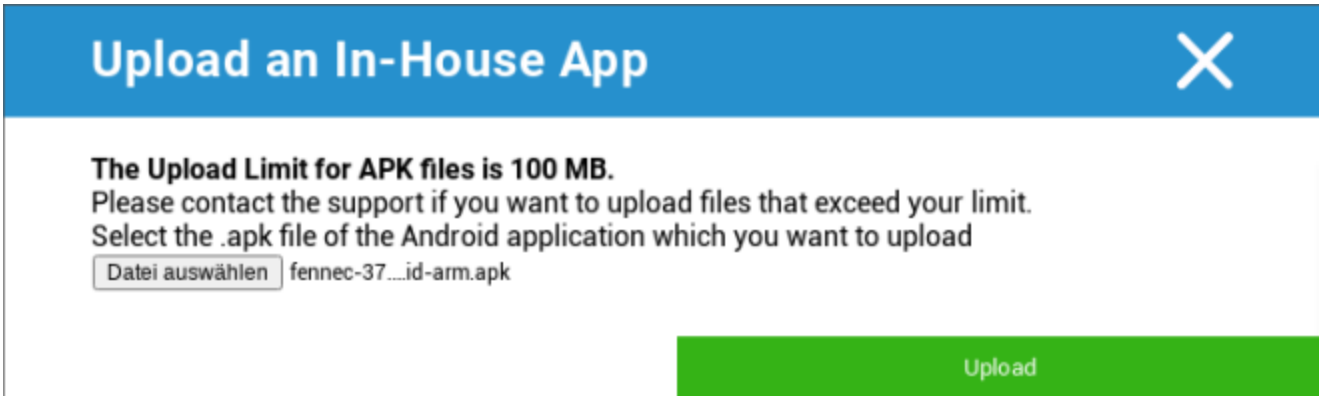
Se non hai distribuito App In-House, riceverai la seguente panoramica:



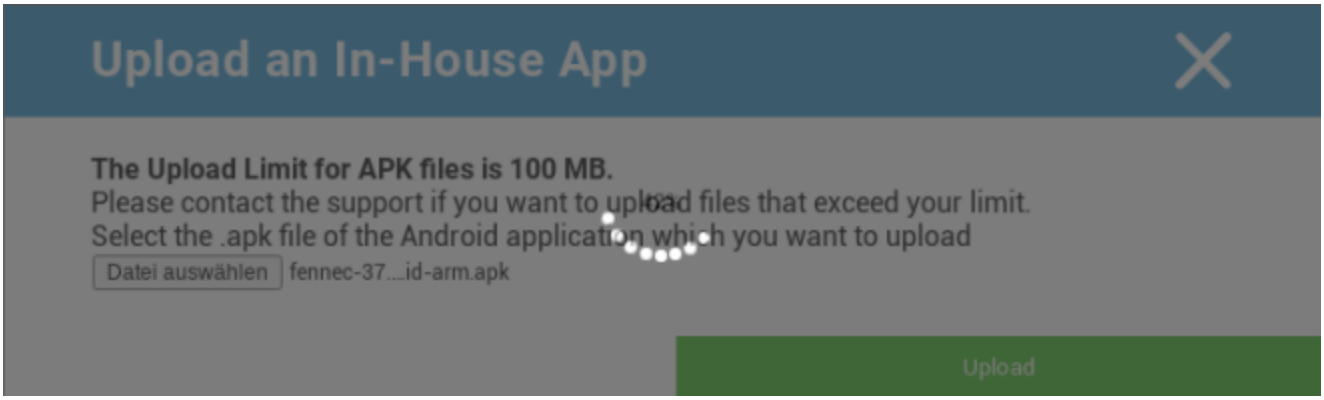
A tal fine, clicca su "Upload In-House App" e riceverai la seguente panoramica:



Ora scegli con "Cerca..." un file .apk e poi clicca su "Carica".



La tua applicazione sarà ora caricata; al centro del cerchio vedrai un indicatore di percentuale, che mostra quanta parte della tua applicazione è già stata caricata.



Se il caricamento della tua app interna è andato a buon fine, potrai trovare l'applicazione caricata nel tuo catalogo delle app.

L'utente ha ora la possibilità di vedere e installare l'applicazione nell'AppTec360 Store sull'utente finale.
sotto la categoria "In-house".

Poiché non si tratta di un'applicazione di Google PlayStore, l'utente non ha bisogno di un account Google memorizzato.
ID sul rispettivo dispositivo dell'utente finale.

Play Store aziendale

AE Play Store

Qui puoi aggiungere applicazioni al Playstore di Android Enterprise. Tieni presente che devi approvare App con il tuo account di amministratore AE prima di poterle aggiungere.

Per approvare un'applicazione, consulta le istruzioni riportate nella sezione Applicazioni obbligatorie.

Modalità chiosco e launcher

Modalità chiosco

La modalità Kiosk ti permette di predefinire un'applicazione o un URL. Allora sarà possibile esclusivamente
eseguire/visitare questa applicazione o URL.

Allo stesso modo, i vari pulsanti hardware possono essere disattivati nella modalità Kiosk.

Avvio automatico	Avvia automaticamente la modalità Kiosk non appena il profilo raggiunge il dispositivo dell'utente finale.
Modalità Kiosk programmata?	Puoi pianificare un orario per la modalità Kiosk, che inizierà e terminerà automaticamente all'orario da te stabilito.
Ora di inizio	Ora di inizio
Tempo in minuti	Tempo in minuti, dopo il quale la modalità Kiosk deve terminare di nuovo.

Tipo di applicazione

App singola	Se vuoi avviare l'applicazione in modalità Kiosk, seleziona "Pacchetto" sotto "Tipo di applicazione".
Applicazione chiosco	Clicca qui per selezionare un'applicazione che deve essere avviata in modalità Kiosk. Troverai la solita panoramica della gestione delle app Puoi scegliere tra "Google Play Store", "Android In-House Apps" e "Packagename".

Tipo di applicazione

URL	Se vuoi lanciare un URL nella modalità Kiosk, seleziona "URL" alla voce "Tipo di applicazione". Quindi definisci l'indirizzo URL desiderato
Cancella il browser dopo l'inattività	Qui puoi definire un intervallo di tempo in minuti, dopo il quale la Modalità Kiosk deve essere riavviata.
Cancella la cache e i cookie del web	Se attivi questa funzione, dopo un riavvio della modalità Kiosk, la cache web (cookie e immagini memorizzate nella cache) verrà cancellata.
Politica della stessa origine	Se questa funzione è attiva, l'utente può navigare solo nelle sottopagine di un URL definito. Ad esempio, hai definito il seguente URL:www.mypage.com Poi, l'utente può navigare su: www.mypage.com/subpage
URL inseriti nella whitelist	Qui puoi mantenere una Whitelist: tutti questi URL sono consentiti Massimo 1 URL per riga Un URL deve iniziare con http:/ o https://
URL nella lista nera	Qui è possibile mantenere una Blacklist, tutti questi URL non sono ammessi Massimo 1 URL per riga Un URL deve iniziare con http:/ o https://
Orientamento dello schermo	Questa impostazione riguarda le regolazioni dello schermo Automatico = automatico Ritratto = formato verticale Paesaggio = modalità paesaggio

Multi App	Se selezioni la modalità Kiosk "Multi App", l'uso del Launcher AppTec360 sarà obbligatorio.
Applicazioni	Applicazione: Seleziona un'applicazione Playstore o un'applicazione interna come applicazione Kiosk. È anche possibile inserire un nome di pacchetto. L'applicazione Kiosk selezionata deve essere installata sul dispositivo. Ricorda di impostare l'applicazione Kiosk come obbligatoria. Scorciatoia sulla homescreen: Se l'opzione è impostata su "On", verrà creata una scorciatoia sulla homescreen. Se è impostata su "Off", l'app verrà comunque visualizzata nell'elenco delle app.

Password di uscita abilitata	Se attivi questa funzione, l'utente potrà terminare la modalità Kiosk con una password predefinita dall'utente.
Password di uscita	Questa è la password che è stata preimpostata dall'utente
Barra di stato a collasso automatico	Se abilitata, la barra di stato sarà automaticamente in collisione. Con questa opzione gli utenti possono vedere le informazioni della barra di stato, ma non possono accedere alle sue funzioni.
Disabilita la barra di stato	La barra di stato contiene notifiche, scorciatoie e informazioni. Disponibile solo per i dispositivi Samsung con SAFE 4.0 o superiore.
Disabilita i tasti del volume	Disabilita i tasti del volume (disponibile solo sui dispositivi Samsung con SAFE 3.0 o superiore)
Disabilita l'interruttore On/Off	Disabilita l'interruttore On/Off (disponibile solo sui dispositivi Samsung con SAFE 3.0 o superiore)
Disabilita il pulsante Home	Disattiva il pulsante Home. Se questa funzione è stata attivata, la modalità Kiosk può essere interrotta solo dalla Console AppTec360. (disponibile solo su dispositivi Samsung con SAFE 3.0 o superiore)
Disabilita la barra di navigazione	Con questa funzione puoi disabilitare la barra di navigazione (Indietro / Menu). Se questa funzione è stata attivata, la modalità Kiosk può essere interrotta solo dalla Console AppTec360. (disponibile solo su dispositivi Samsung con SAFE 3.0 o superiore)

AppTec360 Launcher

Abilita il Launcher di AppTec360	On: Attiva il Launcher di AppTec360. L'utente deve impostarlo come launcher predefinito una volta. Nota: se la modalità Kiosk è abilitata e la modalità Kiosk è impostata su "Multi App", l'uso del launcher AppTec360 sarà obbligatorio.
Icone grandi	On: Mostra una versione più grande delle icone delle app nel Launcher.
Nascondi l'icona dell'app AppTec360	Attiva: Nasconde completamente l'applicazione AppTec360
Nascondi l'icona di AppTec360 Store	Attiva: Nasconde completamente l'AppStore di AppTec360 Enterprise.

Impostazioni di AppTec360

Abilita l'applicazione Impostazioni di AppTec360	L'applicazione AppTec360 Settings fornisce il controllo delle connessioni WiFi e Bluetooth.
Abilita le impostazioni in Multi App Modalità chiosco	Se abilitata, gli utenti possono accedere all'applicazione Impostazioni di AppTec360 mentre è attiva la modalità Kiosk Multi App.

Telecomando

Splashtop

Per avviare una sessione di controllo remoto del tuo dispositivo, l'applicazione "Splashtop Streamer" deve essere installata sul dispositivo aggiungendola a **Gestione applicazioni** → **Enterprise App Manager** → **Applicazioni obbligatorie**.

Successivamente, configura le seguenti impostazioni per Splashtop:

Abilita Splashtop	Se abilitata, AppTec360 configurerà l'applicazione Splashtop in modo da consentire il controllo da remoto
Distribuire il codice	Vai su https://my.splashtop.com e accedi al tuo account Splashtop. Clicca su "Aggiungi computer" e copia il codice di distribuzione di 12 cifre dalla pagina risultante.
Impostare il gateway di distribuzione personalizzato?	Distribuire il gateway
Distribuire il dominio/host del gateway	Distribuire il gateway
Verifica del certificato	Verifica del certificato

Quindi puoi utilizzare l'opzione Splashtop Remote Control del menu contestuale (ingranaggio accanto alla barra di ricerca, quando il dispositivo è selezionato o tasto destro del mouse sul dispositivo nella struttura) per avviare la sessione di controllo remoto.

TeamViewer

Per avviare una sessione di controllo remoto del tuo dispositivo, l'applicazione "TeamViewer QuickSupport" deve essere installata sul dispositivo aggiungendola a **Gestione applicazioni** → **Enterprise App Manager** → **Applicazioni obbligatorie**.

Quindi puoi utilizzare l'opzione **Controllo remoto di TeamViewer** nel menu contestuale (ingranaggio accanto alla barra di ricerca, quando il dispositivo è selezionato o tasto destro del mouse sul dispositivo nella struttura) per avviare la sessione di controllo remoto.

Gestione dei contenuti

ContentBox

Qui puoi attivare il ContentBox.

Non appena avrai impostato "Abilita ContentBox" su "On", verrà installata un'applicazione ContentBox separata.
automaticamente sul dispositivo dell'utente finale.

Browser sicuro

Qui puoi configurare le impostazioni di AppTec360 Secure Browser.

Non appena avrai impostato la sezione "Browser sicuro" su "On", verrà attivata un'applicazione Browser separata.
installato automaticamente sul dispositivo dell'utente finale.

Richiedi la password	Richiedere all'utente di impostare e utilizzare una password per accedere al browser.
Lunghezza minima richiesta per la password	Imposta il numero di caratteri richiesto per la password
Qualità della password richiesta	Imposta la qualità della password richiesta
Limita i download / Apri in	
Limitare i caricamenti	
Carica la Whitelist	Un elenco di URL per i quali il caricamento sarà sempre consentito.
Consenti la copia	Consente di copiare, tagliare o condividere il testo all'interno delle pagine web.
Consenti la cattura dello schermo	Consente di catturare screenshot.
Frequenza di pulizia dei dati	Seleziona con quale frequenza TUTTI i dati dell'utente (cronologia, cache, ecc.) devono essere rimossi automaticamente.
Segnalibri aziendali	I segnalibri verranno visualizzati nella cartella "segnalibri aziendali" dei segnalibri del browser. Non sono modificabili dall'utente.
Nascondi la barra degli indirizzi	
Whitelisting nel browser (senza Universal Gateway)	Abilita la whitelist degli URL lato client. • I segnalibri aziendali sono sempre inseriti nella whitelist • Supportato solo per 100 URL • Utilizza il Gateway Universale per un Black- e Whitelisting illimitato.
URL inseriti nella whitelist	Un elenco di URL consentiti.

Black- e Whitelist basati su gateway	La lista nera ha i seguenti requisiti: • Un AppTec360 Universal Gateway funzionante ("Impostazioni generali" → "Universal Gateway") • Una configurazione VPN funzionante con un server DNS specificato ("Impostazioni generali" → "Gateway universale" → "Impostazioni VPN") • Configurazione della lista nera ("Impostazioni generali" → "Universal Gateway" → "Lista nera dei domini") • Una connessione VPN valida nel profilo ("Gestione connessioni" → "VPN")

API aggiuntive

Samsung KNOX

Restrizioni

Consenti la scheda SD	
Consenti la scrittura della scheda SD	
Consenti la cattura dello schermo	
Consenti gli appunti	
Backup delle impostazioni e dei dati dell'app su Google Cloud	
Ripristinare le impostazioni da Google Cloud quando si reinstalla un'applicazione	
Consenti il debug USB	
Consenti il rapporto di crash di Google	
Consenti il reset di fabbrica	
Consenti l'aggiornamento OTA	
Consenti l'archiviazione host USB	Se abilitato, l'utente può collegare qualsiasi pen drive (memoria USB portatile), HD esterno o lettore di schede Secure Digital (SD) e viene montato come unità di archiviazione sul dispositivo.
Consenti il lettore multimediale USB (MTP, PTP)	
Consenti il microfono	Disattiva il microfono per le applicazioni di terze parti
Consenti NFC (Near Field Communication)	
Consenti fonti sconosciute (APK Sideloading)	Se abilitato, il caricamento laterale delle applicazioni (file APK) è consentito. Una volta disattivata questa impostazione, l'utente deve attivarla manualmente quando si riabilita l'installazione di APK da fonti sconosciute.

Consenti la creazione di utenti	Se abilitato, l'utente può creare più account sul dispositivo, ad esempio account ospite.

Email

Indirizzo e-mail	
Protocollo del server in entrata	
Indirizzo del server in entrata	
Porta del server in entrata	
Login/nome utente del server in arrivo	
Password del server in entrata	
Il server in entrata utilizza SSL	
Il server in entrata utilizza TLS	
Il server in entrata accetta tutti i certificati	
Protocollo del server in uscita	
Indirizzo del server in uscita	
Porta del server in uscita	
Il server in uscita utilizza credenziali extra	Se è disattivato, il sistema utilizza le credenziali in entrata anche per il server in uscita.
Login/nome utente del server in uscita	
Password del server in uscita	
Il server in uscita utilizza SSL	
Il server in uscita utilizza TLS	
Il server in uscita accetta tutti i certificati	
Imposta la firma	
Firma	Nota: per alcuni dispositivi la firma deve essere specificata in formato HTML.
Notifica all'utente la ricezione di una nuova e-mail	

Scambio

Indirizzo e-mail	
Nome host del server	Il nome dell'host del server di Exchange
Nome utente	Il nome utente utilizzato per accedere a Exchange Server
Dominio	Se è abilitata una configurazione ACL Gateway e il campo Dominio non è vuoto, AppTec360 Universal Gateway autenticherà il dispositivo con il seguente nome "Dominio".
Password	
Numero di giorni precedenti da sincronizzare	
Frequenza di sincronizzazione delle e-mail	
Sincronizzazione in roaming	
Imposta la firma	
Firma	Nota: per alcuni dispositivi la firma deve essere specificata in formato HTML.
Conto predefinito	
Utilizza il Secure Sockets Layer (SSL)	
Usa la sicurezza del livello di trasporto (TLS)	
Accetta tutti i certificati	

APN

Nome visualizzato APN	
Nome del punto di accesso	Nome dell'APN
Protocollo del server in uscita	
MCC - Codice paese mobile	Lascia vuoto per utilizzare l'mmc della SIM installata
MNC - Codice di rete mobile	Lasciare vuoto per utilizzare l'mnc della SIM installata
Indirizzo del server	
Numero di porta del server	
Indirizzo proxy del server	
Indirizzo del server MMS	Lasciare vuoto per l'impostazione predefinita
Numero di porta MMS	Lasciare vuoto per l'impostazione predefinita
Indirizzo proxy MMS	Lasciare vuoto per l'impostazione predefinita
Nome utente	
Password	
Tipo di punto di accesso	I tipi accettati sono "default", "mms", "supl".
	Se viene passato null o vuoto, per impostazione predefinita viene utilizzato "default,supl,mms".
	Lascia vuoto per impostazione predefinita.
APN preferito	

Bluetooth

Consenti il rilevamento del dispositivo tramite Bluetooth	
Consenti l'accoppiamento Bluetooth	
Consenti i dispositivi auricolari Bluetooth	
Consenti i dispositivi vivavoce Bluetooth	
Consenti i dispositivi Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile, consente lo streaming audio tra dispositivi.
Consenti le chiamate in uscita	
Consenti il trasferimento dei dati via Bluetooth	
Consenti il tethering Bluetooth	
Consenti la connessione al computer tramite Bluetooth	

Connessione

Consenti solo le chiamate di emergenzaConsenti il Wi-Fi	
Livello minimo di sicurezza della rete Wi-Fi	
Impedisci all'utente di aggiungere reti Wi-Fi	Questa restrizione può essere attivata solo se è stato definito almeno un profilo Wi-Fi attivo in Gestione connessioni.
Consenti SMS e MMS	
Consenti la sincronizzazione durante il roaming	
Consenti il roaming vocale	

Android Enterprise – Dispositivo completamente gestito con profilo di lavoro (COPE)

Spiegazione generale del COPE

COPE è l'abbreviazione di **Corporate Owned Personally Enabled**.

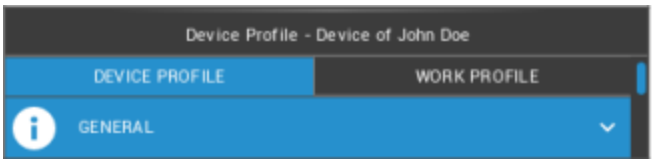
La modalità COPE consente di registrare un dispositivo Android come **dispositivo Android Enterprise - Fully Managed** con profilo **Android Enterprise - Container** integrato.

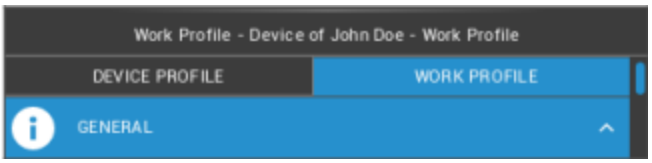
Può trattarsi di un dispositivo Android che è già registrato come **Android Enterprise - Dispositivo completamente gestito** e su cui il **Android Enterprise - Container** o un dispositivo Android appena registrato che è stato registrato direttamente come dispositivo **Android Enterprise - Dispositivo completamente gestito** insieme al **Android Enterprise - Container** in cima ad esso.

La modalità COPE è disponibile solo per i dispositivi con Android 8, 9 e 10.

Configurazione dei profili per i dispositivi COPE

Poiché non esiste un profilo di configurazione per la modalità COPE, la configurazione di **Android Enterprise - Dispositivo completamente gestito** e **Android Enterprise - Contenitore** è separata in due profili all'interno del profilo COPE. È possibile passare da un profilo all'altro per la configurazione di ciascun profilo cliccando sul rispettivo pulsante sul lato sinistro della console:





Entrambi i profili possono essere configurati come descritto per ogni singolo profilo:

Android Enterprise - Dispositivo completamente gestito

Android Enterprise - Container

Ritorno al dispositivo AE completamente gestito

Il profilo **Android Enterprise - Container** può essere rimosso come descritto in **Gestione dei dispositivi mobili**.

Rimuovendo il profilo Container, il profilo COPE si trasformerà in un profilo **Android Enterprise - Fully Managed Device**.

Android Enterprise – Configurazione del contenitore

A seconda che tu abbia selezionato un profilo di gruppo o un dispositivo, la panoramica e i suoi punti secondari sono diversi: ti preghiamo di considerare attentamente questo aspetto!

Generale

Panoramica del profilo (solo a livello di profilo)

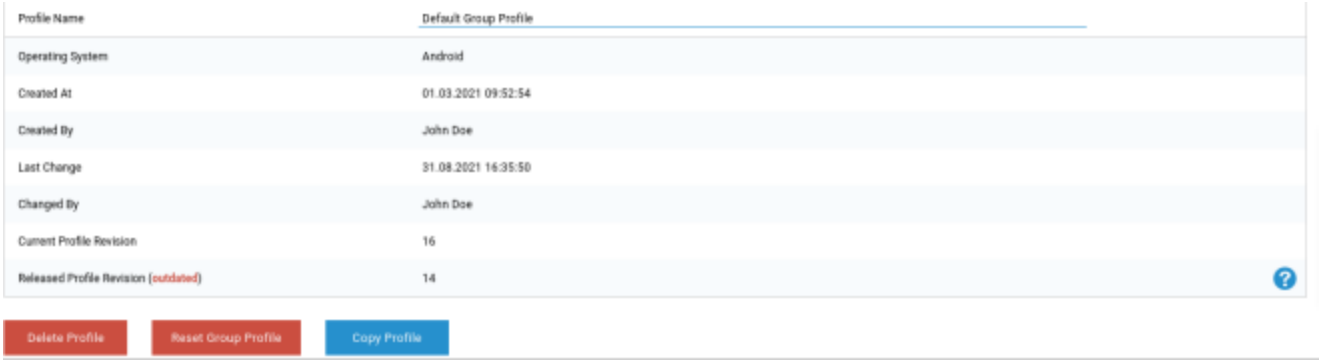
Se ti trovi in un profilo, riceverai una breve panoramica del profilo, per quanto riguarda il nome, il sistema operativo, la data di creazione, l'autore, ecc.

Nome del profilo	Nome del profilo - può essere rinominato direttamente qui
Sistema operativo	Sistema operativo valido per il profilo
Creato a	Data di creazione
Creato da	Creato da
Ultimo cambiamento	Data dell'ultima modifica
Modificato da	L'utente che ha eseguito le ultime modifiche a questo profilo
Revisione del profilo attuale	Numero di volte in cui il profilo è già stato aggiornato
Revisione del profilo rilasciata	Numero di volte in cui il profilo è già stato aggiornato e sono stati assegnati dei dispositivi

Elimina il profilo	Elimina il profilo
Ripristina il profilo del gruppo	Ripristina il profilo del gruppo
Copia del profilo	Copia del profilo

Panoramica del profilo del gruppo (solo a livello di gruppo)

Quando apri il profilo di un gruppo, otterrai una rapida panoramica del profilo.



Nome del profilo	Nome del profilo (può essere modificato qui)
Sistema operativo	Sistema operativo per cui è stato creato il profilo
Creato a	Tempo della creazione
Creato da	Il creatore del profilo
Ultimo cambiamento	Ora dell'ultima modifica al profilo
Modificato da	Account che ha apportato le ultime modifiche
Revisione del profilo attuale	Revisione dello stato del profilo salvato
Revisione del profilo rilasciata	Revisione del profilo assegnata ("Assegna ora"). Se l'etichetta mostra " (outdated)" dietro il testo, significa che hai salvato il profilo ma non l'hai ancora assegnato, quindi i dispositivi riceveranno ancora la versione più vecchia.

Panoramica del dispositivo (solo a livello di dispositivo)

Se ti trovi su un dispositivo, riceverai un riepilogo del dispositivo selezionato:

Nome del dispositivo	Nome del dispositivo
Posizione	Coordinate della posizione
Numero di telefono	Numero di telefono
Applicazioni obbligatorie assegnate	Numero di applicazioni obbligatorie assegnate
Versione OS	Versione del sistema operativo del dispositivo
Sistema operativo	Sistema operativo (Android Enterprise)
Numero di serie	Numero di serie del dispositivo
Proprietà del dispositivo	Dispositivo aziendale o privato
Tipo di dispositivo	Dispositivo gestito da AE Work
Radicati	Stato, che indica se il dispositivo è stato sottoposto a rooting
Conforme	Conformi alle linee guida
Indirizzo IP	Indirizzo IP del dispositivo
Ultimo visto	Momento in cui il dispositivo si è connesso per l'ultima volta ad AppTec.
Ultima spinta	Momento in cui è stato inviato l'ultimo push al dispositivo.
Assegnazione dell'utente	L'utente o il gruppo a cui è assegnato questo dispositivo

Revisione della configurazione

Qui puoi vedere quale profilo di gruppo è assegnato al dispositivo.

Se clicchi sul profilo del gruppo, avrai accesso diretto a questo profilo e potrai eseguire le impostazioni.

Con questo simbolo puoi riportare le applicazioni distribuite alle impostazioni del profilo del gruppo.

Con questo simbolo puoi riportare tutte le app utilizzate alle impostazioni del profilo del gruppo.

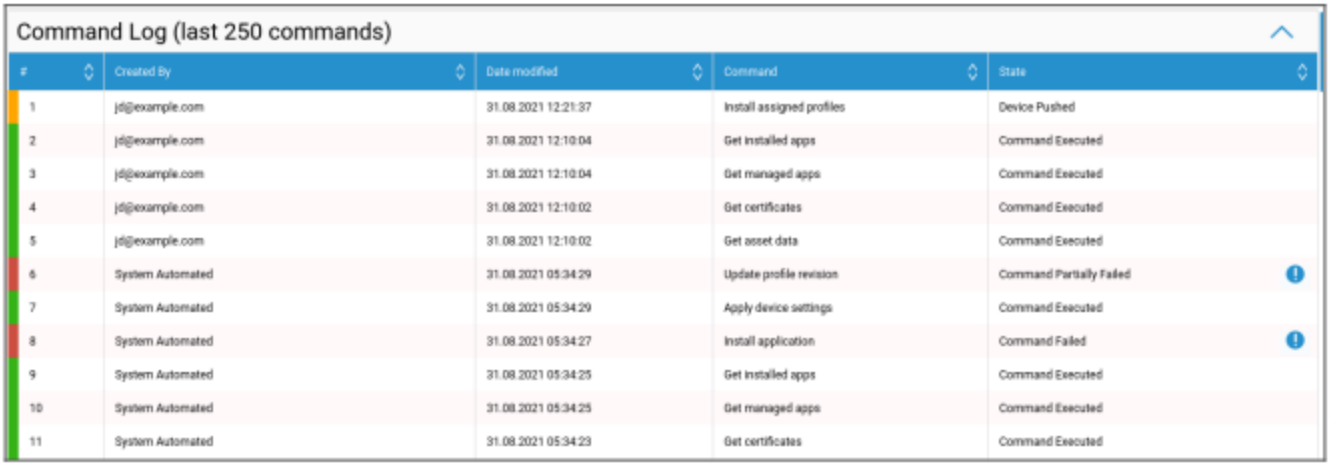
L'indicazione "Revisione più recente disponibile" indica che il profilo del gruppo è stato modificato e salvato ma non assegnato. Il profilo del gruppo deve essere assegnato con "Assegna ora" a livello di gruppo per applicare le modifiche ai dispositivi.

Registro del dispositivo (solo a livello di dispositivo)

Qui riceverai diversi log del dispositivo. Se necessario, puoi scoprire direttamente la causa di un errore qui.

Registro dei comandi

Qui puoi vedere quali comandi sono stati emessi per il dispositivo e qual è il loro stato.



Possibili stati del comando

Dispositivo spinto	È stata inviata una richiesta push al servizio push (ad esempio APNS) per indicare al dispositivo di connettersi nuovamente al server EMM.
Comando creato	Il comando è stato creato nel sistema.
Comando inviato	Il comando è stato inviato al dispositivo dopo la connessione al server.
Comando eseguito	Il comando è stato eseguito con successo.
Comando fallito	Il comando è fallito. *
Comando parzialmente fallito	A seconda del sistema operativo del dispositivo, alcuni comandi possono essere raggruppati. In questo caso alcune parti di questo gruppo di comandi sono fallite. *
Comando eseguito, alla fine fallito	Il comando è stato eseguito ma forse non lo è stato.
Comando Riportato	Il comando è stato ripreso da un utente.
Scartato	Il comando è stato scartato. Ad esempio perché è stato sostituito da un altro comando o perché il dispositivo è stato reinserito e i vecchi comandi sono stati rimossi.

*Se dietro il messaggio c'è un punto esclamativo, puoi ottenere maggiori informazioni passando il cursore sull'icona.

Impostazioni del dispositivo

Configurazione del cliente

Qui puoi eseguire le seguenti configurazioni sul tuo dispositivo Android:

Tempo di non conformità	Il limite di timeout di risposta dell'utente dopo il quale viene applicata l'azione di applicazione.
Azione esecutiva dopo il timeout di conformità	Azione di controllo quando un utente non esegue azioni che portano a uno stato di conformità del dispositivo.
Frequenza di raccolta dei dati	Frequenza con cui raccogliere le informazioni sul dispositivo/GPS
Frequenza del battito cardiaco del dispositivo	Intervallo di tempo in cui il dispositivo deve contattare il Server AppTec Min. 1 minuto Max. 24 ore
Abilita gli aggiornamenti della posizione	Se attivato, il dispositivo invia aggiornamenti sulla posizione al server AppTec.
Posizione Ora di aggiornamento	Determina in quali intervalli di tempo il dispositivo invia ad AppTec gli aggiornamenti sulla posizione.
Usa Google Location Accuracy per l'aggiornamento della posizione	Se attivata, la posizione di rete verrà utilizzata per gli aggiornamenti della posizione (se è stata disattivata in "Restrizioni", questa impostazione non avrà alcun effetto).
Usa la posizione GPS per l'aggiornamento della posizione	Se attivato, il GPS verrà utilizzato per gli aggiornamenti sulla posizione.
Consenti le posizioni fittizie (false)	Consente di falsificare le informazioni sulla posizione tramite applicazioni di terze parti
Azione di perdita della connessione	Se abilitata, puoi specificare un'azione nel caso in cui un dispositivo non si connetta al server MDM nell'intervallo di heartbeat. Ad esempio, se il dispositivo ha un tempo di battito cardiaco di 5 minuti, si connette al server alle 10:35 del mattino. Dopodiché il dispositivo esce dal raggio d'azione del Wi-Fi. Il prossimo battito cardiaco delle 10:40 fallirà e verrà eseguita l'azione specificata.
Azione	L'azione da intraprendere non appena un dispositivo diventa non conforme. • Lock Dispositivo = dispositivo di blocco

	• Wipe Device = il dispositivo verrà ripristinato alle impostazioni di fabbrica. • Wipe Device & SD Card = il dispositivo verrà ripristinato alle impostazioni di fabbrica e la memoria della scheda SD verrà cancellata.
Soglia	Puoi specificare una soglia di battiti cardiaci falliti necessari per attivare l'azione specificata.

Modalità di applicazione dei criteri	Predefinito:	Agli utenti verrà richiesto periodicamente di eseguire le azioni in sospeso.
	Applicazione pigra dei criteri:	Agli utenti non verrà mai richiesto di eseguire azioni in sospeso. Tutte le azioni aperte saranno visualizzate nel client AppTec.
	Applicazione aggressiva dei criteri:	Agli utenti verrà richiesto senza sosta di eseguire le azioni in sospeso.
Blocco della versione di AppTec	Se abilitato, è possibile specificare un codice di versione per l'applicazione AppTec. Il client AppTec si aggiornerà solo alla versione specificata. Le versioni più recenti saranno ignorate. Non è possibile effettuare un downgrade.	
Codice versione	Codice della versione dell'applicazione AppTec da bloccare.	
Disattivare la notifica di AppTec	Se disattivato, il client AppTec non mostrerà alcuna notifica nella barra delle notifiche. Gli utenti possono quindi chiudere il client AppTec tramite il task manager. Se il client AppTec è chiuso, diverse funzioni, tra cui la modalità Kiosk e la lista nera/bianca delle app, non funzioneranno correttamente. I dispositivi Samsung offrono un meccanismo di protezione per il client AppTec. La notifica è disattivata per impostazione predefinita sui dispositivi Samsung che supportano le API KNOX. La notifica non dovrebbe essere disabilitata sui dispositivi con Android 8.0 o superiore.	

Carta da parati

Imposta uno sfondo personalizzato	Abilita/Disabilita lo sfondo personalizzato
Carta da parati	Imposta la modalità di sfondo per utilizzare un codice colore o un'immagine.
Specifica un colore	Specifica un colore di sfondo come valore esadecimale, ad esempio #000000 per il nero o #ffffff per il bianco.
Imposta l'immagine come sfondo	Carica il file dell'immagine che vuoi utilizzare come sfondo

Gestione delle risorse (solo a livello di dispositivo)

Info sul dispositivo

Modello	Denominazione del modello del dispositivo
Sistema operativo	OS
Versione OS	Versione del sistema operativo
Numero di serie	Numero di serie
Nome del dispositivo	Nome del dispositivo
Stato della batteria	Stato della batteria
Memoria libera / totale	Memoria libera / Totale
Samsung Safe	Interfaccia Samsung SAFE, necessaria per una serie di opzioni di impostazione
Scheda SD disponibile	Scheda SD disponibile
Scheda SD emulata	Scheda SD emulata
Scheda SD rimovibile	Scheda SD rimovibile
SD Memoria libera / Memoria totale	SD Libera / Memoria totale della scheda SD

Wi-Fi

Indirizzo IP	Indirizzo IP del dispositivo
WiFi MAC	Indirizzo MAC WiFi

Cellulare

Stato	Stato (scheda SIM installata)
Numero di telefono	Numero di telefono
Roaming (voce/dati)	Roaming per voce/dati
Stato del roaming	Stato attuale del roaming
Indirizzo IP	Indirizzo IP
Operatore/Vettore	Operatore/Vettore
Tecnologia cellulare	Tecnologia cellulare
IMEI	Numero IMEI
ICCID	Si tratta dell'ID della carta SIM, spesso anche Smartcard o Carta a Circuito Integrato (ICC).
IMSI	L'International Mobile Subscriber Identity (IMSI) fornisce nelle reti mobili GSM e UMTS un'identificazione precisa degli utenti della rete. L'IMSI è composto da un massimo di 15 cifre e viene configurato nel modo seguente: • Codice paese mobile (MCC), 3 cifre • Codice di rete mobile (MNC), 2 o 3 cifre • Numero di identificazione dell'abbonato mobile (MSIN), da 1 a 10 cifre
Attuale MCC/MNC	Vedere "SIM MCC/MNC"
SIM MCC/MNC	Il codice del paese mobile è un identificativo del paese stabilito dall'ITU secondo la norma E.212. Standard. Questo funziona insieme al Mobile Network Code (MNC) per l'identificazione della rete mobile. Ovvero il codice di rete nazionale/mobile della carta SIM. Se fai il roaming su un'altra rete mobile, logicamente il "Current MCC/MNC" e il "SIM MCC/MNC" saranno diversi.

Bluetooth

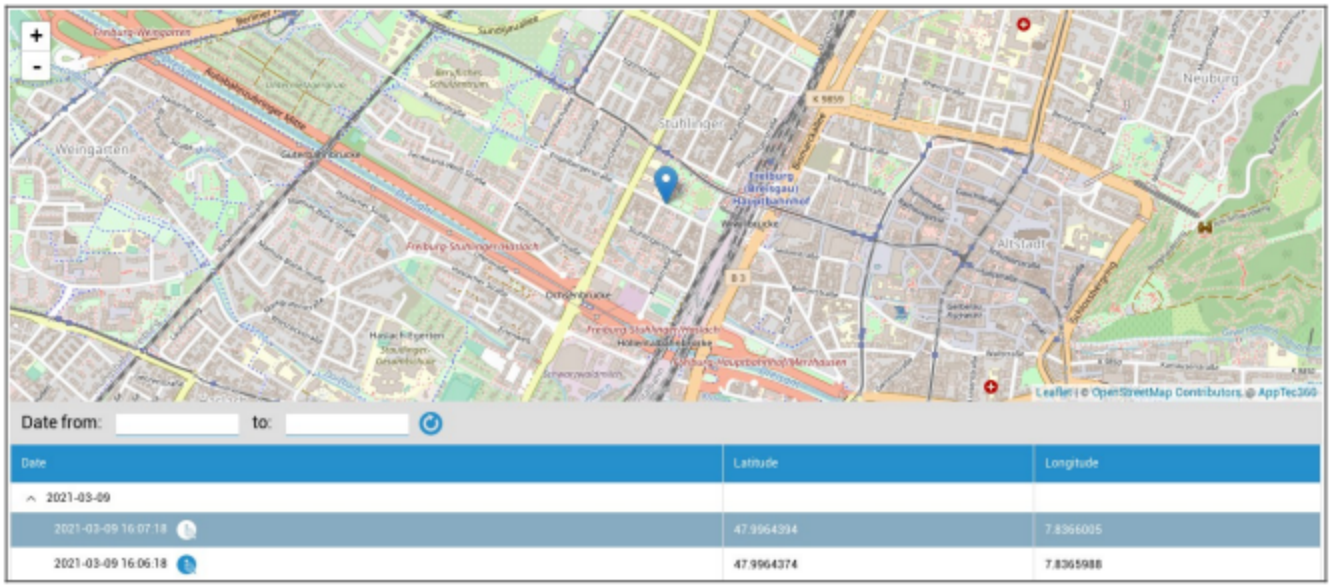
MAC Bluetooth	Indirizzo MAC Bluetooth

Gestione della sicurezza

Antifurto (solo a livello di dispositivo)

Informazioni GPS (solo a livello di dispositivo)

Qui puoi stabilire la posizione attuale/ultima del dispositivo. La localizzazione può essere protetta con una o anche due password - Vedi: Impostazioni generali - Privacy - Accesso GPS



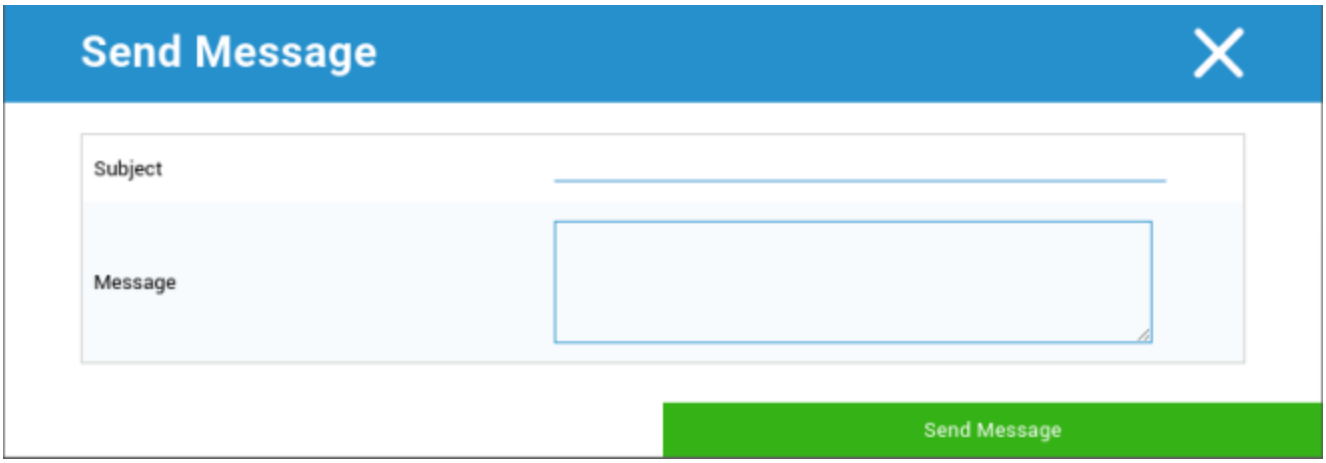
Pulisci e blocca (solo a livello di dispositivo)

Alla voce "Pulisci e blocca", puoi eseguire le seguenti tre azioni:

Pulizia completa	Il dispositivo viene riportato alle impostazioni di fabbrica (i dati aziendali e personali vengono cancellati). Funziona solo per il Profilo di lavoro avanzato
Pulizia aziendale	Solo i dati aziendali vengono rimossi dal dispositivo dell'utente finale (tutte le applicazioni, i dati, ecc. che sono stati forniti da AppTec)
Schermata di blocco	Il blocco dello schermo è attivato, è sufficiente sbloccare il dispositivo con la password/PIN del dispositivo.

Messaggio (solo a livello di dispositivo)

Qui puoi inserire l'oggetto e un messaggio e inviarlo a un dispositivo dell'utente finale.



Configurazione della sicurezza

Codice di accesso al dispositivo

Alla voce "Codice di accesso" puoi assegnare una password al dispositivo; sono disponibili le seguenti opzioni di impostazione

Lunghezza minima della password	Stabilisce il numero minimo di simboli che una password deve contenere	
Qualità della password	Non specificato	Questa politica non prevede requisiti per la password.
	Biometrico debole	Questa politica consente una tecnologia di riconoscimento biometrico a bassa sicurezza. Questo implica tecnologie in grado di riconoscere l'identità di un individuo fino a circa un PIN di 3 cifre (il rilevamento di falsi è inferiore a 1 su 1.000).
	Qualcosa	Questo criterio richiede l'impostazione di un qualche tipo di password o modello, ma non applica alcuna regola specifica.
	Alfabetico	L'utente deve aver inserito una password contenente almeno caratteri alfabetici (o altri simboli).
	Alfanumerico	L'utente deve aver inserito una password contenente almeno due caratteri numerici e alfabetici (o altri simboli).
	Complesso	L'utente deve aver inserito una password contenente almeno una lettera, una cifra numerica e un simbolo speciale, per impostazione predefinita. Con questa qualità di password, le password possono essere limitate a contenere vari set di caratteri, come almeno una lettera maiuscola, ecc.
Lunghezza minima della password	Imposta il numero di caratteri richiesto per la password. Ad esempio, puoi richiedere che il PIN o la password abbiano almeno sei caratteri.	
Cifre numeriche minime richieste nella password	Cifre numeriche minime richieste nella password	
Lettere minuscole minime richieste nella password	Lettere minuscole minime richieste nella password	

Lettere maiuscole minime richieste nella password	Lettere maiuscole minime richieste nella password
Caratteri non letterali minimi richiesti nella password	Caratteri non letterali minimi richiesti nella password
Simboli minimi richiesti nella password	Simboli minimi richiesti nella password

Blocco del tempo massimo di inattività	Inattività massima dell'utente fino al blocco temporale
Timeout di scadenza della password	Stabilisce, dopo quale intervallo di tempo la password scade e deve essere emessa una nuova password.
Limitazione della cronologia delle password	Numero di password precedentemente utilizzate che non sono consentite
Massimo di tentativi di password falliti	Stabilisce quante volte una password può essere inserita in modo errato prima che venga eseguita una cancellazione completa del dispositivo.
Consenti l'autenticazione biometrica	Consente l'autenticazione tramite impronta digitale o scansione dell'iride. Solo per Samsung KNOX 2.1 e successivi

Codice di accesso al contenitore

Alla voce "Codice di accesso" puoi assegnare una password per il contenitore.
a tua disposizione

Lunghezza minima della password	Stabilisce il numero minimo di simboli che una password deve contenere	
Qualità della password	Non specificato	Questa politica non prevede requisiti per la password.
	Biometrico debole	Questa politica consente una tecnologia di riconoscimento biometrico a bassa sicurezza. Questo implica tecnologie in grado di riconoscere l'identità di un individuo fino a circa un PIN di 3 cifre (il rilevamento di falsi è inferiore a 1 su 1.000).
	Qualcosa	Questo criterio richiede l'impostazione di un qualche tipo di password o modello, ma non applica alcuna regola specifica.
	Alfabetico	L'utente deve aver inserito una password contenente almeno caratteri alfabetici (o altri simboli).
	Alfanumerico	L'utente deve aver inserito una password contenente almeno due caratteri numerici e alfabetici (o altri simboli).
	Complesso	L'utente deve aver inserito una password contenente almeno una lettera, una cifra numerica e un simbolo speciale, per impostazione predefinita. Con questa qualità di password, le password possono essere limitate a contenere vari set di caratteri, come almeno una lettera maiuscola, ecc.
Lunghezza minima della password	Imposta il numero di caratteri richiesto per la password. Ad esempio, puoi richiedere che il PIN o la password abbiano almeno sei caratteri.	
Cifre numeriche minime richieste nella password	Cifre numeriche minime richieste nella password	
Lettere minuscole minime richieste nella password	Lettere minuscole minime richieste nella password	
Lettere maiuscole minime richieste nella password	Lettere maiuscole minime richieste nella password	

Caratteri non letterali minimi richiesti nella password	Caratteri non letterali minimi richiesti nella password
Simboli minimi richiesti nella password	Simboli minimi richiesti nella password

Blocco del tempo massimo di inattività	Inattività massima dell'utente fino al blocco temporale
Timeout di scadenza della password	Stabilisce, dopo quale intervallo di tempo la password scade e deve essere emessa una nuova password.
Limitazione della cronologia delle password	Numero di password precedentemente utilizzate che non sono consentite
Massimo di tentativi di password falliti	Stabilisce quante volte una password può essere inserita in modo errato prima che venga eseguita una cancellazione completa del dispositivo.

AntiVirus

Scansione automatica	Abilita le scansioni automatiche periodiche
Intervallo di scansione	Intervallo per l'esame (Rapido / Completo)
Scansione automatica completa	Abilita le scansioni automatiche complete
Aggiornamenti automatici	Abilita gli aggiornamenti automatici
Intervallo di controllo dell'aggiornamento	Ogni quanto tempo l'app e il suo database devono essere aggiornati (virus/codice danneggiato)
Protezione delle app	Abilita la scansione automatica delle app
Protezione della scheda SD	Abilita la scansione automatica della scheda SD
Aggiornamento solo Wi-Fi	Se abilitato, gli aggiornamenti verranno applicati solo quando il dispositivo è connesso correttamente a una rete Wi-Fi.

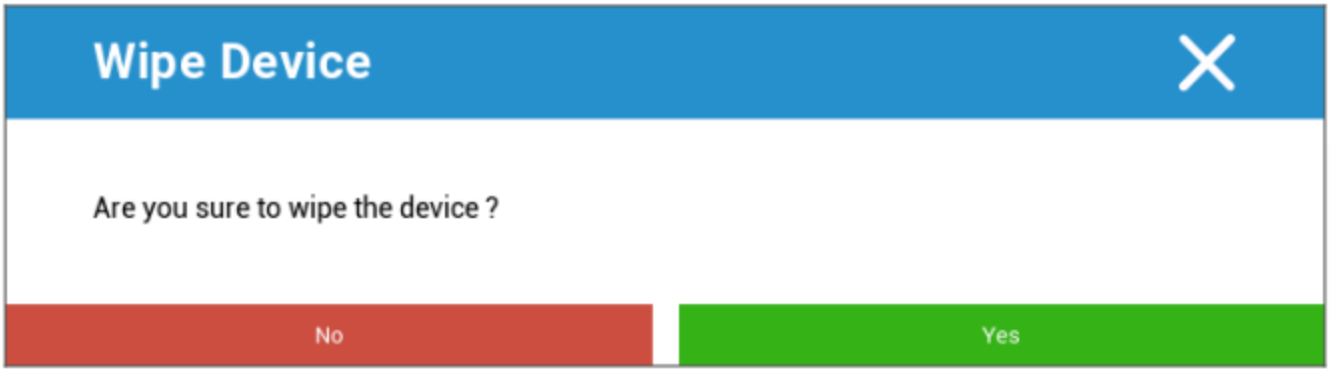
Fine vita (solo a livello di dispositivo)

Pulisci (solo a livello di dispositivo)

In "Pulisci" puoi ripristinare le impostazioni di fabbrica del dispositivo (solo con il Profilo di lavoro avanzato).

In questo caso i dati aziendali e privati verranno eliminati sul dispositivo dell'utente finale.

Cliccando sul "simbolo del meno" riceverai il seguente messaggio:



Con "Sì" puoi eseguire la pulizia.

In "Wipe Report" possono essere visualizzati i seguenti elementi

Cancellata da	Storia di chi ha eseguito la pulizia
Data	Data
Stato	Stato (ad esempio, se il Wipe è stato eseguito con successo)

Impostazioni di restrizione

Restrizioni

Qui è possibile limitare e bloccare una serie di cose.

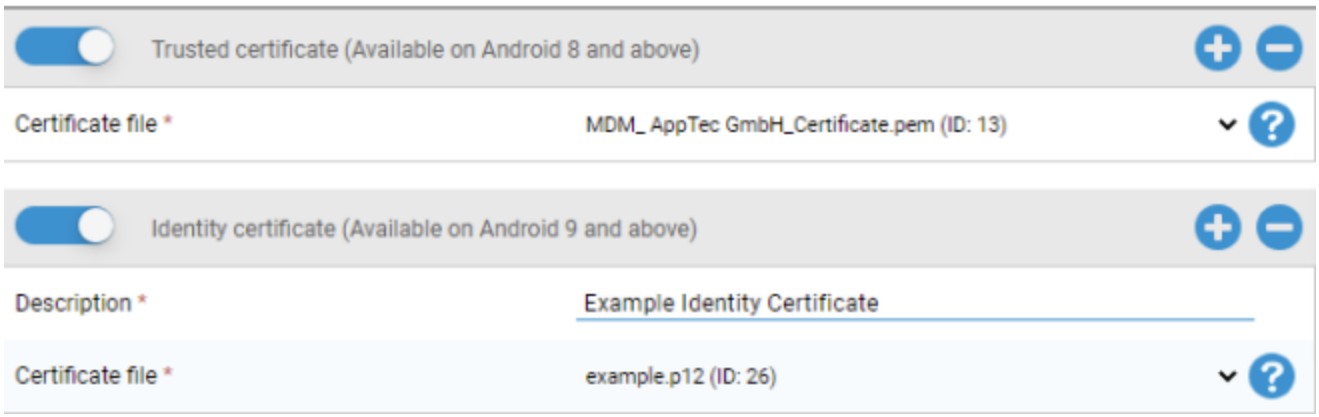
Applicazione della conformità	Modalità Prompt User - All'utente verrà richiesto di eseguire le azioni necessarie. Mode Lock-Down Container - Nasconde tutte le app fino a quando non vengono soddisfatti tutti i requisiti.
Politica dei permessi di runtime	Invita l'utente a richiedere nuovi permessi Accetta sempre le nuove richieste di permesso Rifiuta sempre le richieste di nuovi permessi Attenzione: Alcune applicazioni hanno problemi a riconoscere i permessi se questi sono impostati automaticamente. Se concedi sempre i permessi e riscontri problemi con le app che dicono che mancano i permessi, imposta questo parametro su "richiama l'utente" e reinstalla l'app.
Consenti gli appunti in uscita	Permette di copiare e incollare dall'interno del contenitore verso l'esterno
Consenti la risoluzione dell'ID chiamante	Mostra il nome di una chiamata in arrivo in base ai contatti presenti nel contenitore.
Consenti la risoluzione della ricerca dei contatti	Permette di cercare i nomi nei contatti del contenitore quando si effettua una chiamata.
Consenti la condivisione dei contatti Bluetooth	Permette di accedere al contatto con il contenitore in auto
Disconoscimento del raggio NFC in uscita	Disattiva l'NFC per il contenitore
Consenti fonti sconosciute	Se abilitata, gli utenti possono caricare le applicazioni in modalità sideload installando un file .apk.
Consenti il debug USB	Se abilitato, gli utenti possono attivare il Debug USB.
Disconoscimento della modifica dell'account	Disabilita la creazione, l'eliminazione e la modifica degli account nel contenitore. Tieni presente che alcune applicazioni necessitano di creare o modificare gli account per funzionare come previsto.

Restrizioni del profilo lavorativo. Disponibile solo su dispositivi Android 11 e successivi, con Profilo di lavoro avanzato	
Disconoscimento della fotocamera	Specifica se la telecamera non è consentita nel profilo di lavoro.
Disabilita il Bluetooth	Specifica se il bluetooth non è consentito nel profilo di lavoro.
Abilita la protezione del ripristino di fabbrica	Attiva questa opzione per annullare la protezione dal reset di fabbrica di Android all'account Google che hai definito in "Impostazioni generali" → "Configurazione Android" → "Android Enterprise" → "Protezione dal reset di fabbrica" Se questa opzione è attivata e resetti il dispositivo, dovrai fornire l'account Google configurato per configurare nuovamente il dispositivo.
Controllo dell'aggiornamento del sistema operativo	Attiva questa opzione per impostare il comportamento dell'aggiornamento in automatico, in finestra o posticipato.
Aggiornamento della politica	Automatico: Installa automaticamente non appena è disponibile un aggiornamento. A finestra: Si installa automaticamente all'interno di una finestra di manutenzione giornaliera. Questo configura anche l'aggiornamento delle app Play all'interno della finestra. Questa procedura è fortemente consigliata per i dispositivi kiosk perché è l'unico modo in cui le app persistentemente appuntate in primo piano possono essere aggiornate da Play. Posticipa: Posticipa l'installazione automatica fino a un massimo di 30 giorni.

Restrizioni del profilo personale. Disponibile solo su dispositivi Android 11 e successivi, con Profilo di lavoro avanzato	
Disconoscimento della fotocamera	Specifica se la fotocamera non è consentita nel profilo personale.
Disabilita il Bluetooth	Specifica se il bluetooth non è consentito nel profilo personale.
Consenti fonti sconosciute	Se abilitato, gli utenti del profilo di lavoro possono caricare le applicazioni in modalità sideload installando un file .apk.

Gestione dei certificati

Qui puoi distribuire Certificati di fiducia e Certificati di identità ai tuoi dispositivi. Android 8 o superiore è necessario per distribuire Certificati di fiducia e Android 9 o superiore per distribuire Certificati di identità.



Con il "+" puoi aggiungere più certificati.

I certificati di fiducia devono essere in formato PEM.

I certificati di identità devono essere in formato PKCS12.

Gestione delle connessioni

Wifi

Per questa impostazione, esegui la preconfigurazione dei dispositivi dell'utente finale, per l'accesso all'Accesso interno
Punti

Identificatore del set di servizi (SSID)	SSID per la rete da collegare
Rete nascosta	Attiva, nel caso in cui l'AP non trasmetta il SSID

Tipo di sicurezza

Stabilire il tipo di sicurezza dell'AP

WEP

Password	Password per l'AP

WPA/WPA2

Password	Password per l'AP

802.1x EAP

Metodo EAP

PWD	Identità	Identità
	Password	Password

PEAP	Protocollo di autenticazione di fase 2	nessuno	Nessun protocollo aggiuntivo
		MSCHAPV2	Protocollo MSCHAPV2
		GTC	Protocollo GTC
	Certificato CA	Certificato CA	
	Identità	Identità	
	Identità anonima	Identità anonima	
	Password	Password	

TTLS	Protocollo di autenticazione di fase 2	nessuno	Nessun protocollo aggiuntivo
		PAP	Protocollo PAP
		MSCHAP	Protocollo MSCHAP
		MSCHAPV2	Protocollo MSCHAPV2
		GTC	Protocollo GTC
	Certificato CA	Certificato CA	
	Identità	Identità	
	Identità anonima	Identità anonima	
	Password	Password	

TLS	Certificato CA	Certificato CA
	Identità	Identità
	Password	Password

VPN

Nome della connessione	Nome della connessione VPN

Tipo di VPN

VPN

Client VPN

Cliente VPN AppTec	
Configurazione del gateway	Seleziona la configurazione del Gateway VPN (vedi **Impostazioni generali > Gateway universale > Impostazioni VPN**).
VPN sempre attiva	Abilita il blocco nativo
Abilita il blocco di AppTec	Abilita il blocco di AppTec

Integrato (disponibile solo sui dispositivi Samsung)			
Tipo di connessione	PPTP	Server	Server
		Abilita la crittografia PPTP	Abilita la crittografia PPTP
	L2TP / IPSec PSK	Server	Server
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Abilita il segreto L2TP	Abilita il segreto L2TP
		Segreto L2TP	Segreto L2TP
	IPSec XAuth PSK	Server	Server
		Identificatore IPSec	Identificatore IPSec
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
Ricerca DNS Domini	Ricerca DNS Domini		
Impostazioni dell'esperto	Server DNS	Server DNS	
	Percorsi di inoltro	Percorsi di inoltro	

Aprire una VPN		
Server	Server	
Profilo OpenVPN	Profilo OpenVPN	
App OpenVPN	OpenVPN per Android (consigliato)	
	Connetti OpenVPN	
Impostazioni dell'esperto	Server DNS	Server DNS
	Percorsi di inoltro	Percorsi di inoltro

Samsung / Cigno forte			
Tipo di connessione	PPTP	Server	Server
		Nome utente	Nome utente
		Password	Password
		Abilita la crittografia PPTP	Abilita la crittografia PPTP
	L2TP / IPSec PSK	Server	Server
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
		Abilita il segreto L2TP	Segreto L2TP
	IPSec XAuth PSK	Server	Server
		Identificatore IPSec	Identificatore IPSec
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
Impostazioni dell'esperto	Server DNS	Server DNS	
	Percorsi di inoltro	Percorsi di inoltro	

Cisco Any Connect		
Server	Server	
Modalità certificato	Disabili	Disabili
	Automatico	Automatico
Impostazioni dell'esperto	Server DNS	Server DNS
	Percorsi di inoltro	Percorsi di inoltro

VPN per app

Client VPN

Cliente VPN AppTec		
Configurazione del gateway	Seleziona la configurazione del Gateway VPN (vedi **Impostazioni generali > Gateway universale > Impostazioni VPN**).	
Applicazioni VPN	Applicazioni VPN	
VPN sempre attiva	Abilita il blocco nativo	VPN sempre attiva
Abilita il blocco di AppTec	Abilita il blocco di AppTec	

Samsung / Cigno forte			
Tipo di connessione	PPTP	Server	Server
		Applicazioni VPN	Applicazioni VPN
		Nome utente	Nome utente
		Password	Password
		Abilita la crittografia PPTP	Abilita la crittografia PPTP
	L2TP / IPSec PSK	Server	Server
		Applicazioni VPN	Applicazioni VPN
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
		Abilita il segreto L2TP	Segreto L2TP
	IPSec XAuth PSK	Server	Server
		Applicazioni VPN	Applicazioni VPN
		Identificatore IPSec	Identificatore IPSec
		Chiave precondivisa IPSec	Chiave precondivisa IPSec
		Nome utente	Nome utente
		Password	Password
Impostazioni dell'esperto	Server DNS	Server DNS	
	Percorsi di inoltro	Percorsi di inoltro	

Restrizioni

Qui puoi impostare le restrizioni, in relazione alla gestione delle connessioni

Consenti il roaming dei dati	Consenti i dati mobili in roaming
Forza il roaming dei dati	Se attivato, il roaming per i dati mobili viene attivato in modo permanente (non è consigliato!). Questa impostazione sovrascrive l'impostazione "Consenti roaming dati"!
Usa il server proxy http del sistema	L'utilizzo di un server proxy HTTP, fornito dalle impostazioni del sistema nelle impostazioni, dipende dalla rete connessa (WiFi o APN).

Gestione del PIM

Scambio Gmail

Info: Questa configurazione verrà applicata all'applicazione Gmail. Quindi devi approvare e installare Gmail.

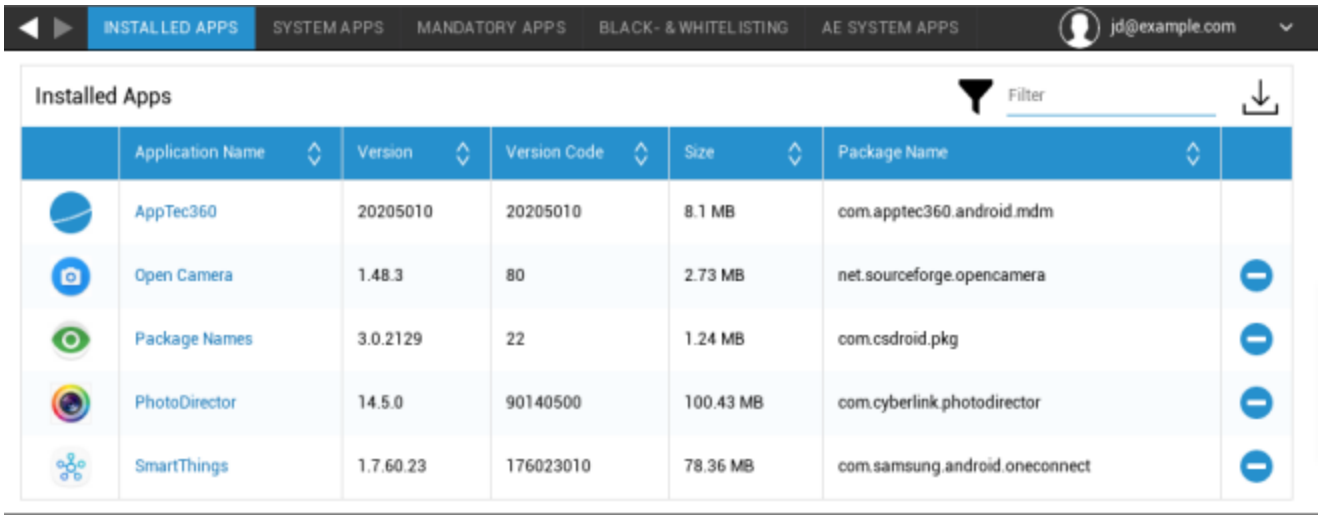
Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Con un clic potrai visualizzarle tu stesso
Nome host del server	Indirizzo del server di Exchange
Nome utente	Il nome di accesso per il rispettivo dispositivo dell'utente finale, si prega di notare anche i "Segnaposto qui".
Firma	È possibile allegare una firma (Suggerimento: alcuni dispositivi richiedono la formattazione HTML per la firma).
Numero di giorni precedenti da sincronizzare	Numero di giorni che determinano il momento in cui le email vengono sincronizzate di nuovo
Identificatore del dispositivo	Una stringa che contiene l'EAS DeviceID. Questo è un elemento del protocollo EAS e deve essere utilizzato in alcuni paesi.
Utilizza il Secure Sockets Layer (SSL)	Usa una connessione SSL
Accetta tutti i certificati	Sono accettati tutti i certificati. Seleziona questa opzione se il tuo Exchange Server utilizza un certificato autofirmato.
Consenti gli account non gestiti	Consente agli utenti di aggiungere o rimuovere qualsiasi account di Exchange, oltre a quello specificato in questa configurazione gestita. Se questa impostazione è attivata, non puoi impedire agli utenti di aggiungere altri account Exchange a Gmail. Inoltre non puoi controllare la condivisione dei dati tra le altre app e gli account Exchange aggiunti dagli utenti. Questa impostazione deve essere attivata solo se i tuoi utenti devono mantenere più di un account Exchange di lavoro in Gmail.
Certificato del cliente	Certificato del cliente. È necessario solo se il tuo server di posta si aspetta che sia presente.

Gestione delle app

Enterprise App Manager

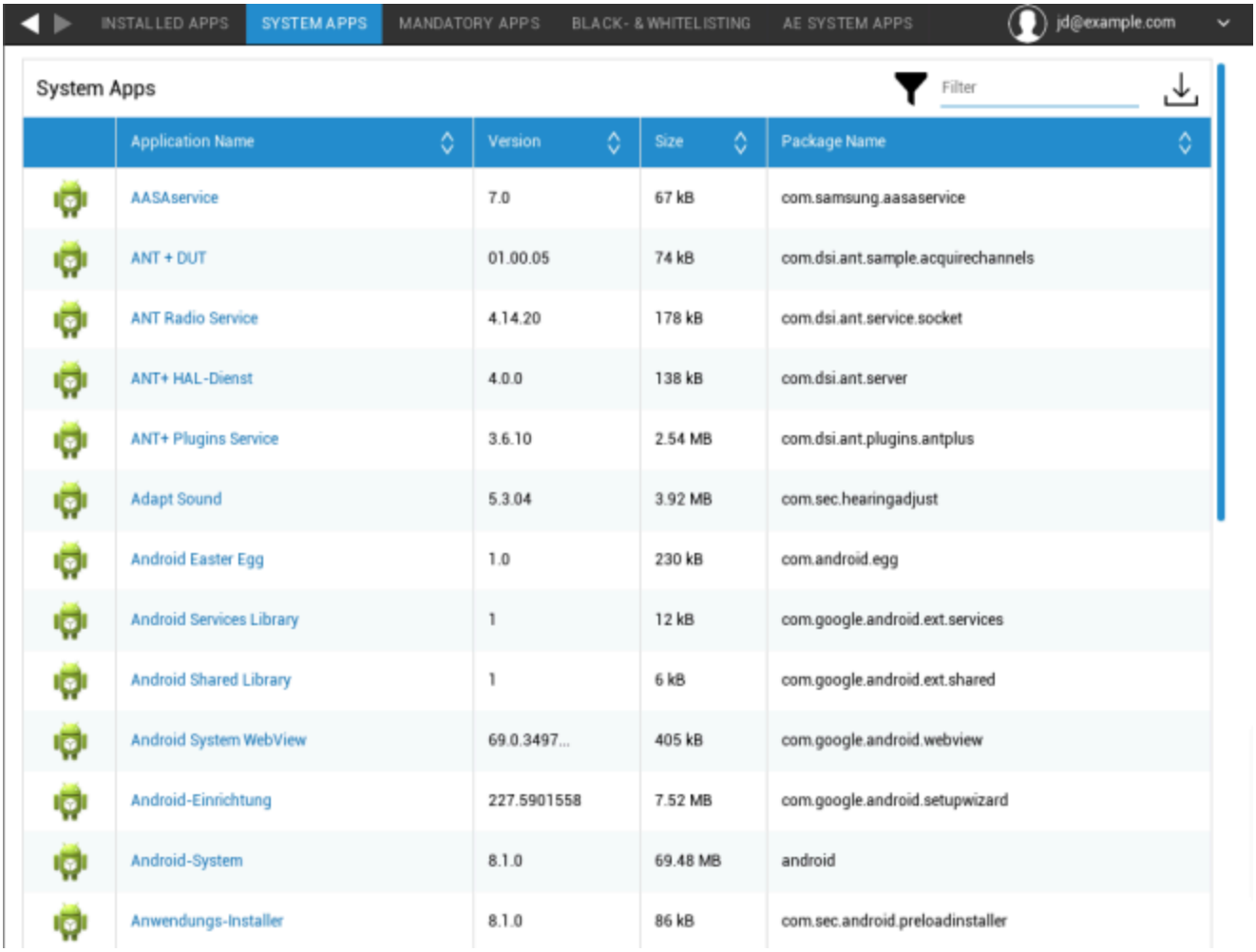
Applicazioni installate (solo a livello di dispositivo)

Qui verranno visualizzate tutte le applicazioni attualmente installate nel contenitore.



App di sistema (solo a livello di dispositivo)

Sotto la voce "App di sistema" sono elencate tutte le applicazioni e i servizi che sono già stati installati sul dispositivo dell'utente finale dal produttore del dispositivo.

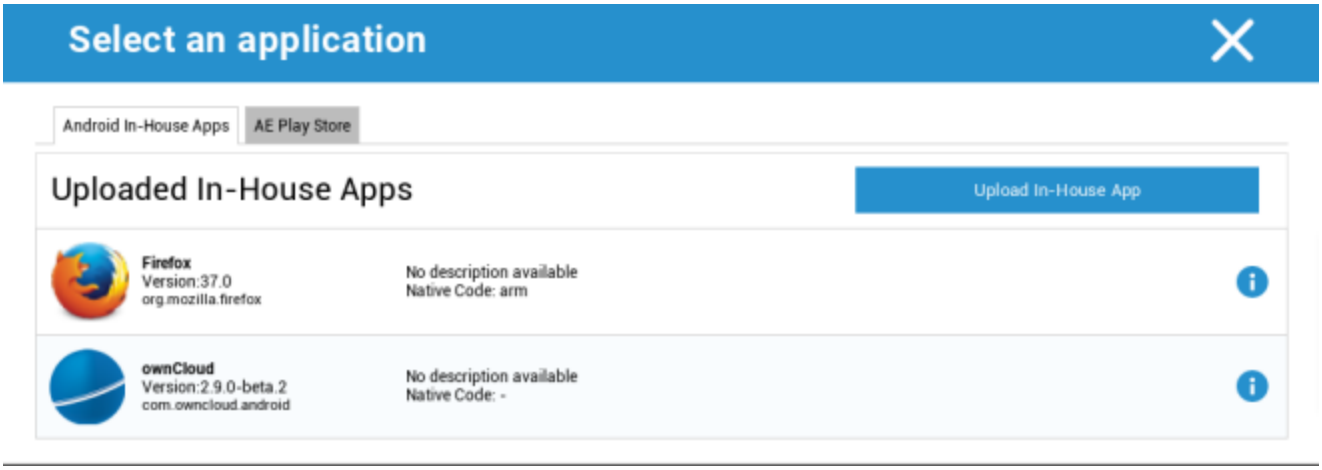


Applicazioni obbligatorie

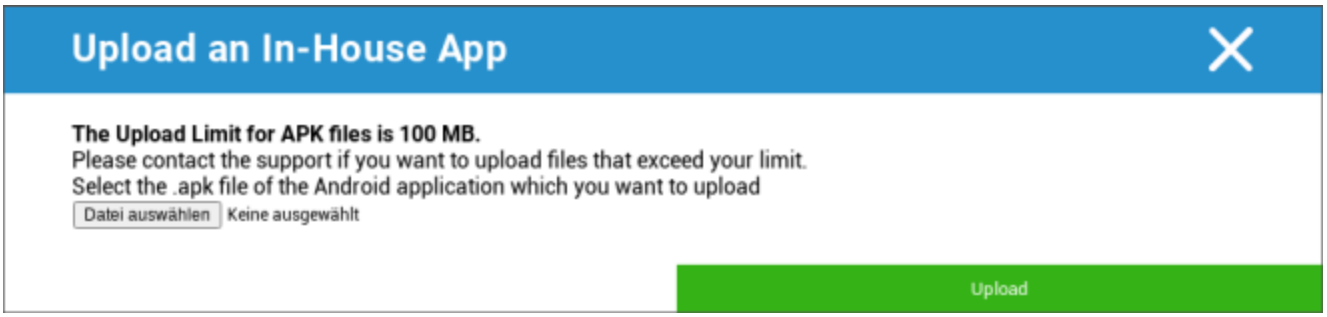
Nella sezione Applicazioni obbligatorie, puoi stabilire le applicazioni obbligatorie. All'utente verrà continuamente richiesto di installare l'applicazione designata, se si tratta di un'applicazione InHouse. Le app del Play Store verranno installate automaticamente.

Tramite l'opzione , è possibile definire l'applicazione obbligatoria.

Può trattarsi di un'applicazione interna tra le "Applicazioni interne Android" che hai caricato nelle Impostazioni generali.

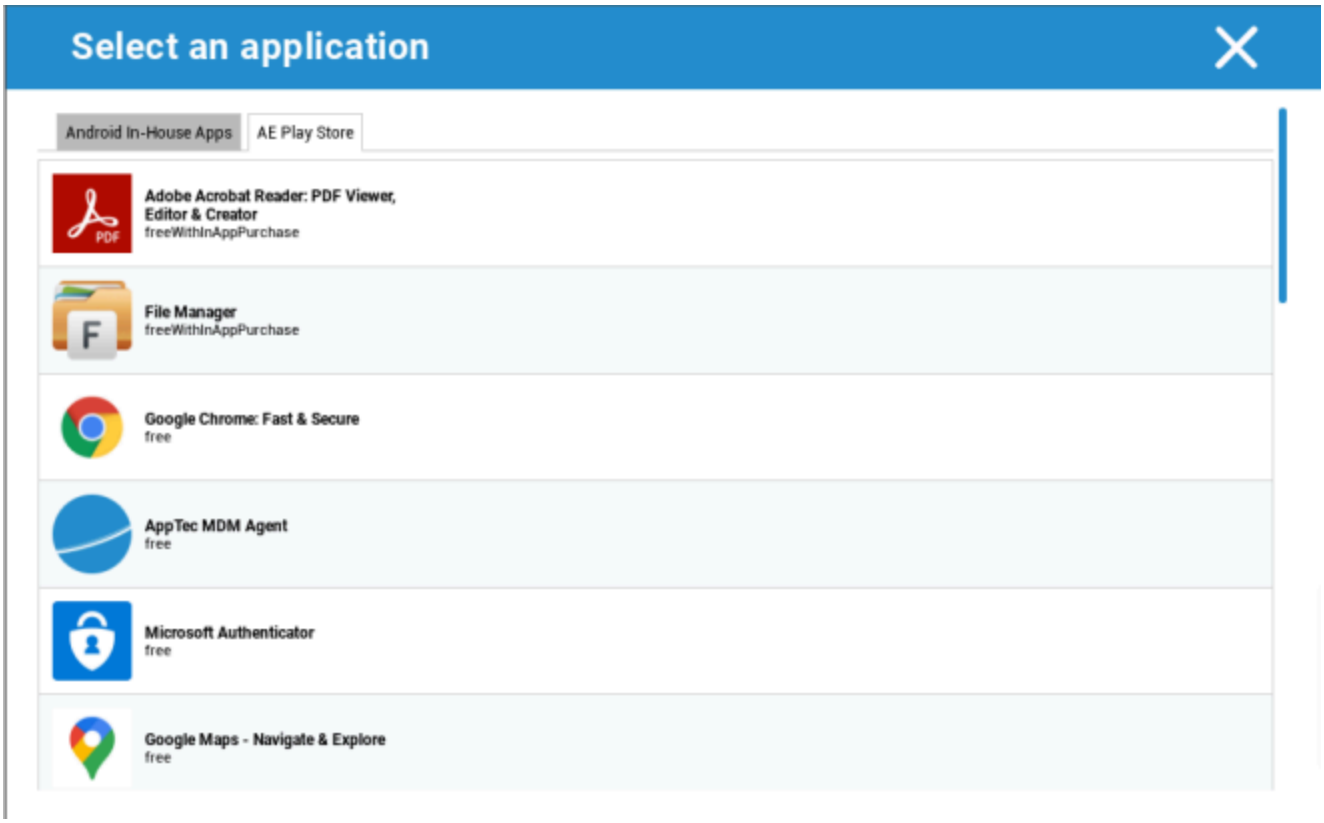


Puoi anche selezionare e caricare direttamente un file apk con "Upload In-House App".



Se stai installando un'App In-House, avrai la possibilità di attivare la funzione "Tieni aggiornato". Se l'opzione è attivata e hai definito una versione più recente nel DB delle app in-house, l'app verrà aggiornata sul dispositivo.

Oppure può essere un'applicazione "AE Play Store" dal Google Work Play Store.



In questa scheda verranno visualizzate solo le "App AE Play Store" approvate.

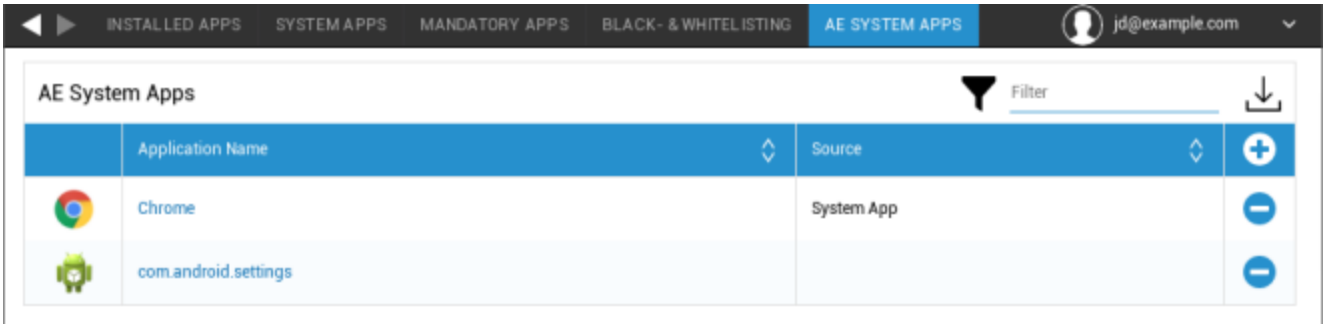
Per approvare un'applicazione "AE Play Store" vai in "Impostazioni generali" > "Gestione app" > "AE Play

Store" e aggiungi un'applicazione tramite il pulsante che ti reindirizzerà alla scheda "Play Store Apps" (oppure puoi andare direttamente alla scheda "Play Store Apps").

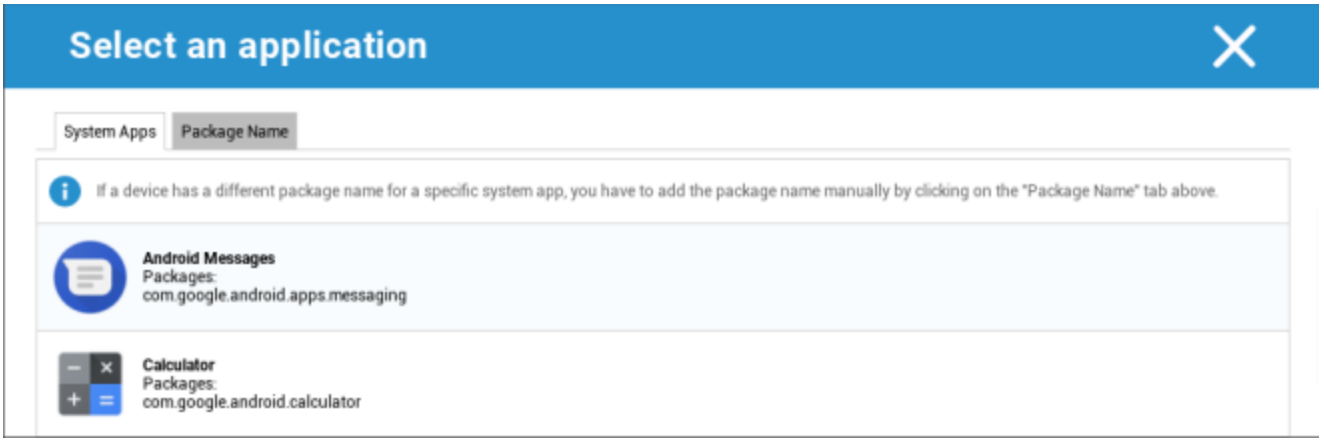
Nella scheda "Play Store Apps" puoi cercare le applicazioni. Quando clicchi su un'applicazione, si apre la pagina dell'applicazione e qui puoi approvare l'applicazione cliccando su "Approva".

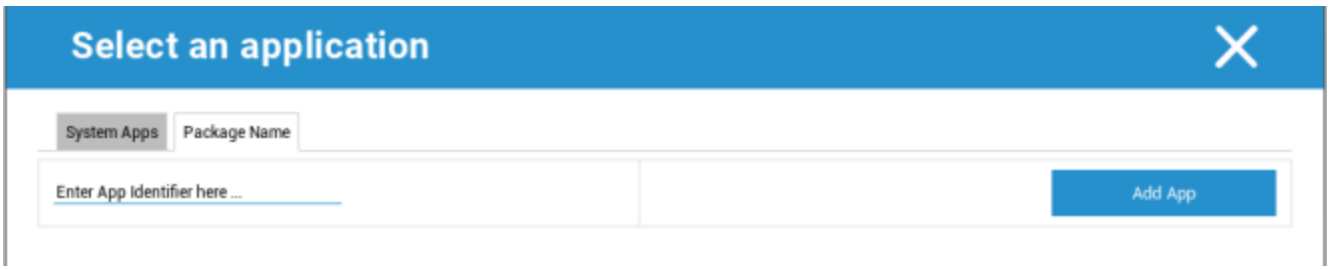
Applicazioni del sistema AE

Qui puoi definire un elenco contenente specifiche app di sistema che devono essere attivate sui dispositivi.



Se fai clic sul pulsante, puoi scegliere da un elenco di possibili app di sistema fornite da Google o inserire direttamente il nome del pacchetto di un'app di sistema da attivare.





Tieni presente che le app di sistema nell'elenco fornito da Google sono solo app che possono essere app di sistema, ma non devono necessariamente essere app di sistema sui tuoi dispositivi.

Tuttavia, questo elenco riguarda solo le app già preinstallate.

L'aggiunta di app che non sono preinstallate sui tuoi dispositivi non avrà alcun effetto sui tuoi dispositivi, indipendentemente dal fatto che l'app provenga dall'elenco fornito da Google o che il nome del pacchetto dell'app venga inserito direttamente.

Restrizioni e impostazioni

Impostazioni di gestione delle app

Qui puoi configurare il comportamento del dispositivo per quanto riguarda gli aggiornamenti delle app.

Frequenza di controllo degli aggiornamenti	Specifica in quale intervallo il client AppTec cercherà gli aggiornamenti delle applicazioni. Il valore predefinito è 24 ore.
Soglia Wi-Fi	Le app di dimensioni superiori a quelle specificate verranno scaricate tramite Wi-Fi. Se si seleziona "Solo Wi-Fi", tutte le app verranno scaricate tramite Wi-Fi.

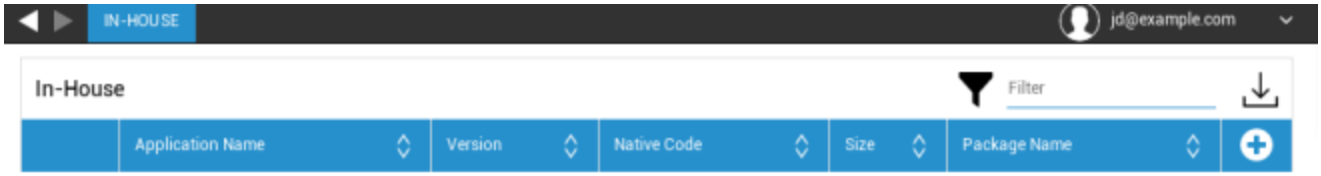
App Store aziendale

In-house

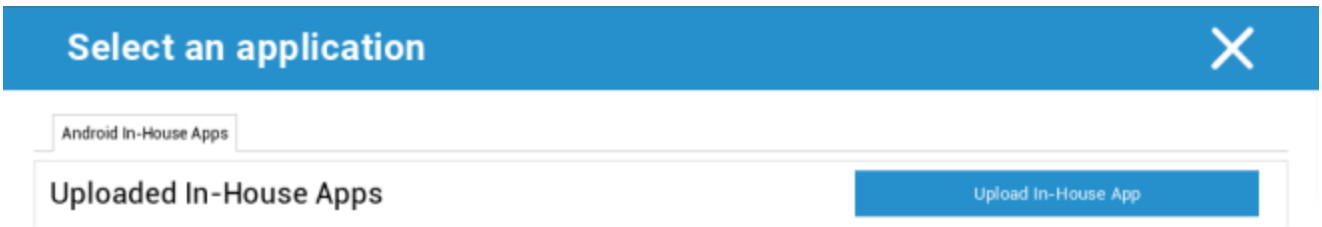
Al punto "In-House", puoi caricare e distribuire le app sviluppate internamente.

Con il simbolo puoi distribuire altre App In-House.

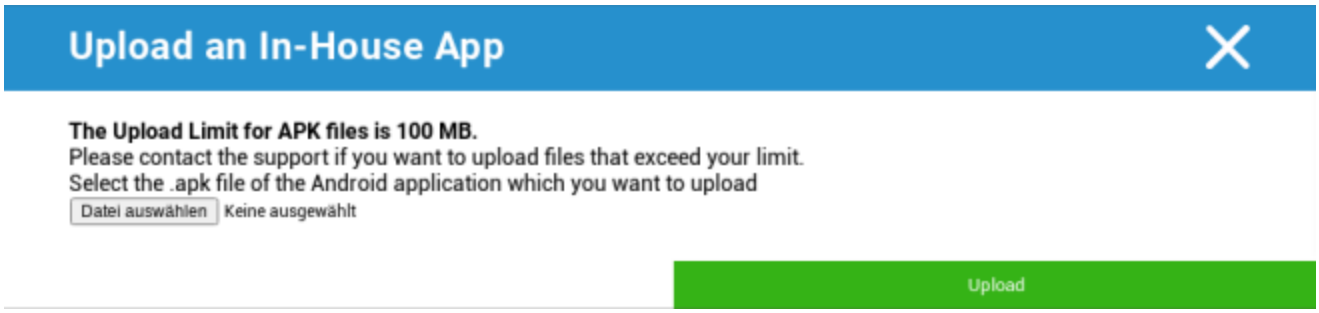
Se stai installando un'App In-House, avrai la possibilità di attivare la funzione "Tieni aggiornato". Se l'opzione è attivata e hai definito una versione più recente nel DB delle app in-house, l'app verrà aggiornata sul dispositivo.



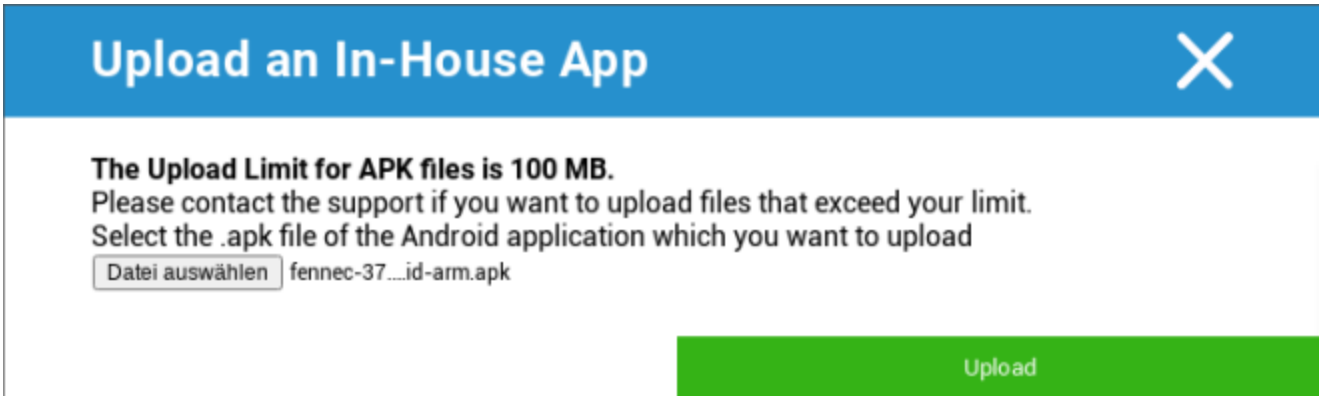
Se non hai distribuito App In-House, riceverai la seguente panoramica:



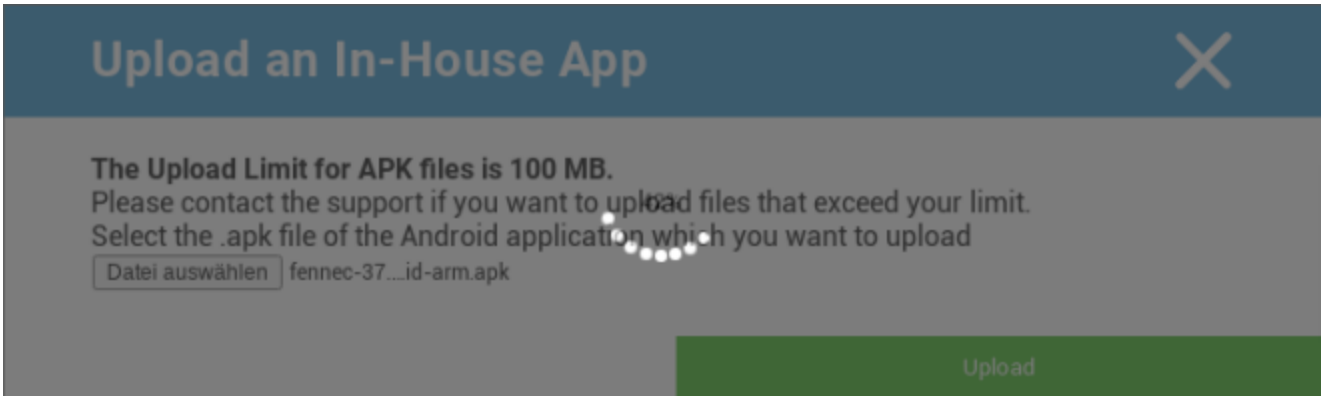
A tal fine, clicca su "Upload In-House App" e riceverai la seguente panoramica:



Ora scegli con "Cerca..." un file .apk e poi clicca su "Carica".



La tua applicazione sarà ora caricata; al centro del cerchio vedrai un indicatore di percentuale che mostra la quantità di app già caricata.



Se il caricamento della tua App In-House è andato a buon fine, potrai trovare l'applicazione caricata nel tuo Catalogo delle App.

L'utente ha ora la possibilità di vedere e installare questa applicazione nell'AppTec Store sul dispositivo dell'utente finale, sotto la categoria "In-House".

Poiché non si tratta di un'applicazione Google PlayStore, l'utente non ha bisogno di un ID Google memorizzato sul proprio dispositivo finale.

Play Store aziendale

AE Play Store

Qui puoi aggiungere applicazioni al Playstore di Android Enterprise. Ricorda che devi approvare le applicazioni con il tuo account di amministratore AE prima di poterle aggiungere.

Per approvare un'applicazione, consulta le istruzioni riportate nella sezione Applicazioni obbligatorie.

Gestione dei contenuti

ContentBox

Qui puoi attivare il ContentBox.

Non appena si imposta "Abilita ContentBox" su "On", un'applicazione ContentBox separata verrà installata automaticamente sul dispositivo dell'utente finale.

Browser sicuro

Qui puoi configurare le impostazioni di AppTec Secure Browser.

Non appena la sezione "Browser sicuro" viene impostata su "On", sul dispositivo dell'utente finale verrà installata automaticamente un'applicazione Browser separata.

Richiedi la password	Richiedere all'utente di impostare e utilizzare una password per accedere al browser.
Lunghezza minima richiesta per la password	Imposta il numero di caratteri richiesto per la password
Qualità della password richiesta	Imposta la qualità della password richiesta
Limita i download / Apri in	
Limitare i caricamenti	
Carica la Whitelist	Un elenco di URL per i quali il caricamento sarà sempre consentito.
Consenti la copia	Consente di copiare, tagliare o condividere il testo all'interno delle pagine web.
Consenti la cattura dello schermo	Consente di catturare screenshot.
Frequenza di pulizia dei dati	Seleziona con quale frequenza TUTTI i dati dell'utente (cronologia, cache, ecc.) devono essere rimossi automaticamente.
Segnalibri aziendali	I segnalibri verranno visualizzati nella cartella "segnalibri aziendali" dei segnalibri del browser. Non sono modificabili dall'utente.
Nascondi la barra degli indirizzi	
Whitelisting nel browser (senza Universal Gateway)	Abilita la whitelist degli URL lato client. • I segnalibri aziendali sono sempre inseriti nella whitelist • Supportato solo per 100 URL • Utilizza il Gateway Universale per un Black- e Whitelisting illimitato.
URL inseriti nella whitelist	Un elenco di URL consentiti.

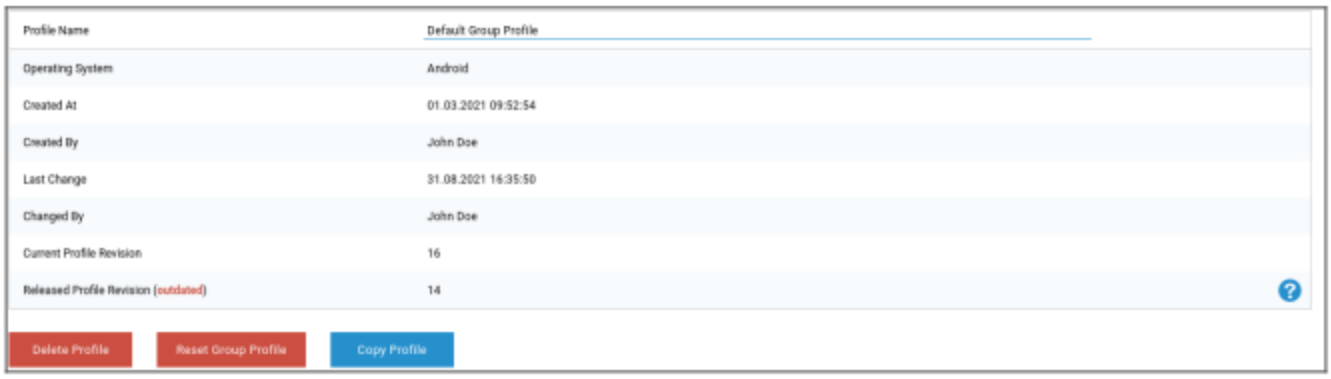
Black- e Whitelist basati su gateway	La lista nera ha i seguenti requisiti: • Un AppTec Universal Gateway funzionante ("Impostazioni generali" → "Universal Gateway") • Una configurazione VPN funzionante con un server DNS specificato ("Impostazioni generali" → "Gateway universale" → "Impostazioni VPN") • Configurazione della lista nera ("Impostazioni generali" → "Universal Gateway" → "Lista nera dei domini") • Una connessione VPN valida nel profilo ("Gestione connessioni" → "VPN")

Configurazione Android

Generale

Panoramica del profilo del gruppo (solo a livello di gruppo)

Quando apri il profilo di un gruppo, otterrai una rapida panoramica del profilo.



Nome del profilo	Nome del profilo (può essere modificato qui)
Sistema operativo	Sistema operativo per cui è stato creato il profilo
Creato a	Tempo della creazione
Creato da	Il creatore del profilo
Ultimo cambiamento	Ora dell'ultima modifica al profilo
Modificato da	Account che ha apportato le ultime modifiche
Revisione del profilo attuale	Revisione dello stato del profilo salvato
Revisione del profilo rilasciata	Revisione del profilo assegnata ("Assegna ora"). Se l'etichetta mostra " (outdated)" dietro il testo, significa che hai salvato il profilo ma non l'hai ancora assegnato, quindi i dispositivi riceveranno ancora la versione più vecchia.

Panoramica del dispositivo (solo a livello di dispositivo)

Se ti trovi su un dispositivo, riceverai un riepilogo del dispositivo selezionato:

Nome del dispositivo	Nome del dispositivo
Ultima posizione conosciuta	Le ultime coordinate GPS conosciute
Numero di telefono	Numero di telefono
Applicazioni obbligatorie assegnate	Il numero di app obbligatorie assegnate
Versione OS	Versione del sistema operativo del dispositivo
Sistema operativo	Sistema operativo (Android / iOS / Windows Phone)
Numero di serie	Numero di serie del dispositivo
Proprietà del dispositivo	Dispositivo aziendale o privato
Tipo di dispositivo	Telefono o tablet
Radicati	Stato, che indica se il dispositivo è stato sottoposto a rooting
Conforme	Conformi alle linee guida
Indirizzo IP	Indirizzo IP
Ultimo visto	Momento in cui il dispositivo si è connesso per l'ultima volta ad AppTec.
Ultima spinta	Punto nel tempo, quando il server ha inviato un push al dispositivo
Assegnazione dell'utente	Una tendina per assegnare il dispositivo a un altro utente

Revisione della configurazione (solo a livello di dispositivo)

Qui potrai vedere quale profilo di gruppo è stato assegnato al dispositivo.

Se clicchi sul profilo del gruppo, accederai direttamente al profilo e potrai eseguire le impostazioni.

Con il simbolo, puoi riportare le app assegnate alle impostazioni del profilo del gruppo.

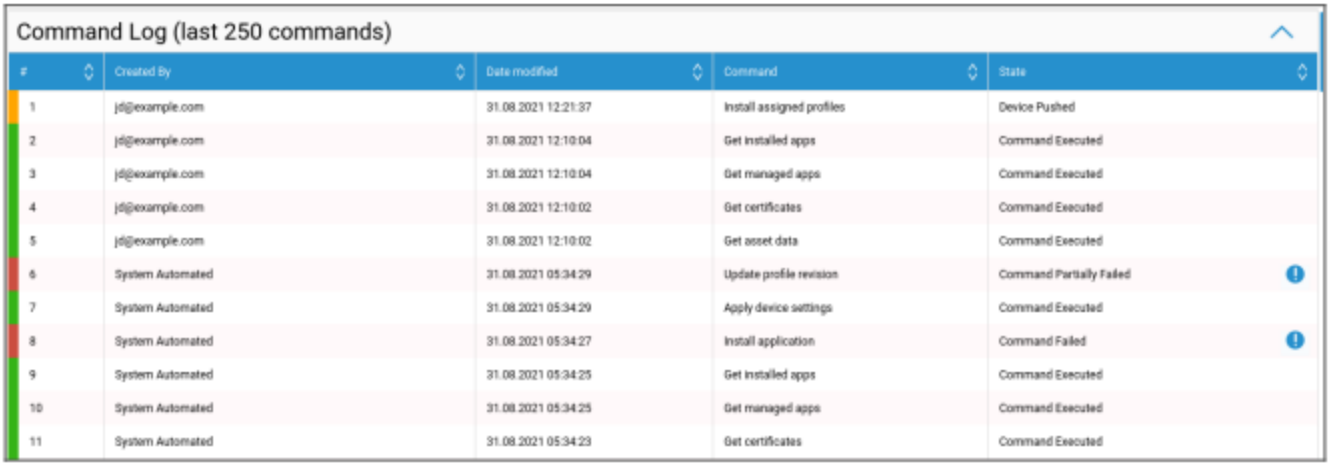
Con il simbolo, puoi reimpostare il profilo del dispositivo in modo che non abbia alcuna impostazione.

L'indicazione "Revisione più recente disponibile" indica che il profilo del gruppo è stato modificato e salvato ma non assegnato. Il profilo del gruppo deve essere assegnato con "Assegna ora" a livello di gruppo per applicare le modifiche ai dispositivi.

Registro del dispositivo (solo a livello di dispositivo)

Registro dei comandi

Qui puoi vedere quali comandi sono stati emessi per il dispositivo e qual è il loro stato.



I comandi creati da "Sistema automatico" vengono creati automaticamente dal sistema.

Possibili stati del comando

Dispositivo spinto	È stata inviata una richiesta push al servizio push (ad esempio APNS) per indicare al dispositivo di connettersi nuovamente al server EMM.
Comando creato	Il comando è stato creato nel sistema.
Comando inviato	Il comando è stato inviato al dispositivo dopo la connessione al server.
Comando eseguito	Il comando è stato eseguito con successo.
Comando fallito	Il comando è fallito. *
Comando parzialmente fallito	A seconda del sistema operativo del dispositivo, alcuni comandi possono essere raggruppati. In questo caso alcune parti di questo gruppo di comandi sono fallite. *
Comando eseguito, alla fine fallito	Il comando è stato eseguito ma forse non lo è stato.
Comando Riportato	Il comando è stato ripreso da un utente.
Scartato	Il comando è stato scartato. Ad esempio perché è stato sostituito da un altro comando o perché il dispositivo è stato reinserito e i vecchi comandi sono stati rimossi.

*Se dietro il messaggio c'è un punto esclamativo, puoi ottenere maggiori informazioni passando il cursore sull'icona.

Impostazioni del dispositivo

Configurazione del cliente

Qui puoi eseguire le seguenti configurazioni sul tuo dispositivo Android:

Messaggio di avviso dopo aver disabilitato Gestione dispositivi	Messaggio di avviso stabilito dopo la disattivazione di Gestione dispositivi
Tempo di non conformità	Limite di tempo dopo il quale verrà eseguita l'"Azione esecutiva dopo la conformità", se il dispositivo non è conforme. Min. 1 minuto Max. 24 ore
Azione esecutiva dopo il timeout di conformità	L'azione da intraprendere non appena un dispositivo diventa non conforme. • non fare nulla = non agire • Dispositivo di blocco = dispositivo di blocco • Wipe Device = il dispositivo verrà ripristinato alle impostazioni di fabbrica.
Frequenza di raccolta dei dati	Frequenza con cui raccogliere le informazioni sul dispositivo/GPS
Frequenza del battito cardiaco del dispositivo	Intervallo di tempo in cui il dispositivo deve contattare il server AppTec360 Min. 1 minuto Max. 24 ore
Abilita gli aggiornamenti della posizione	Se attivato, il dispositivo invia aggiornamenti sulla posizione al server AppTec360.
Posizione Ora di aggiornamento	Determina in quali intervalli di tempo il dispositivo invia ad AppTec gli aggiornamenti sulla posizione.
Usa Google Location Accuracy per l'aggiornamento della posizione	Se attivata, la precisione della localizzazione di Google (precedentemente nota come localizzazione di rete) verrà utilizzata per gli aggiornamenti della posizione (se è stata disattivata in "Restrizioni", questa impostazione non avrà alcun effetto).
Usa la posizione GPS per l'aggiornamento della	Se attivato, il GPS verrà utilizzato per gli aggiornamenti sulla posizione.

posizione	
Consenti le posizioni fittizie (false)	Consente di falsificare le informazioni sulla posizione tramite applicazioni di terze parti
Azione di perdita della connessione	Permette di impostare una determinata azione che verrà eseguita dopo un certo numero di battiti cardiaci falliti
Modalità di applicazione dei criteri	Definisce il grado di aggressività con cui il client AppTec360 chiede all'utente di eseguire determinate azioni che richiedono l'input dell'utente. Intervallo (Predefinito) = chiede a intervalli, in modo che l'utente possa metterlo in secondo piano per un po' di tempo. Nessun avviso = nessun popup per qualsiasi interazione richiesta. Devi aprire manualmente il client AppTec360 per verificare se c'è un'azione richiesta. Avviso costante = L'utente può eseguire solo l'azione richiesta. Il client AppTec360 si posiziona in primo piano se l'utente cerca di evitarlo.
Blocco della versione di AppTec360	Ti permette di definire una versione del client AppTec360 che è la versione massima a cui il client si aggiorna.

Carta da parati

Qui puoi definire uno sfondo personalizzato.

"Specifica un colore" ti permette di definire un colore in formato esadecimale (ad esempio #000000). Sono ammessi solo valori esadecimali.

"Imposta immagine come sfondo" ti permette di caricare un'immagine. Tieni presente che dispositivi diversi con launcher e versioni del sistema operativo differenti funzionano in modo diverso. Non esiste una linea guida generale per le dimensioni e il rapporto, poiché dipende dal dispositivo.

Usa JPG (o JPEG) o PNG per il formato del file.

Gestione delle risorse (solo a livello di dispositivo)

Gestione delle attività

Info sul dispositivo

Modello	**Denominazione del modello del dispositivo**
Sistema operativo	OS
Versione OS	Versione del sistema operativo
Supporto AE	Supporto per Android Enterprise (Container e completamente gestito)
Numero di serie	Numero di serie
Nome del dispositivo	Nome del dispositivo
Stato della batteria	Stato della batteria
Memoria libera / totale	Memoria libera / Totale
Samsung KNOX	Livello API di Samsung KNOX
Scheda SD disponibile	Scheda SD disponibile
Scheda SD emulata	Scheda SD emulata
Scheda SD rimovibile	Scheda SD rimovibile
SD Memoria libera / Memoria totale	SD Libera / Memoria totale della scheda SD

Wi-Fi

Indirizzo IP	Indirizzo IP del dispositivo
WiFi MAC	Indirizzo MAC WiFi

Cellulare

Stato	Stato (scheda SIM installata)
Numero di telefono	Numero di telefono
Roaming (voce/dati)	Roaming per voce/dati
Stato del roaming	Stato attuale del roaming
Indirizzo IP	Indirizzo IP
Operatore/Vettore	Operatore/Vettore
Tecnologia cellulare	Tecnologia cellulare
IMEI	Numero IMEI
ICCID	Si tratta dell'ID della carta SIM, spesso anche Smartcard o Carta a Circuito Integrato (ICC).
IMSI	L'International Mobile Subscriber Identity (IMSI) fornisce nelle reti mobili GSM e UMTS un'identificazione precisa degli utenti della rete. L'IMSI è composto da un massimo di 15 cifre e viene configurato nel modo seguente: • Codice paese mobile (MCC), 3 cifre • Codice di rete mobile (MNC), 2 o 3 cifre • Numero di identificazione dell'abbonato mobile (MSIN), da 1 a 10 cifre
Attuale MCC/MNC	Vedere "SIM MCC/MNC"
SIM MCC/MNC	Il codice del paese mobile è un identificativo del paese stabilito dall'ITU secondo la norma E.212. Standard. Questo funziona insieme al Mobile Network Code (MNC) per l'identificazione della rete mobile. Ovvero il codice di rete nazionale/mobile della carta SIM. Se fai il roaming su un'altra rete mobile, logicamente il "Current MCC/MNC" e il "SIM MCC/MNC" saranno diversi.

Bluetooth

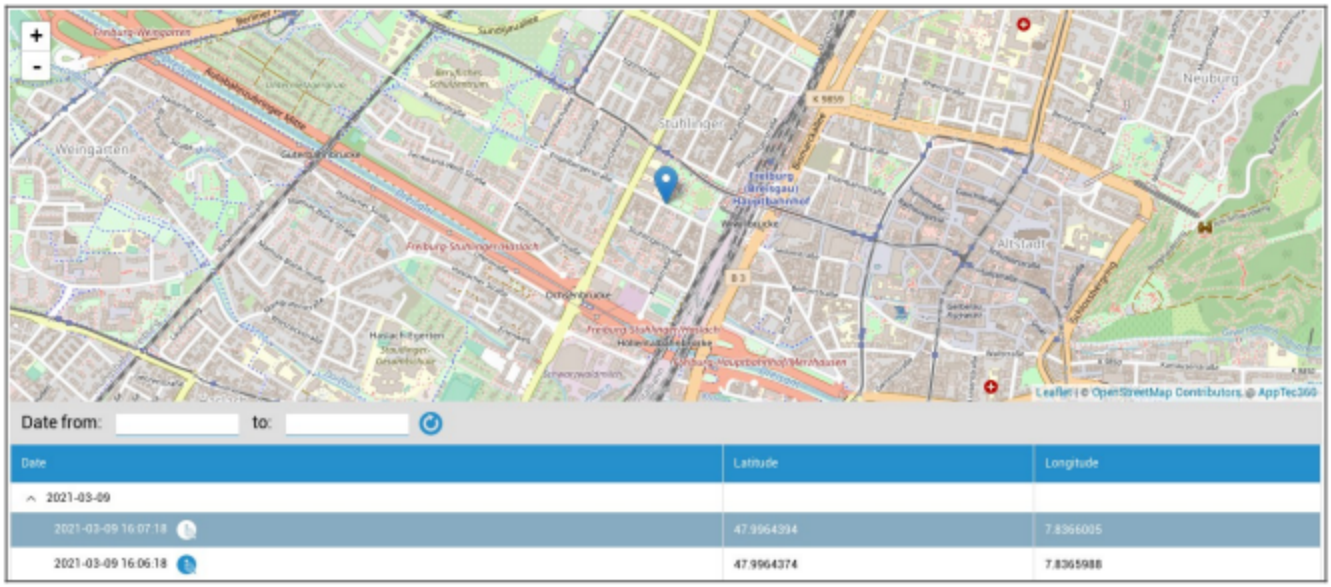
MAC Bluetooth	Indirizzo MAC Bluetooth

Gestione della sicurezza

Antifurto (solo a livello di dispositivo)

Informazioni GPS (solo a livello di dispositivo)

Qui puoi stabilire la posizione attuale/ultima del dispositivo. La localizzazione può essere protetta con una o anche due password - Vedi: Impostazioni generali - Privacy - Accesso GPS



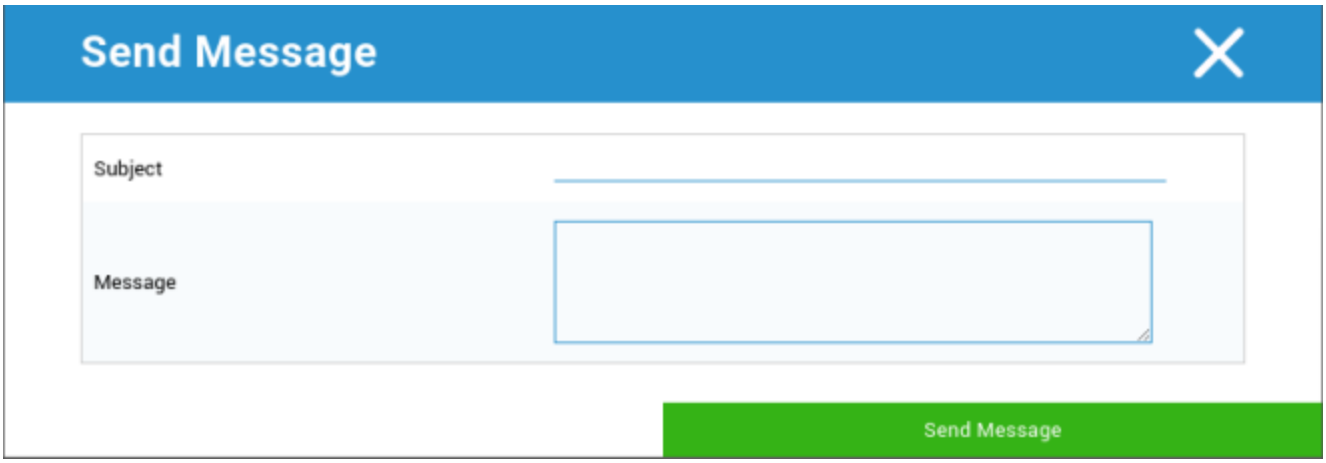
Pulisci e blocca (solo a livello di dispositivo)

Alla voce "Pulisci e blocca", puoi eseguire le seguenti tre azioni:

Pulizia completa	Il dispositivo viene riportato alle impostazioni di fabbrica (i dati aziendali e quelli personali vengono cancellati).
Pulizia aziendale	Solo i dati aziendali vengono rimossi dal dispositivo dell'utente finale (tutte le applicazioni, i dati, ecc. forniti da AppTec360).
Schermata di blocco	Il blocco dello schermo è attivato, è sufficiente sbloccare il dispositivo con la password/PIN del dispositivo.

Messaggio (solo a livello di dispositivo)

Puoi inserire l'oggetto e un messaggio e inviarlo a un dispositivo dell'utente finale. Questo messaggio verrà visualizzato nel client AppTec360.



Configurazione della sicurezza

Codice di accesso

Alla voce "Codice di accesso" puoi assegnare una password al dispositivo; sono disponibili le seguenti opzioni di impostazione

Lunghezza minima della password	Stabilisce il numero minimo di simboli che una password deve contenere
Qualità della password	Forza della password Non specificato = non specificato Ogni password è ok = ogni password è accettabile almeno caratteri numerici = deve contenere almeno caratteri numerici almeno caratteri complessi = deve contenere almeno caratteri speciali almeno caratteri alfanumerici = deve contenere almeno caratteri alfanumerici almeno caratteri alfabetici = deve contenere almeno caratteri alfabetici
Blocco del tempo massimo di inattività	Timeout massimo dello schermo. Questo configura solo il valore massimo che può essere selezionato dall'utente.
Lettere minuscole minime richieste nella password	Lettere minuscole minime richieste nella password
Lettere maiuscole minime richieste nella password	Lettere maiuscole minime richieste nella password
Caratteri non letterali minimi richiesti nella password	Caratteri non letterali minimi richiesti nella password
Cifre numeriche minime richieste nella password	Cifre numeriche minime richieste nella password
Simboli minimi richiesti nella password	Simboli minimi richiesti nella password
Timeout di scadenza della password	Stabilisce, dopo quale intervallo di tempo la password scade e deve essere emessa una nuova password.
Limitazione della cronologia delle password	Numero di password precedentemente utilizzate che non sono consentite
Massimo di tentativi di password falliti	Stabilisce quante volte una password può essere inserita in modo errato prima che venga eseguita una cancellazione completa del dispositivo.

Crittografia

A questo punto, potrai criptare la memoria interna del dispositivo e quella della scheda SD.

Richiedi la crittografia dello storage	Se questa impostazione è attivata, la memoria del dispositivo sarà criptata, a patto che il dispositivo supporti questa funzionalità. Una volta che la memoria del dispositivo è stata crittografata per la prima volta, non è più possibile disincriptarla. Allo stesso modo, il criterio della password sarà automaticamente impostato su 6 simboli alfanumerici.
Richiedi la crittografia della scheda SD	Questa impostazione si applica solo ai dispositivi Samsung! Se questa impostazione è attivata, la scheda SD esterna può essere crittografata e può essere decifrata solo manualmente sul dispositivo dell'utente finale. Allo stesso modo, il criterio della password sarà automaticamente impostato su 6 simboli alfanumerici.

AntiVirus

Abilitando l'AntiVirus, Ikarus verrà installato sui dispositivi. Tieni presente che questo richiede una licenza separata che può essere inserita in Impostazioni generali → Gestione app → App di terze parti.

Scansione automatica	Definisce se Ikarus esegue o meno la scansione automatica e con quale frequenza. Abilitando la "Scansione Automatica Completa" verrà eseguita una scansione completa. Altrimenti verrà eseguita una scansione rapida
Aggiornamenti automatici	Abilita l'aggiornamento automatico del database dei virus e imposta la frequenza con cui questo avviene
Protezione delle app	Abilita la scansione delle applicazioni in aggiunta alla normale scansione che analizza solo i file.
Protezione della scheda SD	Abilita la protezione della scheda SD. Senza questa opzione, la scansione è limitata alla memoria locale.
Aggiornamento solo Wi-Fi	Limita l'aggiornamento al Wi-Fi

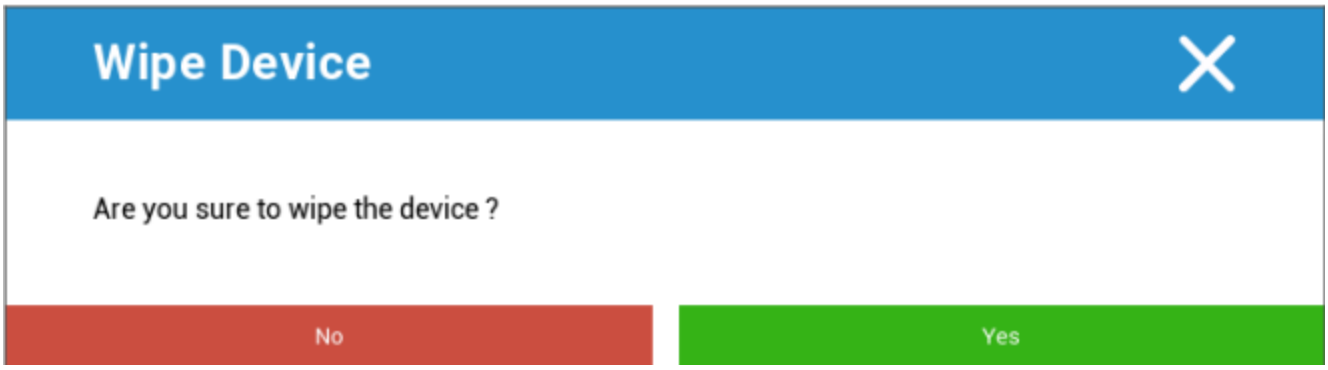
Fine vita (solo a livello di dispositivo)

Pulisci (solo a livello di dispositivo)

Alla voce "Wipe", puoi ripristinare le impostazioni di fabbrica del dispositivo. In questo caso i dati aziendali e privati verranno eliminati sul dispositivo dell'utente finale.

Cliccando sul "Simbolo del meno" riceverai il seguente messaggio

Cancellare anche la scheda SD?	Anche la memoria della scheda SD verrà cancellata.



Con "Sì" puoi eseguire la pulizia.

In "Wipe Report" possono essere visualizzati i seguenti elementi

Cancellata da	Storia di chi ha eseguito la pulizia
Data	Data
Stato	Stato (ad esempio, se il Wipe è stato eseguito con successo)

Impostazioni di restrizione

Restrizioni

Qui è possibile limitare e bloccare una serie di cose.

Abilita la telecamera	Consenti l'uso della fotocamera
Forza la sincronizzazione automatica	Si riferisce all'interfaccia "Sync On = la sincronizzazione è attivata in modo permanente Off = la sincronizzazione è disattivata in modo permanente. Scelta dell'utente = scelta dell'utente
Forza Bluetooth	On = il Bluetooth è attivato in modo permanente Off = il Bluetooth è disattivato in modo permanente Scelta dell'utente = scelta dell'utente
Forza GPS	On = il GPS è attivato in modo permanente Off = il GPS è disattivato in modo permanente Scelta dell'utente = scelta dell'utente
Forza la precisione della posizione di Google	On = Localizzazione permanente su Internet Off = Disattivazione permanente della localizzazione internet Scelta dell'utente = scelta dell'utente

Per i dispositivi Samsung con interfaccia KNOX 1.0 o superiore, sono disponibili le seguenti opzioni di impostazione.

Consenti la scheda SD	Consenti la scheda SD
Consenti la scrittura della scheda SD	Consenti la "scrittura" sulla scheda SD
Consenti la cattura dello schermo	Consenti la cattura dello schermo
Consenti gli appunti	Consenti gli appunti
Backup delle impostazioni e dei dati dell'app su Google Cloud	Off = disattiva Google Backup On = attiva Google Backup Scelta dell'utente = selezionata dall'utente
Consenti il debug USB	Consenti il debug USB (è utilizzato, ad esempio, per la creazione dei log dei dispositivi (ADB))
Consenti il rapporto di crash di Google	Consentire l'invio di Google Crash Report dalle applicazioni
Consenti il reset di fabbrica	Permette all'utente di ripristinare le impostazioni di fabbrica del dispositivo.
Consenti l'aggiornamento OTA	Consenti gli aggiornamenti "Over-The-Air
Consenti l'archiviazione host USB	Se attivato, è possibile collegare una memoria USB, sotto forma di HD o di lettore di schede SD.
Consenti il lettore multimediale USB (MTP, PTP)	Consenti il lettore multimediale USB (MTP, PTP)
Consenti il microfono	On = consente il microfono per le applicazioni di terze parti Off = blocca il microfono per le applicazioni di terze parti Scelta dell'utente = gli utenti possono scegliere, se l'applicazione di terze parti ha accesso al microfono
Consenti NFC (Near Field Communication)	Consenti NFC
Consenti fonti sconosciute (APK Sideloading)	Se abilitato, il caricamento laterale delle applicazioni (file APK) è consentito. Una volta disattivata questa impostazione, l'utente deve attivarla manualmente quando si riabilita l'installazione di APK da fonti sconosciute.
Consenti la creazione di utenti	Permette la creazione di più utenti

Proprietario del dispositivo AE

(Il dispositivo deve essere in modalità Android Enterprise Device Owner) Si consiglia di creare i dispositivi come dispositivi "Android Enterprise" e non come dispositivi "Android".

Sicurezza	
Disconoscimento della posizione della condivisione	Specifica se un utente non può attivare la condivisione della posizione.
Disabilita l'avvio sicuro	Specifica se l'utente non può riavviare il dispositivo in modalità di avvio sicuro.
Disabilita il reset della rete	Specifica se un utente non può ripristinare le impostazioni di rete dalle Impostazioni.
Disabilita il reset di fabbrica	Specifica se un utente non può resettare il dispositivo.
Abilita ADB	Consente la connessione a un PC tramite ADB
Disabilita il Keyguard	Disattiva il Keyguard
Informazioni sulla schermata di blocco del proprietario del dispositivo	Imposta le informazioni sul proprietario del dispositivo da mostrare nella schermata di blocco.
Applicazione della conformità	Modalità Prompt User - All'utente verrà richiesto di eseguire le azioni necessarie. Mode Lock-Down Container - Nasconde tutte le app fino a quando non vengono soddisfatti tutti i requisiti.

Gestione delle app	
Consenti il collegamento tra profili diversi delle app	Permette alle app del profilo padre di gestire i link web del profilo gestito.
Disabilita il controllo delle app	Specifica se un utente non può modificare le applicazioni nelle Impostazioni o nei lanciatori.
Disabilita l'installazione di app	Specifica se un utente non può installare applicazioni.
Disabilita le applicazioni da disinstallare	Specifica se un utente non può disinstallare le applicazioni.
Politica dei permessi di runtime	Specifica come verranno gestite le nuove richieste di autorizzazione da parte delle app.
Consenti fonti sconosciute	Se abilitata, gli utenti possono caricare le applicazioni in modalità sideload installando un file .apk.

Connettività	
Disabilita la configurazione della rete mobile	Specifica se un utente non può configurare le reti mobili.
Configurazione di Disallow Tethering	Specifica se un utente non può configurare il Tethering e gli hotspot portatili.
Disabilita la configurazione VPN	Specifica se un utente non può configurare una VPN.
Disabilita la configurazione Wifi	Specifica se un utente non può cambiare i punti di accesso WiFi.
Disconoscimento del raggio NFC in uscita	Specifica se l'utente non è autorizzato a utilizzare l'NFC per trasmettere dati dalle app.
Blocca la configurazione WiFi	Questa impostazione controlla se le configurazioni WiFi create da un'app Proprietario del dispositivo devono essere bloccate (cioè modificabili o rimovibili solo dall'app Proprietario del dispositivo, non anche dall'app Impostazioni).
Abilita il roaming dati	Attiva il roaming dati

Bluetooth	
Disabilita il Bluetooth	Specifica se il bluetooth non è consentito sul dispositivo. Richiede Android 8.0
Disabilita la condivisione Bluetooth	Specifica se la condivisione bluetooth in uscita non è consentita sul dispositivo. Richiede Android 8.0
Disabilita la configurazione Bluetooth	Specifica se un utente non può configurare il bluetooth.

Gestione degli account	
Disabilita l'aggiunta di un profilo gestito	Specifica se un utente non può aggiungere profili gestiti. Richiede Android 8.0
Disabilita l'aggiunta di utenti	Specifica se un utente non può aggiungere nuovi utenti.
Disallow Rimuovi il profilo gestito	Specifica se i profili gestiti di questo utente possono essere rimossi, se non dal proprietario del profilo. Richiede Android 8.0
Disconoscimento della modifica dell'account	Specifica se un utente non può aggiungere e rimuovere account, a meno che non siano aggiunti programmaticamente da Authenticator.

Telefonia	
Disabilita le chiamate in uscita	Specifica che l'utente non può effettuare chiamate in uscita.
Disabilita gli SMS	Specifica che l'utente non è autorizzato a inviare o ricevere messaggi SMS.

Sistema	
Disabilita la creazione di finestre	Specifica che le finestre diverse da quelle dell'applicazione non devono essere create.
Disabilita l'impostazione dell'icona Utente	Specifica se un utente non può cambiare la propria icona.
Disallow Set Wallpaper	Limitazione dell'utente per impedire l'impostazione di uno sfondo.
Disabilita la barra di stato	La disabilitazione della barra di stato blocca le notifiche, le impostazioni rapide e altre sovrapposizioni dello schermo che permettono di uscire da un dispositivo monouso.
Abilita il tempo automatico	Imposta l'ora automaticamente.
Abilita il fuso orario automatico	Imposta automaticamente il fuso orario.
Rimane acceso quando è collegato alla rete	Il dispositivo rimarrà attivo mentre è collegato a una fonte di alimentazione.

Immagazzinamento	
Disabilita la verifica delle app	Specifica se un utente non può disabilitare la verifica delle applicazioni.

Disallow Mount Physical Media	Specifica se un utente non può montare supporti fisici esterni.
Abilita il servizio di backup	Il servizio di backup gestisce tutti i meccanismi di backup e ripristino sul dispositivo. Impostando questo valore a false si impedisce il backup o il ripristino dei dati. Il servizio di backup è disattivato per impostazione predefinita. Richiede Android 8.0
Abilita l'archiviazione di massa USB	Abilita l'utilizzo della memoria di massa USB.

Tastiera	
Disabilita il riempimento automatico	Specifica se un utente non è autorizzato a utilizzare i servizi di riempimento automatico. Richiede Android 8.0
Disabilita il copia e incolla tra i profili	Specifica se ciò che viene copiato negli appunti di questo profilo può essere incollato nei profili correlati.

Suono	
Disconoscimento dell'adeguamento del volume	Specifica se un utente non può regolare il volume master.
Disabilita il microfono	Specifica se un utente non può regolare il volume del microfono.
Dispositivo Mute	Dispositivo di silenziamento.

Politica di aggiornamento del sistema	
Controlla gli aggiornamenti del sistema operativo	Attiva questa opzione per impostare il comportamento dell'aggiornamento in automatico, in finestra o posticipato.

Contenitore BYOD

Android Enterprise

Android Enterprise

Attiva Android Enterprise	Abilita Android Enterprise (AE). AE è supportato da Android 5.1 in poi.
Applicazione della conformità	Modalità Prompt User - All'utente verrà richiesto di eseguire le azioni necessarie. Mode Lock-Down Container - Nasconde tutte le app fino a quando non vengono soddisfatti tutti i requisiti.
Politica dei permessi di runtime	Invita l'utente a richiedere nuovi permessi Accetta sempre le nuove richieste di permesso Rifiuta sempre le richieste di nuovi permessi Attenzione: Alcune applicazioni hanno problemi a riconoscere i permessi se questi sono impostati automaticamente. Se concedi sempre i permessi e riscontri problemi con le app che dicono che mancano i permessi, imposta questo parametro su "richiama l'utente" e reinstalla l'app.
Consenti gli appunti in uscita	Permette di copiare e incollare dall'interno del contenitore verso l'esterno
Consenti la risoluzione dell'ID chiamante	Mostra il nome di una chiamata in arrivo in base ai contatti presenti nel contenitore.
Consenti la risoluzione della ricerca dei contatti	Permette di cercare i nomi nei contatti del contenitore quando si effettua una chiamata.
Consenti la condivisione dei contatti Bluetooth	Permette di accedere al contatto con il contenitore in auto
Disconoscimento del raggio NFC in uscita	Disattiva l'NFC per il contenitore
Consenti fonti sconosciute	Se abilitata, gli utenti possono caricare le applicazioni in modalità sideload installando un file .apk.
Consenti il debug USB	Se abilitato, gli utenti possono attivare il Debug USB.
Disconoscimento della modifica dell'account	Disabilita la creazione, l'eliminazione e la modifica degli account nel contenitore.

	Tieni presente che alcune applicazioni necessitano di creare o modificare gli account per funzionare come previsto.

Scambio Gmail

Permette di configurare Gmail nel contenitore. Tieni presente che l'attivazione di questa configurazione non comporta l'installazione automatica dell'applicazione. Devi comunque aggiungere questa app come app obbligatoria.

Indirizzo e-mail	Indirizzo e-mail
Nome host del server	Nome host del server
Nome utente	Nome utente
Firma	Firma
Numero di giorni precedenti da sincronizzare	Numero di giorni precedenti da sincronizzare.
Identificatore del dispositivo	Identificatore EAS. Lascia questo campo vuoto se il tuo ambiente non lo richiede
Utilizza il Secure Sockets Layer (SSL)	Abilita l'uso di SSL. Disabilitare questa funzione può ridurre la sicurezza
Accetta tutti i certificati	Accetta tutti i certificati. Abilitare questa opzione può ridurre la sicurezza
Consenti gli account non gestiti	Permette all'utente di aggiungere altri account
Certificato del cliente	Carica il certificato del client se il tuo server Exchange lo richiede

Applicazioni del sistema AE

Qui puoi abilitare le applicazioni di sistema per l'Android Enterprise Container. Tieni presente che l'applicazione specificata deve essere presente nella memoria del sistema, altrimenti non succede nulla.

Codice di accesso al contenitore

Solo per Android 7.0 o superiore

Permette di impostare una password specifica per il contenitore.

Lunghezza minima della password	Stabilisce il numero minimo di simboli che una password deve contenere
Qualità della password	Forza della password Non specificato = non specificato Ogni password è ok = ogni password è accettabile almeno caratteri numerici = deve contenere almeno caratteri numerici almeno caratteri complessi = deve contenere almeno caratteri speciali almeno caratteri alfanumerici = deve contenere almeno caratteri alfanumerici almeno caratteri alfabetici = deve contenere almeno caratteri alfabetici
Blocco del tempo massimo di inattività	Tempo massimo prima che il contenitore venga bloccato. Questo configura solo il valore massimo che può essere selezionato dall'utente.
Lettere minuscole minime richieste nella password	Lettere minuscole minime richieste nella password
Lettere maiuscole minime richieste nella password	Lettere maiuscole minime richieste nella password
Caratteri non letterali minimi richiesti nella password	Caratteri non letterali minimi richiesti nella password
Cifre numeriche minime richieste nella password	Cifre numeriche minime richieste nella password
Simboli minimi richiesti nella password	Simboli minimi richiesti nella password
Timeout di scadenza della password	Stabilisce, dopo quale intervallo di tempo la password scade e deve essere emessa una nuova password.
Limitazione della cronologia delle password	Numero di password precedentemente utilizzate che non sono consentite
Massimo di tentativi di password falliti	Stabilisce quante volte una password può essere inserita in modo errato, prima che il contenitore venga cancellato

Samsung KNOX

Attivazione

Qui puoi attivare il contenitore Samsung KNOX. Tieni presente che questa funzione non è più supportata da Samsung su Android 10 o versioni successive. Usa il contenitore Android Enterprise su

Android 10 o superiore

Codice di accesso Knox

Stabilisci le linee guida che riguardano le impostazioni della password del dispositivo

Lunghezza minima della password	Stabilisce il numero di simboli che deve avere la password
Qualità della password	Forza della password Ogni password è ok = Ogni password è ok Almeno caratteri numerici = Deve essere presente un minimo di caratteri numerici Almeno caratteri complessi = Deve essere presente un minimo di caratteri speciali Almeno caratteri alfanumerici = Deve essere presente un minimo di caratteri alfanumerici Almeno caratteri alfabetici = Devono essere presenti almeno caratteri alfabetici
Caratteri complessi minimi richiesti	Devono essere presenti un minimo di caratteri complessi
Timeout massimo di inattività	Timeout massimo di inattività dell'utente, prima del blocco della tastiera
Consenti l'autenticazione delle impronte digitali	Consenti l'autenticazione tramite impronte digitali
Consenti l'autenticazione dell'iride	Consenti l'autenticazione tramite riconoscimento dell'iride
Età massima della password	Stabilisce dopo quanto tempo la password scade e deve essere emessa una nuova password.
Cronologia delle password memorizzate	Numero di password precedenti non consentite
Massimo di tentativi di password falliti	Stabilisce quante volte la password può essere inserita in modo errato prima che venga effettuata una cancellazione completa del dispositivo.

Knox Security

Limitare le funzionalità specifiche del dispositivo

Abilita la telecamera	Consenti l'uso della fotocamera

Consenti l'App Store Samsung KNOX	Consenti l'uso dell'App Store Samsung KNOX
Consenti i servizi di Google Play	Consenti i servizi di Google Play
Consenti al browser	Consenti l'uso del browser nativo
Consenti screenshot	Consenti la creazione di screenshot
Consenti l'importazione dei contatti	Se attivato, l'accesso ai contatti del dispositivo dal contenitore KNOX è consentito
Consenti l'esportazione dei contatti	Se attivato, l'accesso ai contatti KNOX dal dispositivo è consentito
Consenti l'importazione del calendario	Se attivato, l'accesso al calendario del dispositivo dal contenitore KNOX è consentito.
Consenti l'esportazione del calendario	Se attivato, è consentito l'accesso all'agenda KNOX dal dispositivo
Consenti la tastiera non sicura	Consenti l'uso di una tastiera non sicura
Abilita l'importazione di file	Abilitare l'importazione di file nel contenitore KNOX
Abilita l'esportazione dei file	Abilita l'esportazione dei file dal contenitore KNOX

Scambio Knox

Qui puoi configurare il profilo di Exchange per il contenitore KNOX.

Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Facendo clic su **Mostra segnaposto** potrai visualizzarli da solo
Nome host del server	Indirizzo del server di Exchange
Nome utente	Il nome di accesso per il rispettivo dispositivo dell'utente finale, si prega di notare anche i "segnaposto" qui presenti
Dominio	Indirizzo di dominio
Password (solo a livello di dispositivo)	Opzionalmente è possibile fornire una password al singolo dispositivo; se questa rimane vuota, all'utente verrà richiesto di inserire la propria password di Exchange.
Numero di giorni precedenti da sincronizzare	Numero di giorni che determinano il momento in cui le email vengono sincronizzate di nuovo
Firma	È possibile allegare una firma
Account predefinito	Stabilisce che questo account di posta elettronica è l'account standard
Utilizza il Secure Sockets Layer (SSL)	Usa una connessione SSL
Usa la sicurezza del livello di trasporto (TLS)	Usa una connessione TLS
Accetta tutti i certificati	Sono accettati tutti i certificati. Seleziona questa opzione se il tuo Exchange Server utilizza un certificato autofirmato.

Knox eMail

Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Facendo clic su **Mostra segnaposto** potrai visualizzarli da solo
Protocollo del server in entrata	Protocollo del server in entrata IMAP o POP
Indirizzo del server in entrata	Indirizzo del server in entrata
Porta del server in entrata	Porta del server in entrata
Login/nome utente del server in arrivo	Login/nome utente del server in arrivo
Password del server in entrata	Password del server in entrata
Il server in entrata utilizza SSL	Il server in entrata utilizza SSL
Il server in entrata utilizza TLS	Il server in entrata utilizza TLS
Il server in entrata accetta tutti i certificati	Il server in entrata accetta tutti i tipi di certificati
Protocollo del server in uscita	Protocollo del server in uscita SMTP
Porta del server in uscita	Porta del server in uscita
Il server in uscita utilizza credenziali extra	Credenziali aggiuntive per il server in uscita. Se è impostato su "off", verranno utilizzate le impostazioni del server in entrata.
Login/nome utente del server in uscita	Login/nome utente del server in uscita
Password del server in uscita	Password del server in uscita
Il server in uscita utilizza SSL	Il server in uscita utilizza SSL
Il server in uscita utilizza TLS	Il server in uscita utilizza TLS

Il server in uscita accetta tutti i certificati	Il server in uscita accetta tutti i tipi di certificati
Firma	Qui è possibile allegare una firma
Notifica all'utente la ricezione di una nuova e-mail	Notifica all'utente la ricezione di una nuova e-mail

Applicazioni Knox

Stabilisci qui le app che vuoi distribuire ai dispositivi degli utenti finali. Questi saranno poi disponibili nel contenitore KNOX. Per aggiungere un'applicazione, procedi come nel menu Applicazioni obbligatorie

Nome dell'applicazione	Nome dell'applicazione
Obbligatorio da quando	Momento in cui è stata aggiunta l'applicazione
Fonte	Fonte dell'applicazione (Play Store | In-house)

Cliccando sul simbolo, l'applicazione in questione può essere nuovamente rimossa.

Gestione delle connessioni

Wifi

Per questa impostazione, esegui la preconfigurazione dei dispositivi dell'utente finale, per l'accesso agli Access Point interni

Identificatore del set di servizi (SSID)	SSID per la rete da collegare
Rete nascosta	Attiva, nel caso in cui l'AP non trasmetta il SSID
Tipo di sicurezza	Stabilire il tipo di sicurezza dell'AP

Tipo di sicurezza

WEP

Password	Password per l'AP

WPA/WPA2

Password	Password per l'AP

802.1x EAP

Metodo EAP	

PWD	Identità	Identità
	Password	Password

PEAP	Protocollo di autenticazione di fase 2	nessuno	Nessun protocollo aggiuntivo
		MSCHAPV2	Protocollo MSCHAPV2
		GTC	Protocollo GTC
	Certificato CA	Certificato CA	
	Identità	Identità	
	Identità anonima	Identità anonima	
	Password	Password	

Metodo EAP	

TTLS	Protocollo di autenticazione di fase 2	nessuno	Nessun protocollo aggiuntivo
		PAP	Protocollo PAP
		MSCHAP	Protocollo MSCHAP
		MSCHAPV2	Protocollo MSCHAPV2
		GTC	Protocollo GTC
	Certificato CA	Certificato CA	
	Identità	Identità	
	Identità anonima	Identità anonima	
	Password	Password	

TLS	Certificato CA	Certificato CA
	Identità	Identità
	Password	Password

VPN

Tipo di connessione	Stabilisci il tipo di connessione VPN

Se selezioni "Per-App VPN" come tipo di VPN, i client VPN disponibili cambieranno. Per-App VPN limita la VPN a determinate applicazioni e avvia automaticamente la connessione VPN se viene avviata un'applicazione specifica.

Cliente VPN AppTec360	Utilizza il client VPN di AppTec360 in combinazione con il gateway universale.
Nome della connessione	Nome della connessione VPN
Configurazione del gateway	Seleziona la Configurazione VPN del Gateway Universale
VPN sempre attiva	Impone che la VPN sia sempre attiva, in modo che tutto il traffico passi attraverso la VPN.
Abilita il blocco nativo	Blocca tutte le reti quando il dispositivo non è connesso alla VPN. Utilizzala con attenzione perché, se non configurata correttamente, può causare la perdita completa della connessione. Solo per Android Enterprise su Android 7 o superiore
Abilita il blocco di AppTec360	Blocca l'utilizzo di tutte le applicazioni fino all'avvio della connessione VPN.

Cisco AnyConnect	
Nome della connessione	Nome della connessione VPN
Server	Indirizzo del server
Modalità certificato	Disattivato = disattivato Automatico = automatico

L2TP (solo KNOX)	Disponibile solo su dispositivi Samsung
Nome della connessione	Nome della connessione
Server	Indirizzo del server
Abilita il segreto L2TP	
Ricerca DNS Domini	Ricerca domini DNS

Tipo di connessione	**Stabilisci il tipo di connessione VPN**

PPTP (solo KNOX)	Disponibile solo su dispositivi Samsung
Nome della connessione	Nome della connessione VPN
Server	Indirizzo del server
Abilita la crittografia	Abilita la crittografia
Ricerca DNS Domini	Ricerca domini DNS

L2TP / IPSec PSK (solo KNOX)	Disponibile solo su dispositivi Samsung
Nome della connessione	Nome della connessione VPN
Server	Indirizzo del server
Chiave precondivisa IPSec	Chiave precondivisa per l'autenticazione
Abilita il segreto L2TP	
Segreto L2TP	
Ricerca DNS Domini	Ricerca domini DNS

IPSec XAuth PSK (solo KNOX)	Disponibile solo su dispositivi Samsung
Nome della connessione	Nome della connessione VPN
Server	Indirizzo del server
Identificatore IPSec	Nome utente per la connessione
Chiave precondivisa IPSec	Password per la connessione
Ricerca DNS Domini	Ricerca domini DNS

OpenVPN	

Nome della connessione	Nome della connessione
Profilo OpenVPN	Ecco dove verrà copiato il contenuto del file .ovpn
App OpenVPN	Esistono due diverse applicazioni per l'utilizzo di OpenVPN Ti consigliamo l'applicazione "OpenVPN per Android". In alternativa, è possibile utilizzare l'applicazione "OpenVPN Connect".

Restrizioni

Qui puoi impostare le restrizioni relative alla gestione delle connessioni.

Consenti il roaming dei dati	Consenti i dati mobili in roaming
Forza il roaming dei dati	Se attivato, il roaming per i dati mobili viene attivato in modo permanente (non è consigliato!). Questa impostazione sovrascrive l'impostazione "Consenti roaming dati"!
Le seguenti impostazioni sono disponibili solo su Samsung KNOX 2.0 o versioni successive.	
Consenti solo le chiamate di emergenza	Consenti solo le chiamate di emergenza
Consenti il WiFi	Consenti il WiFi
Livello minimo di sicurezza della rete WiFi	Livello minimo di sicurezza della rete WiFi Aperto = sono ammessi tutti i tipi di WiFi
Impedisci all'utente di aggiungere reti WiFi	L'utente non può aggiungere una rete WiFi da solo Questa impostazione è possibile solo se è stato definito un profilo WiFi in "Gestione connessioni".
Consenti SMS e MMS	Tutti = Tutto il traffico di SMS e MMS è consentito Solo SMS in entrata = Sono consentiti solo gli SMS in entrata. Solo SMS in uscita = Sono consentiti solo gli SMS in uscita. Nessuno = Non è consentito il traffico di SMS/MMS.
Consenti la sincronizzazione durante il roaming	Consenti la sincronizzazione durante il roaming On = attivato Off = disattivato Scelta dell'utente = scelta dell'utente
Consenti il roaming vocale	Consenti il roaming vocale On = attivato Off = disattivato Scelta dell'utente = scelta dell'utente
Usa il server proxy http del sistema	L'utilizzo di un server proxy HTTP, fornito dalle impostazioni del sistema nelle impostazioni, dipende dalla rete connessa (WiFi o APN).

APN

Le seguenti impostazioni sono disponibili solo su Samsung SAFE 2.0 o superiore!

Nome visualizzato APN	Nome visualizzato APN	
Nome del punto di accesso	Nome dell'APN	
Protocollo del server in uscita	Non impostato	
	Nessuno	
	PAP	Protocollo PAP
	CHAP	Protocollo CHAP
	PAP o CHAP	Il protocollo PAP o CHAP
MCC - Codice paese mobile	L'MCC viene inserito qui; lascia questo campo vuoto se deve essere utilizzato l'MCC della scheda SIM inserita.	
MNC - Codice di rete mobile	L'MNC viene inserito qui; lascia questo campo vuoto se deve essere utilizzato l'MCC della scheda SIM inserita.	
Indirizzo del server	Indirizzo del server	
Numero di porta del server	Numero di porta del server	
Indirizzo proxy del server	Indirizzo proxy del server	
Indirizzo del server MMS	Indirizzo del server MMS, per Standard lasciare vuoto	
Numero di porta MMS	Numero di porta MMS	
Indirizzo proxy MMS	Indirizzo proxy MMS	
Nome utente	Nome utente	
Password	Password	
Tipo di punto di accesso	I tipi consentiti sono: "default", "mms", "supl". Se questo campo viene lasciato vuoto, verrà utilizzato "default,supl,mms".	
APN preferito	L'APN è preferibile	

Bluetooth

Qui è possibile eseguire una serie di impostazioni Bluetooth.

Le seguenti impostazioni sono disponibili solo su Samsung KNOX 1.0 o superiore!

Consenti il rilevamento del dispositivo tramite Bluetooth	Consenti la scoperta del dispositivo tramite Bluetooth
Consenti l'accoppiamento Bluetooth	Consenti l'accoppiamento Bluetooth
Consenti i dispositivi auricolari Bluetooth	Consenti i dispositivi auricolari Bluetooth
Consenti i dispositivi vivavoce Bluetooth	Consenti i dispositivi vivavoce Bluetooth
Consenti i dispositivi Bluetooth A2DP	Consenti lo streaming audio Bluetooth A2DP tra i dispositivi
Consenti le chiamate in uscita	Consenti le chiamate in uscita viaBT
Consenti il trasferimento dei dati via Bluetooth	Consente il trasferimento dei dati tramite Bluetooth
Consenti il tethering Bluetooth	Permette di utilizzare il dispositivo come modem (connessione internet Bluetooth)
Consenti la connessione al computer tramite Bluetooth	Consenti la connessione al computer tramite Bluetooth

Gestione del PIM

Scambio

Disponibile solo per Samsung KNOX 1.0 o superiore!

Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Facendo clic su **Mostra segnaposto** potrai visualizzarli da solo
Nome host del server	Indirizzo del server di Exchange
Nome utente	Il nome di accesso per il rispettivo dispositivo dell'utente finale, si prega di notare anche i "Segnaposto qui".
Dominio	Indirizzo di dominio
Password (solo a livello di dispositivo)	Opzionalmente, è possibile fornire una password a un singolo dispositivo; se questa rimane vuota, all'utente verrà richiesto di inserire la propria password di Exchange.
Numero di giorni precedenti da sincronizzare	Numero di giorni che determinano il momento in cui le email vengono sincronizzate di nuovo
Firma	È possibile allegare una firma (Suggerimento: alcuni dispositivi richiedono la formattazione HTML per la firma).
Account predefinito	Stabilisce che questo account di posta è l'account standard
Utilizza il Secure Sockets Layer (SSL)	Usa una connessione SSL
Usa la sicurezza del livello di trasporto (TLS)	Usa una connessione TLS
Accetta tutti i certificati	Sono accettati tutti i certificati. Seleziona questa opzione se il tuo Exchange Server utilizza un certificato autofirmato.

eMail

Qui puoi distribuire gli account IMAP e POP ai rispettivi dispositivi degli utenti finali.

Le seguenti impostazioni sono disponibili solo su Samsung KNOX 1.0 o superiore!		
Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Facendo clic su **Mostra segnaposto** potrai visualizzarli da solo	
Protocollo del server in entrata	Protocollo del server in entrata	IMAP o POP
Indirizzo del server in entrata	Indirizzo del server in entrata	
Porta del server in entrata	Porta del server in entrata	
Login/nome utente del server in arrivo	Login/nome utente del server in arrivo	
Password del server in entrata (solo a livello di dispositivo)	Password del server in entrata (solo a livello di dispositivo)	
Il server in entrata utilizza SSL	Il server in entrata utilizza SSL	
Il server in entrata utilizza TLS	Il server in entrata utilizza TLS	
Il server in entrata accetta tutti i certificati	Il server in entrata accetta tutti i tipi di certificati	
Protocollo del server in uscita	Protocollo del server in uscita	SMTP
Porta del server in uscita	Porta del server in uscita	
Il server in uscita utilizza credenziali extra	Credenziali aggiuntive per il server in uscita. Se è impostato su "off", verranno utilizzate le impostazioni del server in entrata.	
Login/nome utente del server in uscita	Login/nome utente del server in uscita	
Password del server in uscita (solo a livello di dispositivo)	Password del server in uscita	
Il server in uscita utilizza SSL	Il server in uscita utilizza SSL	
Il server in uscita utilizza TLS	Il server in uscita utilizza TLS	
Il server in uscita accetta tutti i certificati	Il server in uscita accetta tutti i tipi di certificati	

Firma	La firma può essere allegata qui (Suggerimento: alcuni dispositivi richiedono la formattazione HTML per la firma).
Notifica all'utente la ricezione di una nuova e-mail	Notifica all'utente la ricezione di una nuova email

AE Gmail Exchange

Info: Questa configurazione verrà applicata all'applicazione Gmail. Quindi devi approvare e installare Gmail.

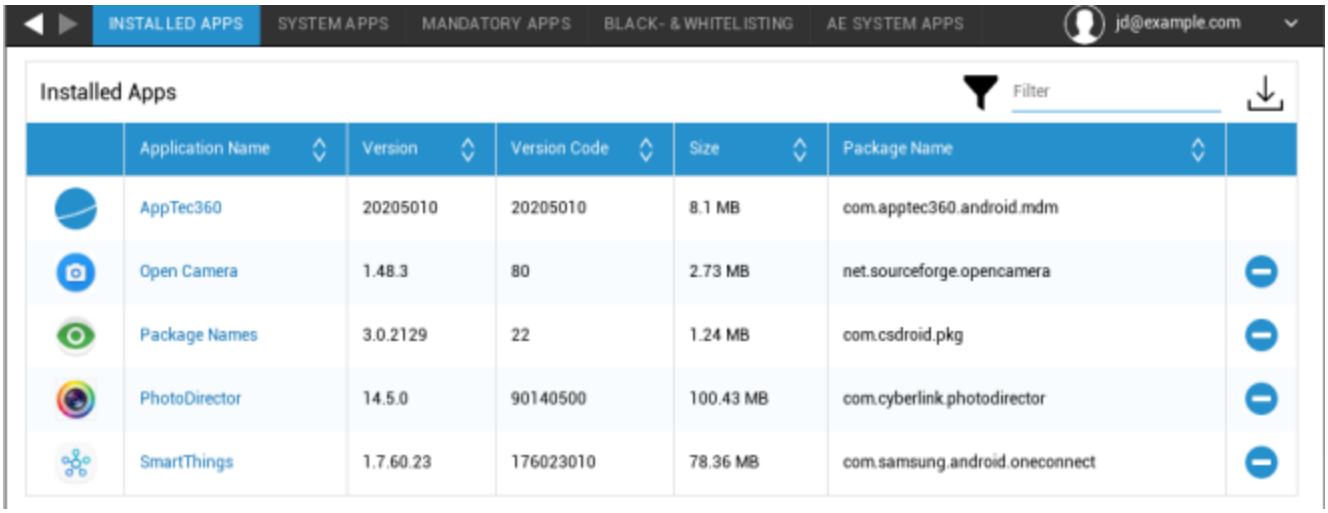
Indirizzo e-mail	L'indirizzo e-mail dell'utente fornito Tieni presente i "Segnaposto", che puoi utilizzare per lavorare con le credenziali e non eseguire le modifiche manualmente su ogni dispositivo. Facendo clic su Mostra segnaposto potrai visualizzarli da solo
Nome host del server	Indirizzo del server di Exchange
Nome utente	Il nome di accesso per il rispettivo dispositivo dell'utente finale, si prega di notare anche i "Segnaposto qui".
Firma	È possibile allegare una firma (Suggerimento: alcuni dispositivi richiedono la formattazione HTML per la firma).
Numero di giorni precedenti da sincronizzare	Numero di giorni che determinano il momento in cui le email vengono sincronizzate di nuovo
Identificatore del dispositivo	Identificatore EAS. Lascia questo campo vuoto se il tuo ambiente non lo richiede
Utilizza il Secure Sockets Layer (SSL)	Usa una connessione SSL
Accetta tutti i certificati	Sono accettati tutti i certificati. Seleziona questa opzione se il tuo Exchange Server utilizza un certificato autofirmato.
Consenti gli account non gestiti	Permette all'utente di aggiungere altri account
Certificato del cliente	Carica il certificato del client se il tuo server Exchange lo richiede

Gestione delle app

Enterprise App Manager

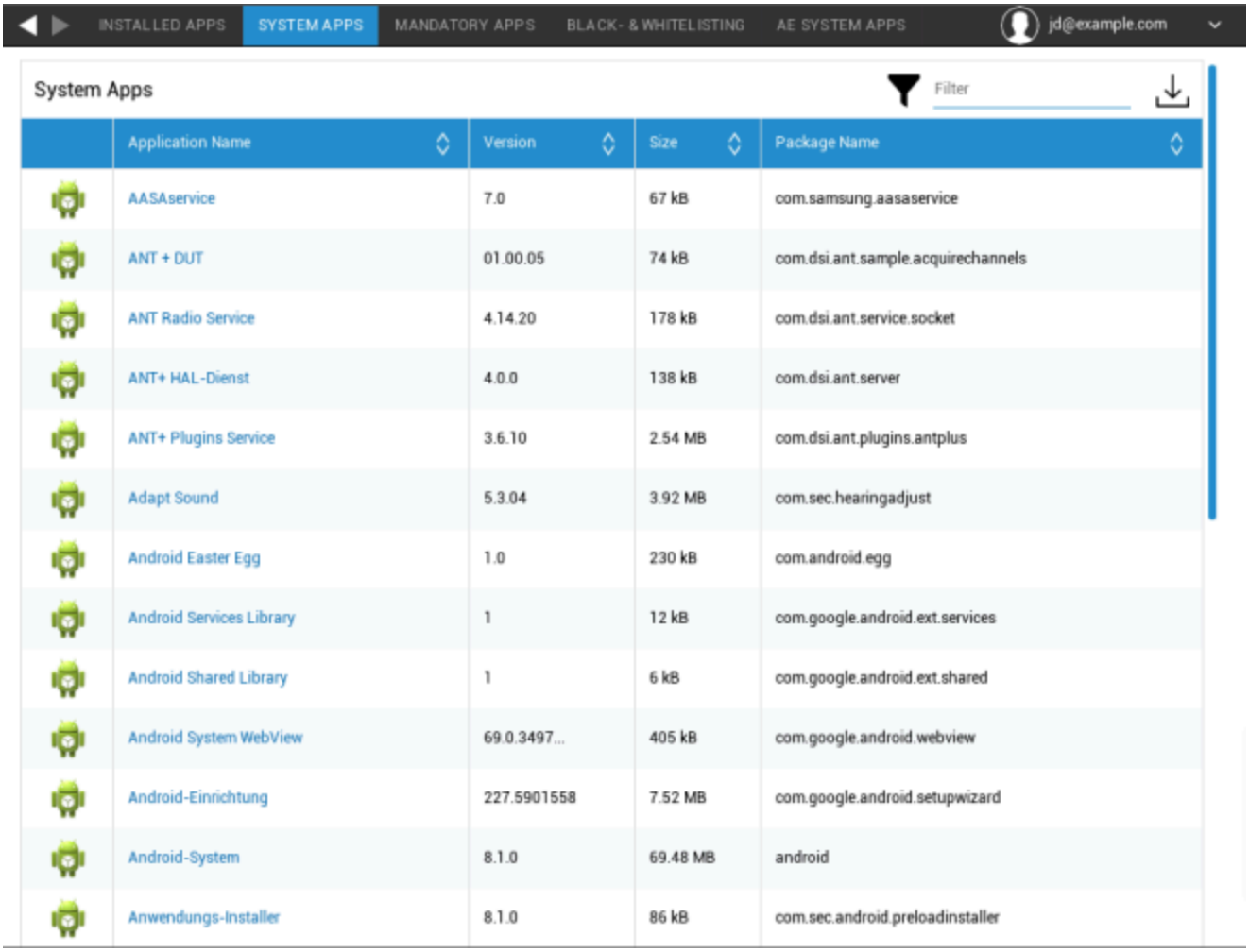
Applicazioni installate (solo a livello di dispositivo)

Qui verranno visualizzate tutte le app attualmente installate sul dispositivo dell'utente finale.


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

App di sistema (solo a livello di dispositivo)

Sotto la voce "App di sistema", verranno elencati tutti i sistemi preinstallati con il nome e la versione del pacchetto.



Applicazioni obbligatorie

In App obbligatorie puoi definire quali app devono essere installate sul dispositivo. A seconda della configurazione e del dispositivo, l'applicazione verrà installata automaticamente o verrà richiesto all'utente di installarla.

Ti ricordiamo che è consigliabile utilizzare Android Enterprise per facilitare la gestione delle app.

Gli scenari sono elencati di seguito:

Applicazioni normali del Play Store

Le installazioni di app su Playstore richiedono sempre un'interazione con l'utente. Inoltre, è necessario configurare un account Google sul dispositivo.

Installazione di app in-house

Sui dispositivi Samsung queste app verranno installate in modo silenzioso. L'unica eccezione è il contenitore, dove l'utente deve confermare l'installazione.

In qualsiasi altro scenario, l'utente deve confermare l'installazione dell'app.

Applicazioni Android Enterprise Play Store

Queste applicazioni saranno sempre installate in modo silenzioso, senza l'interazione dell'utente.

Per aggiungere un'applicazione obbligatoria, clicca sul "+" e seleziona l'applicazione desiderata dall'elenco. Tieni presente che non puoi installare applicazioni dalla scheda "Google Play Store" se il dispositivo è configurato con Android Enterprise come completamente gestito o come contenitore.

Se utilizzi Android Enterprise, seleziona le applicazioni dalla sezione "AE Play Store". Per rendere le app disponibili qui, confermale nel Google Enterprise Play Store andando su Impostazioni generali → AE Play Store → Play Store Apps.

Quando si rimuove un'app obbligatoria, questa verrà disinstallata anche dal dispositivo.

Puoi cliccare sul nome di un'app nell'elenco delle app obbligatorie e accedere alla scheda "configurazione" per configurare un'app. Questo richiede l'utilizzo di Android Enterprise e l'applicazione deve supportarlo. Pertanto le opzioni disponibili dipendono dall'applicazione selezionata.

Applicazioni del sistema AE

Qui puoi abilitare le applicazioni di sistema per i dispositivi Android Enterprise. Tieni presente che l'applicazione specificata deve essere presente nella memoria del sistema, altrimenti non succede

nulla. 296

Restrizioni e impostazioni

Black- e Whitelisting

Qui puoi definire una black- o una whitelist. Tutte le app presenti nella lista nera saranno bloccate. Tutte le app non presenti nella whitelist saranno bloccate. Una blacklist vuota non blocca nulla, mentre una whitelist vuota blocca tutto*.

**Tutte le app obbligatorie e le app dell'Enterprise App Store saranno inserite automaticamente nella whitelist. Non è necessario aggiungerli manualmente*

Cliccando sul "+" puoi cercare un'applicazione che vuoi aggiungere alla tua black- o whitelist oppure inserire manualmente il nome di un pacchetto.

Restrizioni delle applicazioni di sistema

Nella sezione "Restrizioni app di sistema" puoi, tra le altre cose, bloccare le app e i servizi preinstallati, come desideri.

Disabilita il browser	Disabilita il browser standard
Disabilita il calendario	Disabilita il calendario nativo
Disabilita la calcolatrice	Disabilita la calcolatrice
Disabilita il browser Chrome	Disattiva il browser Chrome
Disattivare l'orologio	Disattiva l'orologio
Disabilita i contatti	Disabilita i contatti
Disabilita il dialer	Disabilita il dialer nativo
Disabilita la posta elettronica	Disabilita le e-mail
Disabilita lo scambio	Disabilita gli account di Exchange
Disabilita Facebook	Disattiva l'applicazione di Facebook
Disabilita la Galleria	Disabilita l'applicazione nativa della galleria
Disattivare Gmail	Disattivare Gmail
Disabilita Google Books	Disabilita Google Books
Disabilita il chiosco di Google Play	Disabilita il chiosco di Google Play
Disabilita Google Maps	Disabilita Google Maps
Disattivare Google Music	Disattivare Google Music
Disabilita Google Movies	Disabilita Google Movies
Disattivare il Google Play Store	Disattiva il Google Play Store (App Store pubblico)
Disattivare Google Plus	Disattivare Google Plus
Disattivare la ricerca di Google	Disattivare la ricerca di Google
Disabilita Google Talk / Google Hangouts	Disabilita Google Talk / Google Hangouts
Disattiva il lettore musicale	Disabilita l'applicazione nativa del lettore musicale
Disabilita le impostazioni	Disabilita le impostazioni del dispositivo
Disabilita Sim Toolkit	Disabilita i servizi di Sim Toolkit
Disabilita SMS / MMS	Disabilita SMS / MMS
Disattiva Street View	Disattiva i servizi di Street View
Disabilita Youtube	Disabilita Youtube

Applicazioni Samsung

Alla voce "Samsung Apps", puoi definire ulteriori impostazioni e/o restrizioni per i dispositivi Samsung.

Disattiva AllShare Play / Samsung Link	Disattiva AllShare Play / Samsung Link
Disabilita ChatON	Disabilita ChatON
Disabilita Game Hub	Disabilita Game Hub
Disabilita il gioco di gruppo	Disabilita il gioco di gruppo
Disabilita l'aiuto	Disabilita la Guida Samsung
Disattiva KNOX	Disabilita il contenitore Samsung KNOX
Disabilita il Memo	Disattivare le memorie vocali
Disabilita i miei file	Disabilita i miei file
Disattiva il lettore ottico	Disattiva il lettore ottico
Disabilita Polaris Office	Disabilita Polaris Office
Disattiva Readers Hub / Samsung Books	Disattiva Readers Hub / Samsung Books
Disabilita S Memo	Disattivare l'applicazione Samsung Memo
Disabilita il traduttore S	Disattiva l'applicazione Samsung Translator
Disabilita la voce S	Disattiva l'assistente vocale S
Disattivare le applicazioni Samsung	Disattivare l'App Store di Samsung
Disabilita Samsung Hub	Disabilita i negozi di intrattenimento Samsung
Disattiva il lettore video	Disattiva il lettore video
Disattiva il registratore vocale	Disattiva il registratore vocale
Disabilita WatchON	Disabilita WatchON (simula un telecomando)

Applicazioni Huawei

Alla voce "App Huawei", puoi definire ulteriori impostazioni e/o restrizioni sul dispositivo Huawei.

Disattivare il DLNA	Disattivare il DLNA
Disabilita il programma di installazione delle app	Disabilita il programma di installazione delle app
Disabilita il File Manager	Disabilita il File Manager
Disabilita Backup Manager	Disabilita Backup Manager
Disabilita l'aggiornamento del sistema	Disabilita l'aggiornamento del sistema
Disabilita la casella degli strumenti	Disabilita la casella degli strumenti
Disabilita il meteo	Disabilita il meteo
Disattiva la radio FM	Disattiva la radio FM

Impostazioni di gestione delle app

Qui puoi definire il comportamento di aggiornamento delle app InHouse.

La frequenza di controllo degli aggiornamenti definisce la frequenza con cui l'AppTec360 cerca gli aggiornamenti per le applicazioni InHouse. Una volta rilevata una nuova versione, questa verrà scaricata e installata.

La Soglia Wi-Fi definisce se il download deve essere limitato alle connessioni Wi-Fi se l'App è più grande della Soglia configurata. Se il valore è inferiore o non definisci una soglia, l'app verrà scaricata sia in Wi-Fi che in rete cellulare.

App Store aziendale

Tieni presente che le applicazioni aggiunte qui (Enterprise App Store) NON verranno installate automaticamente sui dispositivi. L'utente deve aprire l'Enterprise App Store sul dispositivo e installare l'applicazione manualmente.

Se vuoi installare automaticamente le app sul dispositivo, vai su "Gestione app" → "Enterprise App Manager" → "App obbligatorie" e aggiungi le app desiderate.

A questo punto, puoi distribuire le App opzionali ai tuoi utenti.

Playstore

Clicca sul "+" per aggiungere un'applicazione del Play Store allo store. Se utilizzi Android Enterprise, vai su "App Management Enterprise Play Store". Tieni presente che per installare le applicazioni definite qui è necessario configurare un account Google sul → dispositivo.

In-house

Al punto "In-House", puoi caricare e distribuire le app sviluppate internamente.

Clicca sul "+" per aggiungere un'applicazione InHouse all'app store aziendale che potrà essere installata dall'utente. In questo dialogo puoi anche caricare una nuova applicazione InHouse.

Play Store aziendale

Tieni presente che le app aggiunte qui (Enterprise Play Store) NON verranno installate automaticamente sui dispositivi. L'utente deve aprire il Play Store sul dispositivo e installare l'applicazione manualmente.

Se vuoi installare automaticamente le app sul dispositivo, vai su "Gestione app" → "Enterprise App Manager" → "App obbligatorie" e aggiungi le app desiderate.

A questo punto, puoi distribuire le App opzionali ai tuoi utenti.

Qui puoi aggiungere applicazioni al Playstore di Android Enterprise. Ricorda che devi approvare le app in Impostazioni generali → AE Play Store → Play Store Apps. Queste applicazioni saranno aggiunte al normale Google Play Store.

Ricorda inoltre che devi prima definire un layout con le app in Impostazioni generali → Gestione app → AE Play Store → Layout del negozio.

Le app devono essere presenti in un Layout prima di poterle aggiungere allo store.

Modalità chiosco e launcher

Modalità chiosco

La modalità Kiosk ti permette di predefinire un'applicazione o un URL. Allora sarà possibile eseguire/visitare esclusivamente questa applicazione o URL.

Allo stesso modo, i vari pulsanti hardware possono essere disattivati nella modalità Kiosk.

Avvio automatico	Avvia automaticamente la modalità Kiosk non appena il profilo raggiunge il dispositivo dell'utente finale.
Modalità Kiosk programmata?	Puoi pianificare un orario per la modalità Kiosk, che inizierà e terminerà automaticamente all'orario da te stabilito.
Ora di inizio	Ora di inizio
Tempo in minuti	Tempo in minuti, dopo il quale la modalità Kiosk deve terminare di nuovo.

Tipo di applicazione

App singola	Se vuoi avviare l'applicazione in modalità Kiosk, seleziona "Pacchetto" sotto "Tipo di applicazione".
Applicazione chiosco	Clicca qui per selezionare un'applicazione che deve essere avviata in modalità Kiosk. Troverai la solita panoramica della gestione delle app Puoi scegliere tra "Google Play Store", "Android In-House Apps" e "Packagename".

Tipo di applicazione

URL	Se vuoi lanciare un URL nella modalità Kiosk, seleziona "URL" alla voce "Tipo di applicazione". Quindi definisci l'indirizzo URL desiderato
Cancella il browser dopo l'inattività	Qui puoi definire un intervallo di tempo in minuti, dopo il quale la Modalità Kiosk deve essere riavviata.
Cancella la cache e i cookie del web	Se attivi questa funzione, dopo un riavvio della modalità Kiosk, la cache web (cookie e immagini memorizzate nella cache) verrà cancellata.
Politica della stessa origine	Se questa funzione è attiva, l'utente può navigare solo nelle sottopagine di un URL definito. Ad esempio, hai definito il seguente URL:www.mypage.com Poi, l'utente può navigare su: www.mypage.com/subpage
URL inseriti nella whitelist	Qui puoi mantenere una Whitelist: tutti questi URL sono consentiti Massimo 1 URL per riga Un URL deve iniziare con http:/ o https://
URL nella lista nera	Qui è possibile mantenere una Blacklist, tutti questi URL non sono ammessi Massimo 1 URL per riga Un URL deve iniziare con http:/ o https://
Orientamento dello schermo	Questa impostazione riguarda le regolazioni dello schermo Automatico = automatico Ritratto = formato verticale Paesaggio = modalità paesaggio

Multi App	Se selezioni la modalità Kiosk "Multi App", l'uso del Launcher AppTec360 sarà obbligatorio.
Applicazioni	Applicazione: Seleziona un'applicazione Playstore o un'applicazione interna come applicazione Kiosk. È anche possibile inserire un nome di pacchetto. L'applicazione Kiosk selezionata deve essere installata sul dispositivo. Ricorda di impostare l'applicazione Kiosk come obbligatoria. Scorciatoia sulla homescreen: Se l'opzione è impostata su "On", verrà creata una scorciatoia sulla homescreen. Se è impostata su "Off", l'app verrà comunque visualizzata nell'elenco delle app.

Password di uscita abilitata	Se attivi questa funzione, l'utente potrà terminare la modalità Kiosk con una password predefinita dall'utente.
Password di uscita	Questa è la password che è stata preimpostata dall'utente
Barra di stato a collasso automatico	Se abilitata, la barra di stato sarà automaticamente in collisione. Con questa opzione gli utenti possono vedere le informazioni della barra di stato, ma non possono accedere alle sue funzioni.
Disabilita la barra di stato	La barra di stato contiene notifiche, scorciatoie e informazioni. Disponibile solo per i dispositivi Samsung con KNOX 1.0 o superiore.
Disabilita i tasti del volume	Disattiva i tasti del volume (disponibile solo sui dispositivi Samsung con KNOX 1.0 o superiore)
Disabilita l'interruttore On/Off	Disabilita l'interruttore On/Off (disponibile solo sui dispositivi Samsung con KNOX 1.0 o superiore)
Disabilita il pulsante Home	Disattiva il pulsante Home. Se questa funzione è stata attivata, la modalità Kiosk può essere interrotta solo dalla Console AppTec360. (disponibile solo su dispositivi Samsung con KNOX 1.0 o superiore)
Disabilita la barra di navigazione	Con questa funzione puoi disabilitare la barra di navigazione (Indietro / Menu). Se questa funzione è stata attivata, la modalità Kiosk può essere interrotta solo dalla Console AppTec360. (disponibile solo su dispositivi Samsung con KNOX 1.0 o superiore)

Impostazioni di aggiornamento dell'app	
Consenti gli aggiornamenti delle app	Agli utenti verrà richiesto di eseguire gli aggiornamenti dell'app anche quando la modalità Kiosk è attiva. Sui dispositivi con Samsung KNOX, le app verranno aggiornate silenziosamente.
Finestra di aggiornamento	Imposta un intervallo di tempo in cui agli utenti verrà richiesto di installare gli aggiornamenti delle app.

TeamViewer	
Abilita l'accesso non presidiato	Se abilitato, gli amministratori possono controllare il dispositivo da remoto senza l'interazione dell'utente. L'applicazione TeamViewer Host deve essere installata sul dispositivo.

AppTec360 Launcher

Abilita il Launcher di AppTec360	On: Attiva il Launcher di AppTec360. L'utente deve impostarlo come launcher predefinito una volta. Nota: se la modalità Kiosk è abilitata e la modalità Kiosk è impostata su "Multi App", l'uso del launcher AppTec360 sarà obbligatorio.
Icone grandi	On: Mostra una versione più grande delle icone delle app nel Launcher.
Nascondi l'icona dell'app AppTec360	Attiva: Nasconde completamente l'applicazione AppTec360
Nascondi l'icona di AppTec360 Store	Attiva: Nasconde completamente l'AppStore di AppTec360 Enterprise.

Impostazioni di AppTec360

Abilita l'applicazione Impostazioni di AppTec360	L'applicazione AppTec360 Settings fornisce il controllo delle connessioni WiFi e Bluetooth.
Abilita le impostazioni in Multi App Modalità chiosco	Se abilitata, gli utenti possono accedere all'applicazione Impostazioni di AppTec360 mentre è attiva la modalità Kiosk Multi App.

Telecomando

Splashtop

Mostra lo stato attuale della configurazione di Splashtop. Qui troverai i passaggi da eseguire per accedere al dispositivo da remoto tramite Splashtop. Qui devi anche inserire il tuo codice di distribuzione che puoi ottenere dal sito web di Splashtop. Il codice di distribuzione è necessario per connettersi al dispositivo.

Teamviewer

Mostra lo stato attuale dell'installazione di Teamviewer. Qui troverai i passaggi da eseguire per accedere al dispositivo da remoto tramite Teamviewer.

Gestione dei contenuti

Contentbox

Qui puoi abilitare il Contentbox per questo dispositivo. Una volta attivata, l'applicazione Contentbox verrà installata sul dispositivo.

Browser sicuro

Qui puoi abilitare il Browser sicuro per questo dispositivo. Una volta attivata, l'applicazione Secure Browser verrà installata sul dispositivo. Questo Browser può essere configurato per offrire un Browser Web sul dispositivo limitato alle tue esigenze.

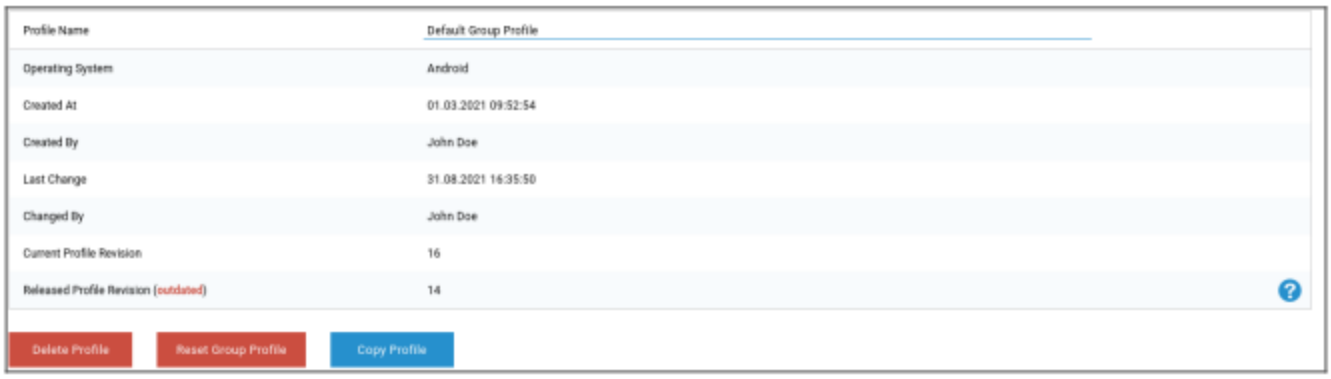
Richiedi la password	Richiedere all'utente di impostare e utilizzare una password per accedere al browser.
Limita i download / Apri in	Blocca i download dai siti web
Limitare i caricamenti	Limita i caricamenti a determinati URL. Non fornire alcun URL per bloccare completamente l'Upload
Consenti la copia	Consente di copiare, tagliare o condividere il testo all'interno delle pagine web.
Consenti la cattura dello schermo	Consente di catturare screenshot.
Frequenza di pulizia dei dati	Seleziona con quale frequenza TUTTI i dati dell'utente (cronologia, cache, ecc.) devono essere rimossi automaticamente.
Segnalibri aziendali	I segnalibri verranno visualizzati nella cartella "segnalibri aziendali" dei segnalibri del browser. Non sono modificabili dall'utente.
Nascondi la barra degli indirizzi	Nasconde la barra degli indirizzi in modo che l'utente non veda l'URL che sta visitando.
Whitelisting nel browser (senza Universal Gateway)	Abilita la whitelist degli URL lato client. - I segnalibri aziendali sono sempre inseriti nella whitelist - Supportato solo per 100 URL - Utilizza il Gateway Universale per un numero illimitato di black- e whitelist
Black- e Whitelist basati su gateway	La blacklist ha i seguenti requisiti: - Un AppTec360 Universal Gateway funzionante ("Impostazioni generali" → "Universal Gateway") - Una configurazione VPN funzionante con un server DNS specificato ("Impostazioni generali" → "Universal Gateway" → "Impostazioni VPN") - Una configurazione Blacklist ("Impostazioni generali" → "Universal Gateway" → "Blacklist domini") - Una connessione VPN valida nel profilo ("Gestione connessioni" → "VPN")

Configurazione PC Windows 10

Generale

Panoramica del profilo del gruppo (solo a livello di gruppo)

Quando apri il profilo di un gruppo, otterrai una rapida panoramica del profilo.



Nome del profilo	Nome del profilo (può essere modificato qui)
Sistema operativo	Sistema operativo per cui è stato creato il profilo
Creato a	Tempo della creazione
Creato da	Il creatore del profilo
Ultimo cambiamento	Ora dell'ultima modifica al profilo
Modificato da	Account che ha apportato le ultime modifiche
Revisione del profilo attuale	Revisione dello stato del profilo salvato
Revisione del profilo rilasciata	Revisione del profilo assegnata ("Assegna ora"). Se l'etichetta mostra " (outdated)" dietro il testo, significa che hai salvato il profilo ma non l'hai ancora assegnato, quindi i dispositivi riceveranno ancora la versione più vecchia.

Panoramica del dispositivo (solo a livello di dispositivo)

Il riepilogo del dispositivo, che contiene quanto segue:

Nome del PC	Nome del PC
Cliente	I dispositivi di tipo Windows
Ultima posizione conosciuta	La latitudine e la longitudine dell'ultima posizione nota del dispositivo
Applicazioni obbligatorie assegnate	Numero di applicazioni obbligatorie assegnate al dispositivo
PC UID	UID del PC
Edizione OS	Mostra la tua edizione di Windows
Versione OS	Versione di Windows attualmente installata
Build del sistema operativo	Build attuale di Windows
Sistema operativo	Sistema operativo attualmente installato
Numero di serie	Numero di serie del dispositivo
Proprietà del dispositivo	Il tipo di proprietà configurato
Tipo di dispositivo	Il tipo di dispositivo
Radicati	Mostra se il dispositivo è rootato
Conforme	Mostra se il dispositivo è conforme
Ultimo visto	Data e ora in cui sono state apportate le modifiche al profilo
Assegnazione dell'utente	Visualizza l'utente o il gruppo a cui questo dispositivo è attualmente assegnato. Puoi spostare il dispositivo selezionando un altro utente o gruppo dall'elenco a discesa.

Impostazioni

Consenti l'aggiornamento automatico	Consenti o meno gli aggiornamenti automatici del sistema operativo.

Revisione della configurazione (solo a livello di dispositivo)

Qui potrai vedere quale profilo di gruppo è stato assegnato al dispositivo.

Se clicchi sul profilo del gruppo, accederai direttamente al profilo e potrai eseguire le impostazioni.

Con il simbolo, puoi riportare le app assegnate alle impostazioni del profilo del gruppo.

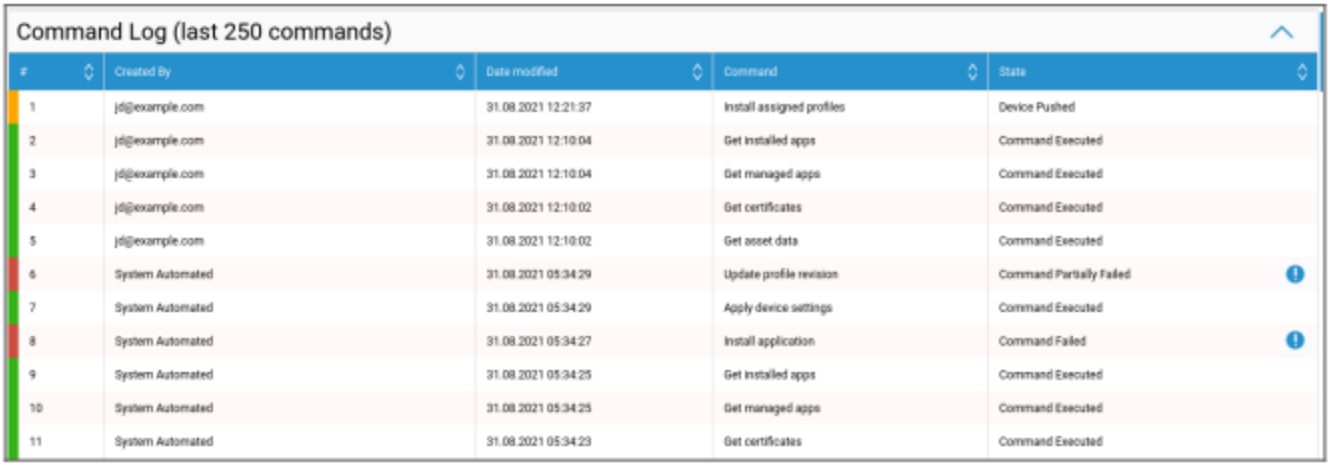
Con il simbolo, puoi reimpostare il profilo del dispositivo in modo che non abbia alcuna impostazione.

L'indicazione "Revisione più recente disponibile" indica che il profilo del gruppo è stato modificato e salvato ma non assegnato. Il profilo del gruppo deve essere assegnato con "Assegna ora" a livello di gruppo per applicare le modifiche ai dispositivi.

Registro del dispositivo (solo a livello di dispositivo)

Registro dei comandi

Qui puoi vedere quali comandi sono stati emessi per il dispositivo e qual è il loro stato.



I comandi creati da "Sistema automatico" vengono creati automaticamente dal sistema.

Possibili stati del comando

Dispositivo spinto	È stata inviata una richiesta push al servizio push (ad esempio APNS) per indicare al dispositivo di connettersi nuovamente al server EMM.
Comando creato	Il comando è stato creato nel sistema.
Comando inviato	Il comando è stato inviato al dispositivo dopo la connessione al server.
Comando eseguito	Il comando è stato eseguito con successo.
Comando fallito	Il comando è fallito. *
Comando parzialmente fallito	A seconda del sistema operativo del dispositivo, alcuni comandi possono essere raggruppati. In questo caso alcune parti di questo gruppo di comandi sono fallite. *
Comando eseguito, alla fine fallito	Il comando è stato eseguito ma forse non lo è stato.
Comando Riportato	Il comando è stato ripreso da un utente.
Scartato	Il comando è stato scartato. Ad esempio perché è stato sostituito da un altro comando o perché il dispositivo è stato reinserito e i vecchi comandi sono stati rimossi.

*Se dietro il messaggio c'è un punto esclamativo, puoi ottenere maggiori informazioni passando il cursore sull'icona.

Gestione delle risorse (solo a livello di dispositivo)

Info sul dispositivo

Produttore	Produttore del dispositivo
Modello	Modello di dispositivo
Numero di modello	Numero di modello
Sistema operativo	Sistema operativo
Versione OS	Versione del sistema operativo
Numero di serie	Numero di serie
ExchangeID	ExchangeID
RAM totale	RAM totale
Risoluzione del display	Risoluzione del display
Lingua del telefono	Lingua del dispositivo
Versione del firmware	Versione del firmware
Versione del client DM	Versione del client di gestione dei dispositivi
Versione hardware	Versione hardware del dispositivo
Architettura della CPU	Architettura della CPU (tipo di processore)

Cellulare

SIM Rete del vettore	Rete di trasportatori
Numero di telefono	Numero di telefono
Stato del roaming	Stato del roaming
IMEI	IMEI
IMSI	IMSI
Firmware del modem	Firmware del modem

Informazioni sulla sincronizzazione

Connessione DM istantanea	Il dispositivo dovrebbe creare immediatamente una connessione con AppTec.
Tempo iniziale di riprova	Tempo di riprova iniziale per questa prima connessione
Tentativi di connessione	Numero di tentativi di connessione dopo una disconnessione dal Connection Manager o un errore a livello di WinInet.
Tempo massimo di sonno	Tempo massimo di sospensione dopo l'errore di invio del pacchetto
Primi tentativi di sincronizzazione	Tempo per la prima fase dopo l'iscrizione
Intervallo del primo tentativo	Tempo per la prima fase dopo l'iscrizione
Secondo tentativo di sincronizzazione	Tempo per la seconda fase dopo l'arruolamento
Intervallo di ripetizione di un secondo	Tempo per la seconda fase dopo l'arruolamento
Riproduzione regolare della sincronizzazione	Tempo per le fasi aggiuntive dopo l'iscrizione
Intervallo regolare di ripetizione	Tempo per le fasi aggiuntive dopo l'iscrizione

Gestione della sicurezza

Antifurto (solo a livello di dispositivo)

Informazioni GPS (solo a livello di dispositivo)

Qui puoi stabilire la posizione attuale/ultima del dispositivo. La localizzazione può essere protetta con una o anche due password - Vedi: "Impostazioni generali" > "Privacy" > "Accesso al GPS".

Impostazioni GPS

Abilita il tracciamento GPS	Abilita la sincronizzazione regolare delle informazioni GPS.
Intervallo di tracciamento	Imposta l'intervallo di sincronizzazione delle informazioni GPS.

Configurazione della sicurezza

Codice di accesso

Lunghezza minima della password	Lunghezza minima della password	
Composizione della password	Specifica il numero di caratteri specifici che la password deve contenere Si tratta di lettere maiuscole, lettere minuscole, numeri e simboli speciali.	
Qualità della password	Qui puoi impostare la qualità della password	
	Alfanumerico	Solo numeri e lettere
	Numerico	Solo numeri
	Numerico o Alfanumerico	Numeri o numeri e lettere
Blocco del tempo massimo di inattività	Numero di minuti di inattività dell'utente sul dispositivo, dopo i quali il dispositivo verrà bloccato. Dopo questo periodo, l'utente deve sbloccare il dispositivo inserendo la propria password.	
Scadenza della password	Imposta il tempo necessario per impostare una nuova password.	
Limitazione della cronologia delle password	Numero di password usate in precedenza che non sono consentite	
Tentativi massimi di password falliti	Numero di volte in cui la password può essere inserita in modo errato, prima che venga eseguita una cancellazione completa del dispositivo.	

Antivirus

Impostazioni antivirus - Imposta la configurazione della scansione	
Tipo di scansione	Seleziona se eseguire una scansione rapida o una scansione completa.
Imposta l'avvio della scansione	Seleziona l'ora del giorno in cui Windows Defender inizierà la scansione.
Frequenza di scansione	Seleziona il giorno in cui la scansione di Windows Defender deve essere eseguita
Frequenza di aggiornamento della firma	Specifica l'intervallo di tempo in ore che verrà utilizzato per verificare la presenza di firme.

Configura il tipo di file da scansionare	
Consente la scansione dei file di archivio	Consentire o meno la scansione degli archivi (ad esempio .zip) quando si accede.
Consenti la scansione degli script	Consente o meno la funzionalità di scansione degli script di Windows Defender.
Consenti la scansione delle e-mail	Consenti o meno la scansione delle e-mail.
Consenti la scansione dei file di rete	Consente o meno la scansione dei file di rete.
Consente la scansione completa delle unità di rete mappate	Consente o non consente la scansione delle unità di rete mappate (abilitata solo quando è abilitata la scansione completa).
Controllo della scansione bidirezionale	Controlla quali set di file devono essere monitorati.
Consente la scansione completa delle unità rimovibili	Consenti o meno la scansione completa delle unità rimovibili. Solo quando viene avviata la scansione completa.

Tipo di file da escludere dalla scansione	
Ignora i tipi di file per la scansione	Definisce un insieme di tipi di estensioni di file. Ogni estensione di file per ogni campo.
Ignora i percorsi delle directory	Definisce un insieme di percorsi di directory per non scansionarli. Un percorso per campo. Esempi: "C:\Example", "C:\Windows" o "C:\Users".
Escludi i processi dalla scansione	Escludi i file che sono stati aperti da processi specifici dalle scansioni di Microsoft Defender Antivirus. . Un percorso per campo. Esempi: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat".

Impostazioni extra	
Consenti il monitoraggio in tempo reale	Consenti o meno la funzionalità di Monitoraggio in tempo reale di Windows Defender
Consenti il monitoraggio del comportamento	Consenti o meno la funzionalità di Monitoraggio del comportamento di Windows
Consenti la protezione del cloud	Consenti o meno a Windows Defender di inviare informazioni a Microsoft su qualsiasi problema riscontrato. Microsoft analizzerà queste informazioni, scoprirà il problema che affligge il dispositivo e offrirà soluzioni migliori.
	Comportamento per l'invio di campioni
Consenti la protezione IOAV di Windows Defender	Consenti o disconosci la protezione IOAV di Windows Defender
Consenti l'accesso all'interfaccia utente di Defenders "Protezione all'accesso".	
Fattore di carico medio della CPU	Rappresenta il fattore di carico medio della CPU per la scansione di Windows Defender (in percentuale).

Gestione del malware	
Bassa gravità	Puoi definire per ogni livello di gravità come il dispositivo gestisce il malware. Le opzioni disponibili sono: • Pulito • Quarantena • Rimuovi • Consenti • Definito dall'utente • Blocco
Gravità moderata	
Gravità elevata	
Gravità grave	
Giorni per conservare il malware pulito	Periodo di tempo in giorni in cui i file/gli elementi in quarantena saranno conservati nel sistema. Il valore predefinito è 0, che mantiene gli elementi in quarantena e non li rimuove automaticamente. Il valore massimo è 90.

Centro di sicurezza

Centro sicurezza di Windows - Impostazioni per la sicurezza di Windows	
Disattiva l'interfaccia utente per la protezione da virus e minacce	
Hide Ransomware Data Recovery UI	
Disattiva la protezione dell'account UI	
Disattiva il firewall e la protezione di rete dell'interfaccia utente	
Disattiva l'interfaccia utente di controllo delle app e del browser	
Disabilita le modifiche alla protezione Exploit	Disabilita l'utente a modificare le impostazioni di protezione dagli exploit
Disattiva l'interfaccia utente di sicurezza del dispositivo	
Nascondi la risoluzione dei problemi del TPM	Nascondi le impostazioni di risoluzione dei problemi del TPM
Disabilita il pulsante Cancella TPM	
Disabilita l'interfaccia utente per le prestazioni e la salute del dispositivo	
Disattiva l'interfaccia utente delle opzioni della famiglia	

Personalizza i brindisi	
Abilita le informazioni di supporto personalizzate	Abilita la visualizzazione delle informazioni di contatto dell'assistenza personalizzata per la tua azienda in basso a destra dell'app del centro di sicurezza.
Indirizzo e-mail	Imposta l'indirizzo e-mail dell'azienda
Nome della società	Imposta il nome dell'azienda
Telefono dell'azienda	Imposta il telefono dell'azienda
URL di aiuto	Imposta l'URL di aiuto dell'azienda

Impostazioni extra	
Disattivare le notifiche	Disattiva la visualizzazione delle notifiche del Centro sicurezza di Windows Defender.
Raccomandazioni per l'aggiornamento del firmware TPM	Nascondi la raccomandazione di aggiornare il firmware TPM quando viene rilevato un firmware vulnerabile.
Visualizza il nome dell'azienda e le opzioni di contatto	Visualizza il nome della tua azienda e le opzioni di contatto in una scheda di contatto che appare nel Centro sicurezza di Windows Defender.
Nascondere il Secure Boot	Nascondi l'area di avvio della sicurezza.
Nascondi il controllo dell'area di notifica della sicurezza	Nascondi il controllo dell'area di notifica di Windows Security.

Configurazione del firewall

Configurazione del firewall - Impostazioni globali	
Ignora l'autenticazione impostata	Ignora l'intero set di autenticazione se non supporta tutte le suite di autenticazione specificate nel set.
Tipo di accodamento dei pacchetti	Specifica come viene abilitato il ridimensionamento del software sul lato di ricezione sia per la ricezione criptata che per il percorso di inoltro per lo scenario del gateway tunnel IPsec.
Disabilita l'esecuzione del filtraggio FTP stateful	Se è disattivato, non esegue il filtraggio stateful del File Transfer Protocol (FTP) per consentire le connessioni secondarie.
Tempo di inattività dell'associazione di sicurezza	Questo campo configura il tempo di inattività dell'associazione di sicurezza, in secondi. Le associazioni di sicurezza vengono eliminate dopo che il traffico di rete non viene visto per un determinato periodo di tempo.
Codifica della chiave preshared	Imposta la codifica della chiave preshared
Eccezioni IPSec	Configurare le eccezioni del protocollo Internet
Controllo della lista di revoca dei certificati	

Profili firewall (Profilo di dominio / Profilo privato / Profilo pubblico)	
Abilita il Firewall per questo profilo	
Disattivare le notifiche	Disabilita la visualizzazione della notifica all'utente quando un'applicazione è bloccata dall'ascolto su una porta.
Bloccare le risposte unicast alle trasmissioni multicast	
Applicare le regole del firewall delle applicazioni autorizzate	Se non viene applicata, le regole del firewall delle applicazioni autorizzate nell'archivio locale vengono ignorate e non applicate.
Applicare le regole del firewall globale delle porte	Se non viene applicata, le regole del firewall della porta globale nell'archivio locale vengono ignorate e non applicate. L'impostazione ha significato solo se è impostata o enumerata nell'archivio dei Criteri di gruppo o se è enumerata dall'archivio GroupPolicyRSoPStore.
Applicare le regole del firewall	Se non viene applicata, le regole del firewall dell'archivio locale vengono ignorate e non applicate.
Applicare le regole di sicurezza delle connessioni	Se non viene applicata, le regole di sicurezza della connessione dell'archivio locale vengono ignorate e non applicate.
Azione in uscita predefinita	L'azione che il firewall esegue per impostazione predefinita sulle connessioni in uscita
Azione in entrata predefinita	L'azione che il firewall esegue per impostazione predefinita sulle connessioni in entrata
Disattiva la modalità Stealth	La modalità Stealth è un meccanismo di Windows Firewall che impedisce agli utenti malintenzionati di scoprire informazioni sui computer della rete e sui servizi che essi eseguono.
Disabilita la prevenzione della risposta al traffico non richiesto	Se disattivate, le regole della modalità stealth del firewall non devono impedire al computer host di rispondere al traffico di rete non richiesto se tale traffico è protetto da IPsec.

Regole del firewall

Regole del firewall	
Nome	Nome della regola
Descrizione	Descrizione della regola
Azione	Specifica se questa regola deve bloccare il traffico o consentirlo. Tieni presente che l'opzione Blocca potrebbe anche bloccare il traffico (a seconda del resto della configurazione) tra il server MDM e il dispositivo.
Direzione	
Abilita l'attraversamento del bordo (disponibile solo quando la **direzione** è impostata sul **traffico in entrata**)	Indica che uno specifico traffico in entrata è autorizzato ad attraversare i NAT e altri dispositivi edge utilizzando la tecnologia di tunneling Teredo.

Programmi e servizi	
Definire le applicazioni, tutto il resto	Se non è abilitato, allora prenderà in considerazione tutte le applicazioni
Nome della famiglia di pacchetti	Il nome della famiglia di pacchetti a cui si applica la regola.
Percorso del file dell'applicazione	L'applicazione completa, ad esempio C:\Windows\System\Notepad.exe, a cui si applicherà la regola
Nome binario completamente qualificato	Il nome binario completamente qualificato a cui si applica la regola. Un FQBN è una stringa nella forma seguente: {Editore/Prodotto/Filename,Versione}
Nome del servizio	Inserisci il nome di un servizio (ad esempio "EventLog"). Puoi ottenere un elenco dei nomi dei servizi con Powershell eseguendo il comando "Get-Service".

Protocolli e porte				
Protocollo	Il protocollo utilizzato dalla regola.			
	Valori disponibili: - Qualsiasi - Personalizzato - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - Percorso IPv6 - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Quando è impostato su Personalizzato	Inserisci un numero di protocollo compreso tra 0 e 255	Il numero di protocollo
		Quando è impostato su TCP o UDP	Specifica le porte locali, altrimenti saranno tutte utilizzate	Le porte locali che la regola utilizzerà, sono ammesse anche le porte di range
			Porto locale	Una singola porta o una serie di porte. Ad esempio, 100-120, 200, 300-320.
			Specifica le porte remote, altrimenti saranno tutte utilizzate	Porte remote che la regola utilizzerà, sono ammesse anche le porte di range
			Porta remota	Una singola porta o una serie di porte. Ad esempio, 100-120, 200, 300-320.

Ambito di applicazione	
Specifica gli IP locali, altrimenti qualsiasi IP	Insieme di IP locali, può essere anche un intervallo di IP separati da -
Indirizzo IP locale	Un insieme di singoli IP o un intervallo di IP separati da -
Specifica gli IP remoti, qualsiasi IP remoto altrimenti	Specifica un insieme di IP remoti, può essere anche un intervallo di IP separati da "-".
Indirizzo IP remoto	Specifica singoli IP o un intervallo di IP
Gettoni	Token che possono essere impostati insieme agli indirizzi remoti. Tokens Intranet, RmtIntranet e Ply2Renders sono supportati in Windows 10, versione 1809 e successive.

Impostazioni avanzate	
Specifica i profili, altrimenti verranno utilizzati tutti	Se disattivato, verranno utilizzati tutti i profili
Dominio	Profilo del dominio
Privato	Profilo privato
Pubblico	Profilo pubblico
Specifica le interfacce, altrimenti saranno tutte utilizzate	Se disabilitato, verranno utilizzate tutte le interfacce
Rete locale	Interfaccia di rete locale
Accesso remoto	Interfaccia di accesso remoto
Senza fili	Interfaccia wireless

Presidi locali	
Aggiungi utenti locali autorizzati	Permetti di aggiungere un elenco di utenti locali che utilizzeranno questa regola
Utenti autorizzati	Elenco degli utenti locali autorizzati per questa regola. L'utente deve essere in formato Security Description Definition language (SDDL), ad esempio PC_NAME\USERNAME. Questo campo non deve essere compilato se il nome di un servizio è impostato per utilizzare questa regola.

Impostazioni di restrizione

Funzionalità del dispositivo

Consenti la scheda SD	Consenti l'utilizzo di una scheda SD
Consenti alla fotocamera	Consenti l'uso della fotocamera
Consenti il servizio di localizzazione	Consenti il servizio di localizzazione del dispositivo
Consenti il Sideloading delle app	Consenti l'installazione di applicazioni da fonti sconosciute
Consenti la modalità sviluppatore	Permette la modalità sviluppatore
Consenti il roaming dei dati cellulari	Consenti il roaming dei dati cellulari
Consenti a Cortana	Consenti all'assistente vocale Cortana
Consenti alla ricerca di utilizzare la posizione	Consenti alla ricerca di utilizzare la posizione
Consenti l'aggiunta di un account e-mail non Microsoft	Specifica se l'utente può aggiungere account e-mail non MSA.
Consenti la connessione dell'account Microsoft	Specifica se consentire l'utilizzo dell'account MSA per l'autenticazione e i servizi di connessione non legati alla posta elettronica.
Consenti la sincronizzazione delle mie impostazioni	Permette la sincronizzazione delle impostazioni su tutto il dispositivo.
Nomi di dominio aziendali protetti	Specifica i nomi dei domini aziendali separati da ";".
Consenti all'utente di disabilitare il	Permette all'utente di disabilitare il Ripristino del Sistema. **ATTENZIONE!**

ripristino del sistema	Questa funzione deve essere utilizzata solo sui dispositivi di proprietà o forniti dall'azienda o dall'organizzazione aziendale o su un dispositivo di proprietà dell'utente, se l'utente consente che il dispositivo sia gestito completamente dall'azienda. Se disattivi questa impostazione di criterio, il Ripristino configurazione di sistema è disattivato e non è possibile accedere alla procedura guidata di Ripristino configurazione di sistema. Anche l'opzione di configurare il Ripristino del sistema o di creare un punto di ripristino attraverso la Protezione del sistema è disattivata.
Consenti la disiscrizione dell'utente	Permette all'utente di rimuovere la parte aziendale dal dispositivo e quindi di disconnettersi dai server AppTec360. In questo caso, non sarà più possibile gestire il dispositivo. **ATTENZIONE!** Questa funzione deve essere utilizzata solo sui dispositivi di proprietà o forniti dall'azienda o dall'organizzazione aziendale o su un dispositivo di proprietà dell'utente, se l'utente consente che il dispositivo sia gestito completamente dall'azienda. Se disattivi questa impostazione di criterio, gli utenti non potranno rimuovere le iscrizioni MDM. Specifica se l'utente può eliminare l'account della postazione di lavoro tramite il pannello di controllo della postazione di lavoro. Il server MDM può sempre eliminare l'account da remoto.

BitLocker

Configurazione di BitLocker

Impostazioni generali	
Richiedi la crittografia del dispositivo	A seconda dell'edizione di Windows e della configurazione del sistema, agli utenti potrebbe essere chiesto di attivare la crittografia del dispositivo: - Per confermare che la crittografia di un altro provider non è abilitata. - Per disattivare BitLocker Drive Encryption e poi riattivare BitLocker.
Metodi di crittografia	
Metodo di crittografia per le unità del sistema operativo	
Metodo di crittografia per unità di dati fisse	
Metodo di crittografia per unità dati rimovibili	
Disattiva l'avviso sulla crittografia dei dischi di terze parti	Disattiva l'avviso di un servizio di crittografia del disco di terze parti in uso sul dispositivo. A partire dalla versione 1803 di Windows 10, questa impostazione è supportata solo per i dispositivi uniti ad Azure Active Directory.
Consenti l'esecuzione della crittografia quando l'utente non amministratore è collegato	È supportato solo per i dispositivi uniti ad Azure Active Directory

Estensioni AppTec360	
Crittografia silenziosa	Se viene selezionato insieme a "Richiedi la crittografia del dispositivo", AppTec360 Management Service eseguirà la crittografia automatica e silenziosa delle unità del dispositivo.
Genera automaticamente le credenziali utente	L'unità OS crittografata sarà protetta da credenziali utente generate automaticamente. O un PIN TPM, quando è disponibile un TPM, o una password testuale di 6 cifre. Le credenziali generate vengono inviate all'indirizzo e-mail registrato per il dispositivo in questione. Se questa opzione è disattivata, l'unica protezione possibile per la crittografia silenziosa è l'utilizzo del TPM. In questo caso, per i dispositivi senza TPM, la crittografia silenziosa fallirà.
Crittografa le unità fisse	Tutte le unità dati fisse disponibili saranno inoltre crittografate e protette con lo "Sblocco Automatico" utilizzando una chiave memorizzata sull'unità OS.

Impostazioni dell'unità del sistema operativo

Richiedi un'autenticazione aggiuntiva all'avvio	Questa impostazione ti permette di configurare se BitLocker richiede un'autenticazione ad ogni avvio del computer. Questa impostazione viene applicata durante la configurazione di BitLocker. Se attivi questa impostazione, gli utenti possono configurare le opzioni di avvio avanzate nella procedura guidata di BitLocker.
Blocca BitLocker senza un TPM compatibile	
Solo TPM	
TPM e PIN	
TPM e chiave	
TPM, chiave e PIN	Se vuoi richiedere l'uso di un PIN e di una chiavetta USB (chiave), l'utente deve configurare BitLocker utilizzando lo strumento da riga di comando "manage-bde" invece della procedura guidata di configurazione di BitLocker Drive Encryption.

Richiedi la lunghezza minima del PIN

	Caratteri minimi

Configura il messaggio e l'URL del recupero pre-avvio	Configura l'intero messaggio di recupero o sostituisci l'URL esistente che viene visualizzato nella schermata di recupero della chiave pre-avvio quando l'unità OS è bloccata. Nota: non tutti i caratteri e le lingue sono supportati nel pre-boot. Si consiglia vivamente di verificare che i caratteri utilizzati vengano visualizzati correttamente nella schermata di ripristino pre-avvio.
	Opzione messaggio di ripristino pre-avvio
	Messaggio di recupero personalizzato
	URL di recupero personalizzato

Opzioni di recupero dell'unità OS		Questa impostazione ti permette di controllare come vengono recuperate le unità del sistema operativo protette da BitLocker in assenza delle credenziali necessarie. Questa impostazione viene applicata durante la configurazione di BitLocker. Per impostazione predefinita è consentito un agente di recupero dati basato su certificati, le opzioni di recupero possono essere specificate dall'utente, compresa la password e la chiave di recupero, e le informazioni di recupero non vengono salvate in AD DS.
	Agente di recupero dati basato su certificati a blocchi	Specifica se un agente di recupero dati può essere utilizzato con le unità del sistema operativo protette da BitLocker. Prima di poter utilizzare un agente di recupero dati, deve essere aggiunto dalla voce Criteri di chiave pubblica nella Console di gestione dei Criteri di gruppo o nell'Editor dei Criteri di gruppo locali. Consulta la BitLocker Drive Encryption Deployment Guide su Microsoft TechNet per maggiori informazioni sull'aggiunta di agenti di recupero dati.
	Impostazioni della password di recupero BitLocker	
	Impostazioni della chiave di recupero BitLocker	
	Salvare le informazioni di recupero di BitLocker nei servizi di dominio di Active Directory	
	Configurazione dello storage di recupero AD DS BitLocker	La memorizzazione del pacchetto di chiavi supporta il recupero dei dati da un'unità danneggiata fisicamente.
	Richiedi l'archiviazione dei dati di recupero in AD DS	Impedisci agli utenti di abilitare BitLocker a meno che il computer non sia connesso al dominio e che non sia stato attivato il sistema.

Impostazioni fisse dell'unità	
Opzioni di recupero delle unità fisse	Questa impostazione ti permette di controllare come vengono recuperate le unità fisse protette da BitLocker in assenza delle credenziali necessarie. Questa impostazione viene applicata durante la configurazione di BitLocker. Per impostazione predefinita è consentito un agente di recupero dati basato su certificati, le opzioni di recupero possono essere specificate dall'utente, compresa la password e la chiave di recupero, e le informazioni di recupero non vengono salvate in AD DS.
Agente di recupero dati basato su certificati a blocchi	
Impostazioni della password di recupero BitLocker	
Impostazioni della chiave di recupero BitLocker	
Salvare le informazioni di recupero di BitLocker nei servizi di dominio di Active Directory	
Configurazione dello storage di recupero AD DS BitLocker	La memorizzazione del pacchetto di chiavi supporta il recupero dei dati da un'unità danneggiata fisicamente.
Richiedi l'archiviazione dei dati di recupero in AD DS	Impedisci agli utenti di abilitare BitLocker a meno che il computer non sia connesso al dominio e il backup delle informazioni di ripristino di BitLocker in AD DS abbia successo. Nota: la password di recupero viene generata automaticamente.
Negare l'accesso in scrittura alle unità fisse non protette	

Impostazioni dell'unità rimovibile	
Negare l'accesso in scrittura alle unità rimovibili non protette	Negare l'accesso in scrittura alle unità dati rimovibili che non sono protette da Bitlocker. Nota: se "Dischi rimovibili: Nega accesso in scrittura" è abilitato nei criteri di gruppo, questa impostazione del criterio verrà ignorata.
Negare l'accesso in scrittura ai dispositivi configurati in un'altra organizzazione	Solo le unità con campi di identificazione corrispondenti a quelli del computer potranno accedere alla scrittura. Questi campi sono definiti dall'impostazione del criterio di gruppo "Fornisci gli identificatori unici per la tua organizzazione".

Stato di BitLocker

Qui puoi vedere lo stato attuale delle unità crittografate con BitLocker

C [OS Drive]
Stato della crittografia
Crittografato (%)
Stato di protezione
Metodo di crittografia
Protezioni per chiavi
Recupero password

Con un clic sul pulsante "Ruota la password di recupero" puoi ruotare la password di recupero di BitLocker.

Gestione dei certificati

Elenco dei certificati

Ecco un elenco dei certificati installati sul dispositivo visualizzato.

Configurazione del certificato

Qui puoi configurare i certificati e le modalità di installazione sul dispositivo.

Certificato attendibile	
Descrizione	Descrizione del certificato
Ambito di applicazione	Ambito di distribuzione del certificato: Utente corrente vs Dispositivo
Negozio di certificati	La funzione "Certificati non attendibili" è disponibile solo a partire da Windows 10, versione 1803.
File di certificato	Carica un file PKCS#1

Certificato di identità			
Descrizione	Descrizione del certificato		
Ambito di applicazione	Ambito di distribuzione del certificato: Utente corrente vs Dispositivo		
Posizione chiave	Il Key Storage Provider in cui installare la chiave privata.		
		TPM. Fallisce se non è presente un TPM	
	TPM. Se non è presente il TPM, si passa al Software KSP.		
	Fornitore di chiavi di archiviazione software	Segna la chiave privata come esportabile	
	Windows Hello per le aziende	Nome del contenitore	Specifica il nome del contenitore di Windows Hello for Business (precedentemente noto come Microsoft Passport for Work).
		Testo del PIN	Specifica il testo personalizzato da mostrare nella richiesta del PIN di Windows Hello for Business durante la registrazione del certificato.
Credenziale	Carica un file PKCS#12		

SCEP

Descrizione	Descrizione del server SCEP		
Ambito di distribuzione	Ambito di distribuzione del certificato: Dispositivo attuale vs Utente		
URL del server SCEP	Uno o più server che rilasciano certificati tramite SCEP		
Oggetto	Rappresentazione di un nome X.500. Ad esempio "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".		
Nomi alternativi del soggetto	Tipo	Indirizzo e-mail	
		DNS	
		URI	
		Nome principale dell'utente (UPN)	
Impronta digitale CA	L'impronta digitale SHA1 del certificato dell'Autorità di Certificazione. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Unità del periodo di validità	Giorni, mesi o anni		
Periodo di validità			
Sfida	Utilizzato come segreto preconfermato per l'iscrizione automatica		
Riprova	Il numero di volte che il dispositivo deve riprovare se il server invia una risposta PENDING. Il valore predefinito è 5. Il valore massimo è 30.		
Ritardo del tentativo	Numero di minuti da attendere prima di riprovare. Il valore predefinito è 5. Il valore minimo è 1.		
Dimensione della chiave	Dimensione della chiave in bit		
Algoritmo di hash	Famiglia di algoritmi di hash		
Utilizzo chiave	L'estensione di utilizzo della chiave definisce lo scopo (ad esempio, cifratura, firma) della chiave contenuta nel certificato. È necessario selezionare almeno una delle opzioni "Firma digitale" o "Cifratura".		
Utilizzo esteso della chiave	Specifica l'utilizzo di chiavi estese, in base alla configurazione del server SCEP. Specifica l'elenco degli OID corrispondenti, ad esempio 1.3.6.1.5.5.7.3.2		

	(Autenticazione client)		
Posizione chiave	Il Key Storage Provider in cui installare la chiave privata.		
		TPM. Fallisce se non è presente un TPM	
	TPM. Se non è presente il TPM, si passa al Software KSP.		
	Fornitore di chiavi di archiviazione software		
	Windows Hello per le aziende	Nome del contenitore	Specifica il nome del contenitore di Windows Hello for Business (precedentemente noto come Microsoft Passport for Work).
		Testo del PIN	Specifica il testo personalizzato da mostrare nella richiesta del PIN di Windows Hello for Business durante la registrazione del certificato.

Gestione delle connessioni

Wifi

Con questa impostazione, esegui la preconfigurazione dei dispositivi dell'utente finale per l'accesso agli Access Point interni.

Identificatore del set di servizi (SSID)	SSID della rete verso la quale verrà stabilita la connessione
Auto Join	Attiva l'adesione automatica alla rete
Rete nascosta	Attiva, nel caso in cui l'AP non trasmetta il SSID

Tipo di sicurezza

Stabilire il tipo di sicurezza dell'AP

Sistema aperto WEP	
Password	Password per l'AP

WPA PSK	
Password	Password per l'AP

WPA EAP	
Tipo di autenticazione	Tipo di autenticazione, possibile solo con "PEAP-MSCAHPv2".
Ricollegamento veloce	I dispositivi possono passare da un Access Point all'altro, senza doversi autenticare di nuovo.
Accesso per gli ospiti	L'utente non dispone di un account e deve quindi registrarsi come ospite.
Controlli di quarantena	Il client deve eseguire i controlli NAP (Network Access Protection) e condividere i risultati con il sistema, che decide se il client può connettersi.
Richiedi un legame crittografico	L'autenticazione è possibile solo tramite il Crypto Binding.
Convalida del server	Il client controlla se il certificato del server è valido. Se questo è il caso, verrà stabilita una connessione
Richiesta di certificati	Permette all'utente di accettare certificati non attendibili.
Nomi dei server	Offre la possibilità di visualizzare il nome del server RADIUS che offre l'autenticazione e l'autorizzazione della rete.

WPA2-PSK	
Password	Password AP

WPA2 EAP	
Tipo di autenticazione	Tipo di autenticazione, possibile solo con "PEAP-MSCAHPv2".
Ricollegamento veloce	
Accesso per gli ospiti	
Controlli di quarantena	Attiva la protezione dell'accesso alla rete NAP
Richiedi il binding crittografico	L'autenticazione è possibile solo tramite il Crypto Binding.
Convalida del server	
Richiesta di certificati	Richiede un certificato di server convalidato, un nome o un certificato di autenticazione di root (CA).
Nomi dei server	Elenco dei server di cui si devono fidare i dispositivi
Nessuno	Nessuna sicurezza stabilita
Usa il server proxy	Utilizzo di un server proxy
Indirizzo del server	Indirizzo del server proxy
Porta del server	Porta del server proxy

Usa il server proxy

Abilita l'uso del server proxy.

Indirizzo del server	Indirizzo del server proxy utilizzato da questa rete.
Porta del server	Porta del server proxy utilizzata da questa rete.

Restrizioni Wifi

Qui puoi definire varie restrizioni Wifi.

Consenti il WiFi	Consenti/rifiuta il WiFi
Consenti la condivisione di Internet	Consenti l'uso di un Hotspot
Consenti la connessione automatica agli hot spot WiFi Sense	Consenti la connessione automatica agli hot spot WiFi Sense
Consenti la configurazione manuale del WiFi	Consentire all'utente di connettersi a reti WiFi che non sono state definite da AppTec.
Frequenza di scansione WLAN	Stabilisce l'intervallo di scansione WLAN. In questo caso, un valore più alto aumenta la capacità di riconoscere le reti WIFI.

VPN

Esegui qui le impostazioni appropriate per configurare le connessioni VPN

Nome della connessione	Nome della connessione indicata		
Tipo di VPN	Una connessione VPN per app viene utilizzata per proteggere il traffico di alcune applicazioni.		
	VPN	Sempre acceso	In questo modo la VPN si connetterà automaticamente al momento dell'accesso e rimarrà connessa fino a quando l'utente non si disconnetterà manualmente.
	VPN per app	Applicazioni VPN	Definisci le applicazioni che utilizzano questa connessione VPN
		Blocco per app	Il blocco per app fa sì che le app selezionate possano connettersi solo attraverso questa connessione VPN. Questa funzione dipende da Windows Defender Firewall.
	Profilo WIP	Dominio WIP per questa connessione	Enterprise ID, necessario per collegare questo profilo VPN a un criterio Windows Information Protection (WIP).

Tipo di connessione

AppTec360 VPN	
Per "AppTec360 VPN" è necessario che il sideloading delle app sia consentito. Abilita l'opzione "Consenti il Sideloading delle app" in "Gestione della sicurezza" → "Impostazioni di restrizione" → "Funzionalità del dispositivo".	
Configurazione del gateway	Per configurare una connessione VPN con blacklist, seleziona una configurazione VPN con un server DNS specificato. Puoi impostare una configurazione VPN in "Impostazioni generali" → "Gateway universale" → "Impostazioni VPN".

IKEv2		
Server	Elenco dei server VPN	
Tunnel del dispositivo	Abilita la connessione prima dell'accesso dell'utente.	
Metodo di autenticazione	EAP	EAP XML
	Certificati macchina	
Algoritmo di crittografia		
Algoritmo di controllo dell'integrità		
Gruppo Diffie-Hellman		
Algoritmo di trasformazione cifrata		
Algoritmo di trasformazione dell'autenticazione		
Gruppo di segretezza in avanti perfetta (PFS)		

PPTP		
Server	Elenco dei server VPN	
Metodo di autenticazione	EAP	EAP XML

L2TP		
Server	Elenco dei server VPN	
Metodo di autenticazione	EAP	EAP XML
Algoritmo di crittografia		
Algoritmo di controllo dell'integrità		
Gruppo Diffie-Hellman		
Algoritmo di trasformazione cifrata		
Algoritmo di trasformazione dell'autenticazione		
Gruppo di segretezza in avanti perfetta (PFS)		

Automatico		
Server	Elenco dei server VPN	
Metodo di autenticazione	EAP	EAP XML

Configurazioni VPN generiche

Ricorda le credenziali ad ogni accesso	
Registra gli indirizzi IP con il DNS interno	
Regole di filtraggio del traffico di rete	Limita la connessione VPN all'insieme di regole definite.
Elenco di ricerca dei suffissi DNS	Suffissi DNS da aggiungere all'elenco di ricerca DNS per l'instradamento dei nomi brevi.
Regole della tabella dei criteri di risoluzione dei nomi (NRPT)	Le regole della Name Resolution Policy table (NRPT) definiscono il modo in cui il DNS risolve i nomi quando si è connessi alla VPN.
Rilevamento della rete affidabile	Elenco dei suffissi DNS per identificare la rete affidabile.
Tunneling diviso	Il tunneling diviso significa che il traffico può passare su qualsiasi interfaccia determinata dallo stack di rete.
Dividere i percorsi di tunneling	Elenco delle rotte da aggiungere alla tabella di routing per l'interfaccia VPN.
Configurazione del proxy	Configura il Proxy utilizzato in questa rete
Indirizzo proxy	Indirizzo del server proxy come nome host completamente qualificato o indirizzo IP.
Porto	Porta del server proxy.
URL di configurazione automatica del proxy	URL per recuperare automaticamente le impostazioni del proxy.

Restrizioni VPN

Qui puoi definire le varie restrizioni della VPN.

Consenti impostazioni VPN	Questa linea guida permette/impedisce all'utente di disattivare e modificare le impostazioni della VPN
Consenti la VPN su cellulare	Consente/impedisce al dispositivo di stabilire una connessione VPN, se il dispositivo utilizza i dati mobili.
Consenti il roaming VPN su cellulare	Consente/impedisce al dispositivo di stabilire una connessione VPN, se il dispositivo è in roaming

Bluetooth

Qui puoi stabilire se il Bluetooth deve essere consentito o meno.

Consenti il Bluetooth	Attiva/disattiva il Bluetooth

Gestione del PIM

Sincronizzazione attiva di Exchange

Impostazione dell'account ActiveSync sul dispositivo dell'utente finale

Nome del conto	Nome dell'account e-mail
Nome host del server	Indirizzo del server/FQDN
Nome di dominio	Dominio del server
Indirizzo e-mail	Indirizzo e-mail
Nome utente	Nome utente
Password utente	Facoltativamente, puoi già allegare una password all'utente
Usa l'SSL	Usa la connessione SSL
Intervallo di sincronizzazione	Qui è possibile stabilire l'intervallo di sincronizzazione Sincronizzazione manuale = L'utente deve scaricare le proprie e-mail ed eseguire una sincronizzazione manuale.
Filtro per l'età della posta	Tempo necessario per la sincronizzazione delle email Nessun filtro = illimitato
Livello del registro	Definizione dei livelli di registrazione per il traffico ActiveSync
Sincronizza l'e-mail	Attivato = le email sono sincronizzate
Sincronizza i contatti	Attivato = i contatti sono sincronizzati
Sincronizza il calendario	Attivato = il calendario è sincronizzato
Sincronizza le attività	Attivato = le attività sono sincronizzate

eMail

Creazione di account POP3/IMAP4 sul dispositivo dell'utente finale.

Descrizione dell'account	Nome dell'account e-mail
Nome del mittente	Nome del mittente visualizzato
Nome di dominio	Nome del dominio per l'account e-mail
Indirizzo e-mail	Indirizzo e-mail dell'utente
Nome utente	Nome utente
Password utente	Facoltativamente, puoi già allegare una password all'utente
Credenziali alternative per il server in uscita	Qui si può definire se sono necessarie altre credenziali per il server in uscita
Nome di dominio in uscita	Nome del dominio in uscita
Nome utente del server in uscita	Nome utente del server in uscita
Password del server in uscita	Password del server in uscita
Protocollo e-mail	POP3 o IMAP4, può essere utilizzato come protocollo
Nome host del server di posta in arrivo	Nome host del server di posta in arrivo
Usa l'SSL per le email in arrivo	Usa l'SSL per le email in arrivo
Nome host del server di posta in uscita	Nome host del server di posta in uscita
Usa l'SSL per le email in uscita	Usa l'SSL per le email in uscita
Autenticazione del server in uscita	È richiesta l'autenticazione del server in uscita
Intervallo di sincronizzazione	Qui è possibile stabilire l'intervallo di sincronizzazione Sincronizzazione manuale = L'utente deve scaricare le proprie e-mail ed eseguire una sincronizzazione manuale.
Filtro per l'età della posta	Tempo necessario per la sincronizzazione delle email Nessun filtro = illimitato

Gestione delle app

Enterprise App Manager

Applicazioni installate

Ecco un elenco delle app attualmente installate sul dispositivo visualizzato.

Applicazioni obbligatorie

Qui puoi configurare un elenco di app obbligatorie sul dispositivo.

Questo elenco verrà controllato ogni volta che il dispositivo si connette all'MDM e installerà tutte le app presenti nell'elenco che risultano non installate sul dispositivo, indipendentemente dal fatto che l'app sia stata disinstallata o che non sia mai stata installata prima.

Puoi caricare le applicazioni Windows 10 In-House e poi aggiungerle a questo elenco oppure puoi aggiungere le configurazioni di Microsoft Office che devono essere configurate in precedenza in "Impostazioni generali" > "Gestione app" > "Microsoft Office".

Restrizioni delle applicazioni di sistema

Applicazioni Inbox
Consenti allarmi e orologio
Consenti la calcolatrice
Consenti alla fotocamera
Consenti di contattare l'assistenza
Consenti a Cortana
Consenti a File Explorer
Consenti di iniziare
Permetti la musica Groove
Permetti le mappe
Consenti la messaggistica
Consenti a Microsoft Edge
Consenti i film e la TV
Consenti il denaro
Consenti le notizie
Consenti a OneDrive
Consenti a OneNote
Consenti il calendario e la posta di Outlook
Consenti alle persone
Consenti il telefono
Consenti le foto
Consenti Powerpoint
Consenti impostazioni
Consenti a Skype
Consenti lo sport
Consenti il negozio
Consenti il registratore vocale
Consenti il portafoglio
Consenti il tempo

Consenti a Windows Feedback Hub
Consenti a Word
Consenti a Xbox

Pagine di impostazione
Consenti account sul posto di lavoro
Consenti informazioni avanzate
Angolo delle applicazioni consentite
Consenti il blocco e il filtro
Consenti il profilo colore
Consenti la modalità di guida
Consenti e-mail e account
Consenti l'equalizzatore
Consenti la tastiera
Consenti la barra di navigazione
Consenti la modalità aereo della rete
Consenti la condivisione di Internet in rete
Consenti i servizi di rete
Consenti rete Wi-Fi
Consenti al sistema Bluetooth del PC
Consenti di valutare il tuo dispositivo
Consenti il ripristino dell'aggiornamento
Consenti la condivisione
Consenti l'avvio
Tempo concesso Lingua
Permetti la regione del tempo
Consenti la schermata di blocco predefinita di Windows
Consenti l'account di lavoro o di scuola

Black- e Whitelisting

In "Black- & Whitelisting", puoi scegliere tra la modalità "Whitelist" e la modalità "Blacklist".

Whitelist	Solo le app e i servizi aggiunti all'elenco possono essere installati sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno attivati e impostati in modo che l'utente possa eseguirli.
	Tutte le altre app non aggiunte all'elenco non possono essere installate sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno disattivati e impostati in modo che l'utente non possa eseguirli.
Lista nera	Le app e i servizi aggiunti all'elenco non possono essere installati sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno disattivati e impostati in modo che l'utente non possa eseguirli.
	Tutte le altre app non aggiunte all'elenco possono essere installate sul dispositivo dell'utente finale. Se questi sono già preinstallati sul dispositivo dell'utente finale, verranno attivati e impostati in modo che l'utente possa eseguirli.

Tramite il pulsante , puoi aggiungere altre app o servizi all'elenco di quelli attualmente utilizzati.

Tramite il pulsante , puoi aggiungere altre applicazioni o servizi all'elenco attualmente inattivo.

Puoi aggiungere un'applicazione dal "Windows App Store" o inserire direttamente un "identificatore di app" da aggiungere alla black- o whitelist.

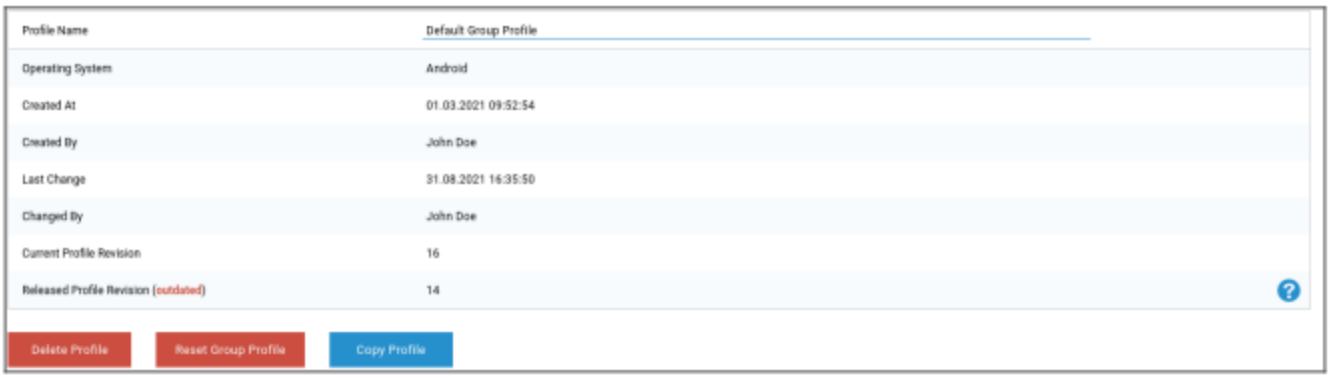
Configurazione MacOS

A seconda che tu abbia selezionato un profilo o un dispositivo, la visualizzazione e i relativi sottopunti sono diversi: presta molta attenzione a questo aspetto!

Generale

Panoramica del profilo del gruppo (solo a livello di gruppo)

Quando apri il profilo di un gruppo, otterrai una rapida panoramica del profilo.



Nome del profilo	Nome del profilo (può essere modificato qui)
Sistema operativo	Sistema operativo per cui è stato creato il profilo
Creato a	Tempo della creazione
Creato da	Il creatore del profilo
Ultimo cambiamento	Ora dell'ultima modifica al profilo
Modificato da	Account che ha apportato le ultime modifiche
Revisione del profilo attuale	Revisione dello stato del profilo salvato
Revisione del profilo rilasciata	Revisione del profilo assegnata ("Assegna ora"). Se l'etichetta mostra " (outdated)" dietro il testo, significa che hai salvato il profilo ma non l'hai ancora assegnato, quindi i dispositivi riceveranno ancora la versione più vecchia.

Panoramica del dispositivo (solo a livello di dispositivo)

La panoramica riassuntiva del dispositivo.

Nome del dispositivo	Nome del dispositivo
Modello	Modello
Sistema operativo	Sistema operativo
Numero di serie	Numero di serie del dispositivo
Proprietà del dispositivo	Il tipo di proprietà configurato
Tipo di dispositivo	Il tipo di dispositivo
Conforme	Mostra se il dispositivo è conforme
Indirizzo IP	L'indirizzo IP da cui il dispositivo si è collegato al server
Ultimo visto	Ora dell'ultima connessione dal dispositivo
Ultima spinta	Ora dell'ultimo push inviato al dispositivo
Assegnazione	Qui puoi spostare il dispositivo ad un altro utente o gruppo.

Revisione della configurazione (solo a livello di dispositivo)

Qui potrai vedere quale profilo di gruppo è stato assegnato al dispositivo.

Se clicchi sul profilo del gruppo, accederai direttamente al profilo e potrai eseguire le impostazioni.

Con il simbolo, puoi riportare le app assegnate alle impostazioni del profilo del gruppo.

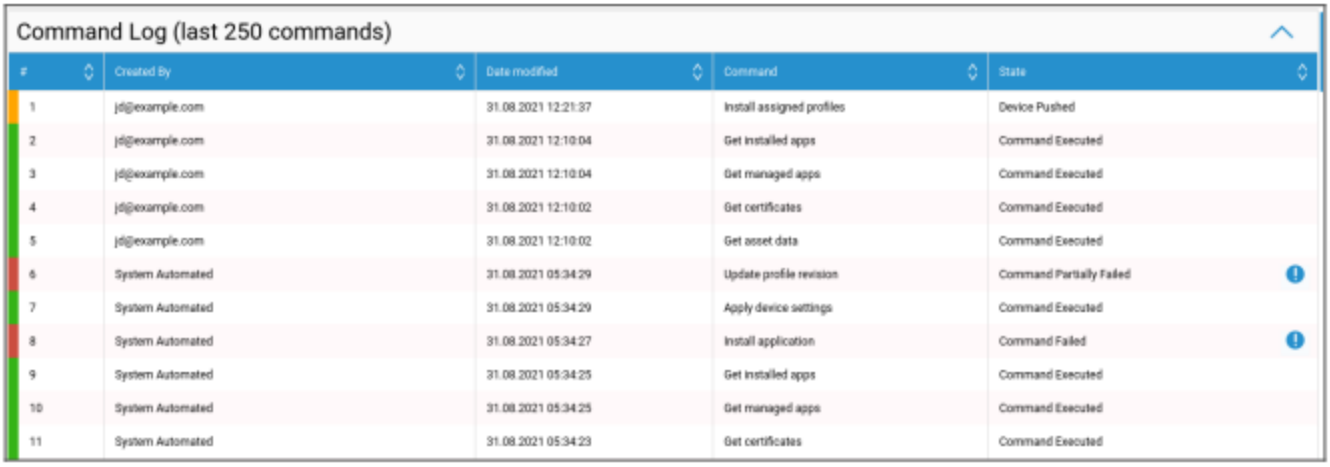
Con il simbolo, puoi reimpostare il profilo del dispositivo in modo che non abbia alcuna impostazione.

L'indicazione "Revisione più recente disponibile" indica che il profilo del gruppo è stato modificato e salvato ma non assegnato. Il profilo del gruppo deve essere assegnato con "Assegna ora" a livello di gruppo per applicare le modifiche ai dispositivi.

Registro del dispositivo (solo a livello di dispositivo)

Registro dei comandi

Qui puoi vedere quali comandi sono stati emessi per il dispositivo e qual è il loro stato.



I comandi creati da "Sistema automatico" vengono creati automaticamente dal sistema.

Possibili stati del comando

Dispositivo spinto	È stata inviata una richiesta push al servizio push (ad esempio APNS) per indicare al dispositivo di connettersi nuovamente al server EMM.
Comando creato	Il comando è stato creato nel sistema.
Comando inviato	Il comando è stato inviato al dispositivo dopo la connessione al server.
Comando eseguito	Il comando è stato eseguito con successo.
Comando fallito	Il comando è fallito. *
Comando parzialmente fallito	A seconda del sistema operativo del dispositivo, alcuni comandi possono essere raggruppati. In questo caso alcune parti di questo gruppo di comandi sono fallite. *
Comando eseguito, alla fine fallito	Il comando è stato eseguito ma forse non lo è stato.
Comando Riportato	Il comando è stato ripreso da un utente.
Scartato	Il comando è stato scartato. Ad esempio perché è stato sostituito da un altro comando o perché il dispositivo è stato reinserito e i vecchi comandi sono stati rimossi.

*Se dietro il messaggio c'è un punto esclamativo, puoi ottenere maggiori informazioni passando il cursore sull'icona.

Gestione delle risorse (solo a livello di dispositivo)

Info sul dispositivo

Numero di modello	Numero di modello
Nome host	Nome host
Nome host locale	Nome host locale
Sistema operativo	Sistema operativo
Versione OS	Versione del sistema operativo
UDID	UDID
Memoria libera / totale	Memoria libera / totale

WiFi

Indirizzo IP	Indirizzo IP
WiFi MAC	WiFi MAC

Cellulare

Numero di telefono	Numero di telefono
Stato del roaming	Stato del roaming
Roaming (voce/dati)	Roaming (voce/dati)
Indirizzo IP	Indirizzo IP
Operatore/Vettore	Operatore/Vettore
SIM Rete del vettore	Rete di trasportatori
Versione per il trasporto	Versione per il trasporto
ICCID	ICCID
Attuale MCC/MNC	Attuale MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

MAC Bluetooth	MAC Bluetooth

Gestione degli aggiornamenti (solo a livello di dispositivo)

Aggiornamenti

Questa scheda mostra informazioni sulle impostazioni di aggiornamento del sistema del dispositivo.

Autocheck abilitato	Se il sistema controlla automaticamente l'aggiornamento.
Aggiornamento automatico delle app abilitato	Se il sistema installa automaticamente gli aggiornamenti delle app.
Aggiornamenti automatici del sistema operativo abilitati	Se il sistema installa automaticamente gli aggiornamenti del sistema operativo.
Aggiornamenti automatici di sicurezza abilitati	Se il sistema installa automaticamente gli aggiornamenti di sicurezza.
Aggiornamento dell'app in background - Download abilitato	Se il sistema scarica gli aggiornamenti delle app in background.
URL del catalogo	L'URL del catalogo degli aggiornamenti software che il client sta utilizzando.
È il catalogo predefinito	Se "sì", Catalog è il catalogo predefinito.
Esegui un controllo periodico	Se "sì", avvia una nuova scansione.
Data della scansione precedente	La data dell'ultima scansione di aggiornamento del software.
Risultato della scansione precedente	Il codice del risultato dell'ultima scansione dell'aggiornamento software.

Gestione della sicurezza

Anti Furto

Pulisci e blocca

Pulizia completa	Invia un comando per resettare il dispositivo
Pulizia aziendale	Rimuovi l'MDM dal dispositivo e rimuovi tutti i dati MDM (ad esempio, account e applicazioni).
Schermata di blocco	Fai in modo che il dispositivo torni alla schermata di blocco

Configurazione della sicurezza

Codice di accesso

Disattivazione del codice consentita	Determina se l'utente è obbligato a impostare un PIN. La semplice impostazione di questo valore (e non di altri) obbliga l'utente a inserire un codice di accesso, senza imporre una lunghezza o una qualità.
Consenti un valore semplice	Consenti all'utente di utilizzare stringhe di numeri uguali, crescenti e decrescenti (es. 1234, 1111).
Richiedi un valore alfanumerico	Le password devono contenere almeno una lettera
Lunghezza minima del codice di accesso	Lunghezza minima della password
Numero minimo di caratteri complessi	Numero minimo di simboli alfanumerici nella password
Età massima del codice di accesso	Numero di giorni dopo i quali la password deve essere cambiata
Blocco automatico massimo	Tempo massimo dopo il quale il dispositivo viene bloccato
Periodo massimo di tolleranza per il blocco del dispositivo	Per quanto tempo il dispositivo può essere bloccato senza che venga richiesto il codice di accesso al momento dello sblocco.
Età massima del passcode (1-730 giorni, o nessuno)	Giorni dopo i quali il codice di accesso deve essere cambiato
Cronologia dei codici (1-50 codici o nessuno)	Numero di passcode unici prima del riutilizzo

Certificato

PKCS#1	
Descrizione	Inserisci una descrizione per il certificato
Credenziale	Carica un file pkcs1

PKCS#12	
Descrizione	Inserisci una descrizione per il certificato
Credenziale	Carica un file pkcs12

Impostazioni di restrizione

Funzionalità del dispositivo

Consenti alla fotocamera	Consenti l'uso della fotocamera
Consenti Game Center	Quando è falso, Game Center viene disattivato e la sua icona viene rimossa dalla schermata iniziale.
Consentire il gioco in multiplayer	Quando è falso, proibisce il gioco multiplayer.
Consente di aggiungere amici a Game Center	Quando è falso, vieta l'aggiunta di amici a Game Center.
Consenti la Libreria foto di iCloud	Se impostato su false, disattiva la Libreria foto di iCloud. Le foto non completamente scaricate dalla Libreria foto di iCloud sul dispositivo verranno rimosse dall'archivio locale.
Consenti Touch ID	Se falso, impedisce a Touch ID di sbloccare un dispositivo.

iCloud

Blocca alcune funzionalità durante l'accoppiamento con iCloud

Consenti la sincronizzazione dei documenti	Consenti la sincronizzazione dei documenti
Consenti la sincronizzazione del Portachiavi iCloud	Consenti la sincronizzazione del Portachiavi iCloud
Consenti le note di iCloud	Quando è falso, disattiva i servizi iCloud Notes di macOS.
Consenti iCloud BTMM	Quando è falso, disattiva il servizio iCloud di MacOS Torna al mio Mac.
Consenti iCloud FMM	Quando è falso, disattiva il servizio iCloud di MacOS Trova il mio Mac.
Consenti i segnalibri di iCloud	Quando è falso, disattiva la sincronizzazione dei segnalibri iCloud di MacOS.
Consenti la posta di iCloud	Quando è falso, disattiva i servizi iCloud di MacOS Mail.
Consenti il Calendario iCloud	Quando è falso, disattiva i servizi iCloud di MacOS Cloud.
Consenti i promemoria di iCloud	Quando è falso, disattiva i servizi di promemoria di iCloud.

Consenti la rubrica di iCloud	Quando è falso, disattiva i servizi della Rubrica iCloud di macOS.

Gestione dei media

Espulsione al logout	Espelli tutti i supporti rimovibili al logout
Consenti alla rete	Consenti l'accesso ai media di rete
Consenti il disco interno	Consenti l'accesso al disco interno.
Richiedi l'autenticazione	Richiedi l'autenticazione per l'utilizzo di questo supporto
Solo lettura	L'utente è in grado di leggere i dati solo dal supporto
Consenti disco esterno	Consenti l'accesso al disco esterno.
Richiedi l'autenticazione	Richiedi l'autenticazione per l'utilizzo di questo supporto
Solo lettura	L'utente è in grado di leggere i dati solo dal supporto
Consenti l'utilizzo di immagini disco	Consenti l'accesso alle immagini.
Richiedi l'autenticazione	Richiedi l'autenticazione per l'utilizzo di questo supporto
Solo lettura	L'utente è in grado di leggere i dati solo dal supporto
Consente l'utilizzo di DVD-RAM	Consenti l'accesso al disco DVD-RAM.
Richiedi l'autenticazione	Richiedi l'autenticazione per l'utilizzo di questo supporto
Solo lettura	L'utente è in grado di leggere i dati solo dal supporto
Consenti l'utilizzo di DVD	Consenti l'accesso al disco DVD.
Richiedi l'autenticazione	Richiedi l'autenticazione per l'utilizzo di questo supporto
Consenti l'uso dei CD	Consenti l'accesso al disco CD.
Richiedi l'autenticazione	Richiedi l'autenticazione per l'utilizzo di questo supporto

Gestione delle connessioni

Wi-Fi

Qui puoi aggiungere e configurare le connessioni Wi-Fi

Identificatore del set di servizi (SSID)	SSID della rete alla quale verrà stabilita la connessione
Auto Join	Abilita l'auto join per la rete
Rete nascosta	Abilita, nel caso in cui l'AP non trasmetta l'SSID
Configurazione del proxy	Configurazione di un proxy per ogni punto di accesso
Nessuno	Non utilizzare un server proxy
Manuale	Stabilire un Proxy manuale
URL del server proxy	Indirizzo per accedere alle impostazioni del proxy
Porto	Stabilisci la porta per il Proxy
Autenticazione	Nome utente per l'autenticazione sul Proxy
Password	Password per l'autenticazione sul Proxy
Automatico	Stabilisci automaticamente un Proxy
URL del server proxy	URL del file delle impostazioni del proxy
Tipo di sicurezza	Stabilire il tipo di sicurezza per l'AP
WEP	
Password	Password per l'AP
WPA/WPA2	
Password	Password per l'AP
WEP Enterprise - WPA / WPA2 Enterprise / Qualsiasi impresa	Vedi Tabella Errore: Fonte di riferimento non trovata
Nessuno	Non stabilire alcuna sicurezza
Disabilita la randomizzazione dell'indirizzo MAC	Disattiva la randomizzazione dell'indirizzo MAC per quella rete Wi-Fi mentre è associata alla rete. Inoltre, nelle Impostazioni viene visualizzato un avviso sulla privacy che indica che il network ha ridotto le protezioni sulla privacy.

Configurazione Wi-Fi aziendale

Nota: è disponibile solo se "Tipo di sicurezza" è impostato su un tipo Enterprise.

Protocolli	Protocollo di autenticazione supportato dalla rete di destinazione
TLS	Abilita / Disabilita l'uso
TTLS	Abilita / Disabilita l'uso
Autenticazioni interne	Protocollo di autenticazione da utilizzare: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Abilita / Disabilita l'uso
PEAP	Abilita / Disabilita l'uso
EAP-FAST	Abilita / Disabilita l'uso
EAP-SIM	Abilita / Disabilita l'uso
Usa il PAC	Uso del PAC (Controllo dell'accesso protetto)
Provvedimento PAC	Configurazione di Provision PAC
Fornitura di PAC in forma anonima	Fornitura anonima di PAC
Autenticazione	
Nome utente	Nome utente di autenticazione
Non usare Per connessione Password	Non usare la password per la connessione
Password	La password da utilizzare
Certificato di identità	Carica/seleziona il certificato di autenticazione
Identità esterna	Identità visibile all'esterno
Fiducia	
Certificato di fiducia 1	Carica il primo certificato attendibile
Certificato di fiducia 2	Carica il secondo certificato attendibile
Certificato di fiducia 3	Carica un terzo certificato attendibile
Server di fiducia Nomi dei certificati	I nomi dei certificati del server previsti (in un elenco separato da virgole)

VPN

A seconda del tipo di connessione selezionata, possono essere visibili campi diversi.

Nome della connessione	Nome del profilo VPN
Tipo di VPN	
VPN	Tutto il traffico di rete del dispositivo sarà instradato attraverso una connessione VPN.
Tipo di connessione	Stabilisci il tipo di connessione VPN
IPsec (cisco)	Protocollo IPsec di cisco
L2TP	Protocollo L2TP
SSL personalizzato	Connessione tramite SSL personalizzato
IKEv2	Protocollo IKEv2
Configurazione del proxy	Configurazione di un Proxy per la connessione VPN
Nessuno	Non stabilire un Proxy
Manuale	Stabilire manualmente un Proxy
URL del server proxy	Indirizzo per accedere alle impostazioni del proxy
Porto	Stabilisci la porta per il Proxy
Autenticazione	Nome utente per l'autenticazione al Proxy
Password	Password per l'autenticazione al Proxy
Automatico	Stabilisci automaticamente un Proxy
URL del server proxy	URL per accedere alle impostazioni del Proxy

Proxy HTTP

Tipo di proxy	
Manuale	Stabilisci un Proxy manualmente
URL del server proxy	Indirizzo per accedere alle impostazioni del Proxy
Porto	Stabilisci la porta Proxy
Autenticazione	Nome utente per l'autenticazione al Proxy
Password	Password per l'autenticazione al Proxy
Automatico	Stabilisci automaticamente un Proxy
URL PAC proxy	URL PAC proxy
Consenti la connessione diretta se il PAC non è raggiungibile	Consenti la connessione diretta (senza VPN), se il PAC non è raggiungibile
Consente di bypassare il proxy per accedere a reti riservate	Consente di bypassare il proxy per accedere a reti interne vincolate

AirPrint

Indirizzo IP	Indirizzo IP della stampante
Percorso delle risorse	Percorso definito per il dispositivo AirPrint

AirPlay

Nome del dispositivo	Nome del dispositivo
Password	Password di accoppiamento
Whitelist	Definisci un elenco di dispositivi con cui il dispositivo può accoppiarsi in modo esclusivo

Gestione del PIM

Sincronizzazione attiva di Exchange

Nome del conto	Nome del conto.
Indirizzo e-mail	L'indirizzo dell'account (ad esempio max@company.com)
Nome host del server	Hostname interno
Nome utente	"Dominio" e "Nome di accesso" devono essere vuoti affinché il dispositivo richieda l'utente.
Dominio	"Dominio" e "Nome di accesso" devono essere vuoti affinché il dispositivo richieda l'utente. Se è abilitata una configurazione ACL Gateway e il campo Dominio non è vuoto, AppTec360 Universal Gateway autenticherà il dispositivo con il seguente nome "Dominio".
Password	La password dell'account (ad esempio secretUserPassword)
Giorni passati di Mail to Sync	Il numero di giorni passati di posta da sincronizzare
Usa l'SSL	Usa SSL per l'host interno di Exchange
Opzione avanzata	Mostra le opzioni avanzate
Porta del server	Porta interna
Percorso del server	Percorso interno
Nome host esterno	Host esterno
Porta esterna	Porta esterna
Percorso esterno	Percorso esterno
Usa l'SSL per l'esterno Host di scambio	Usa SSL per l'host esterno di Exchange

eMail

Configurazione di account POP3 / IMAP sul dispositivo dell'utente finale

Descrizione dell'account	Nome degli account e-mail
Tipo di conto	
IMAP	
Prefisso del percorso	Il prefisso di percorso per le cartelle speciali
POP	
Nome visualizzato dall'utente	Nome utente visualizzato
Indirizzo e-mail	Indirizzo e-mail dell'utente

Posta in arrivo	Impostazioni del server in entrata
Indirizzo del server di posta	Indirizzo del server di posta
Porta del server di posta	Porta del server di posta
Nome utente	Nome utente rispettivo
Tipo di autenticazione	Tipo di autenticazione
Nessuno	Nessun tipo di autenticazione
Password (solo a livello di dispositivo)	Richiesta di password
Sfida-Risposta MDM	
NTLM	Autenticazione NTLM
Digest MD5 HTTP	
Usa l'SSL	Usa l'SSL, se necessario

Posta in uscita	Impostazioni del server in uscita
Indirizzo del server di posta	Indirizzo del server di posta
Porta del server di posta	Porta del server di posta
Nome utente	Nome utente rispettivo
Tipo di autenticazione	
Nessuno	Nessun metodo di autenticazione
Password (solo a livello di dispositivo)	Richiesta di password
Sfida-Risposta MDM	
NTLM	Autenticazione NTLM
Digest MD5 HTTP	
Usa l'SSL	Usa l'SSL, se necessario
La password in uscita è la stessa di quella in entrata	La password in uscita è la stessa di quella in entrata
Utilizzare solo per la posta	Attiva, se tutte le e-mail in uscita devono essere inviate tramite la Mail-App

CalDav

Configura la configurazione e la distribuzione di un account CalDav

Descrizione dell'account	Nome visualizzato dell'account
Nome host	Nome host e/o indirizzo IP
Porto	Porta dell'account CalDav
URL principale	URL principale dell'account
Nome utente	Nome utente CalDav corrispondente
Password (solo a livello di dispositivo)	La rispettiva password CalDav
Usa l'SSL	Usa l'SSL, se necessario

CardDav

Configurare la configurazione e la distribuzione di un account CardDav

Descrizione dell'account	Nome visualizzato dell'account
Nome host	Nome host e/o indirizzo IP
Porto	Porta dell'account CardDav
URL principale	URL principale dell'account
Nome utente	Nome utente CardDav corrispondente
Password (solo a livello di dispositivo)	Password CardDav corrispondente
Usa l'SSL	Usa l'SSL, se necessario

LDAP

In quest'area, imposta una connessione LDAP per consentire lo scambio dinamico di certificati tra il dispositivo dell'utente finale e Active Directory.

Ricorda che l'utente selezionato deve avere i rispettivi permessi di lettura.

Descrizione dell'account	Descrizione dell'account
Nome utente dell'account	Utente per l'accesso a LDAP
Password dell'account	Password per l'accesso a LDAP
Nome host dell'account	Nome host/indirizzo IP del server LDAP
Usa l'SSL	Usa l'SSL, se necessario

Nella seconda parte, puoi definire dei filtri individuali per la ricerca nel registro LDAP.

Descrizione	Ambito di applicazione	Base di ricerca
Descrizione del filtro	Livello di ricerca nel registro LDAP	Definisci il filtro individuale

Dashboard e reportistica

Impostazioni del cruscotto

Qui puoi vedere quali dashboard esistono, modificarli o crearne di nuovi. Ogni dashboard ha un proprio set di dati da mostrare e una configurazione grafica.

Controllo delle impostazioni della dashboard

Pubblico	Imposta la Dashboard pubblica, in modo che altri utenti possano vederla. Naturalmente gli utenti devono poter accedere e visualizzare le dashboard. Se l'opzione "Pubblico" non è attivata, solo il creatore può vederla.
Predefinito	Imposta la Dashboard come predefinita in modo che si apra automaticamente la prossima volta che accedi alla vista Dashboard.
	Mostra la dashboard e i suoi grafici
	Elimina la dashboard
	Modifica il nome e le impostazioni della dashboard
	Crea una copia della dashboard
	Aggiungi una dashboard completamente nuova

Vista del cruscotto

Mostra i dati e i grafici del Dashboard selezionato e ti permette di modificarli.

Controllo del cruscotto

	Permette di definire quali dati vengono mostrati nella Dashboard, la quantità di dati da mostrare e le dimensioni di questi dati.
	Ti riporta alla Panoramica del cruscotto
	Riporta la Dashboard aperta al suo valore predefinito.
	Salva tutte le modifiche apportate alla Dashboard attualmente aperta (ad esempio, quali dati mostrare).
	Cambia il tipo di grafico in grafico a pilastri
	Cambia il tipo di grafico in grafico a torta
	Cambia il tipo di grafico in grafico a ciambella
	Cambia il tipo di grafico in grafico ad area polare
	Cambia l'ordine di ordinamento

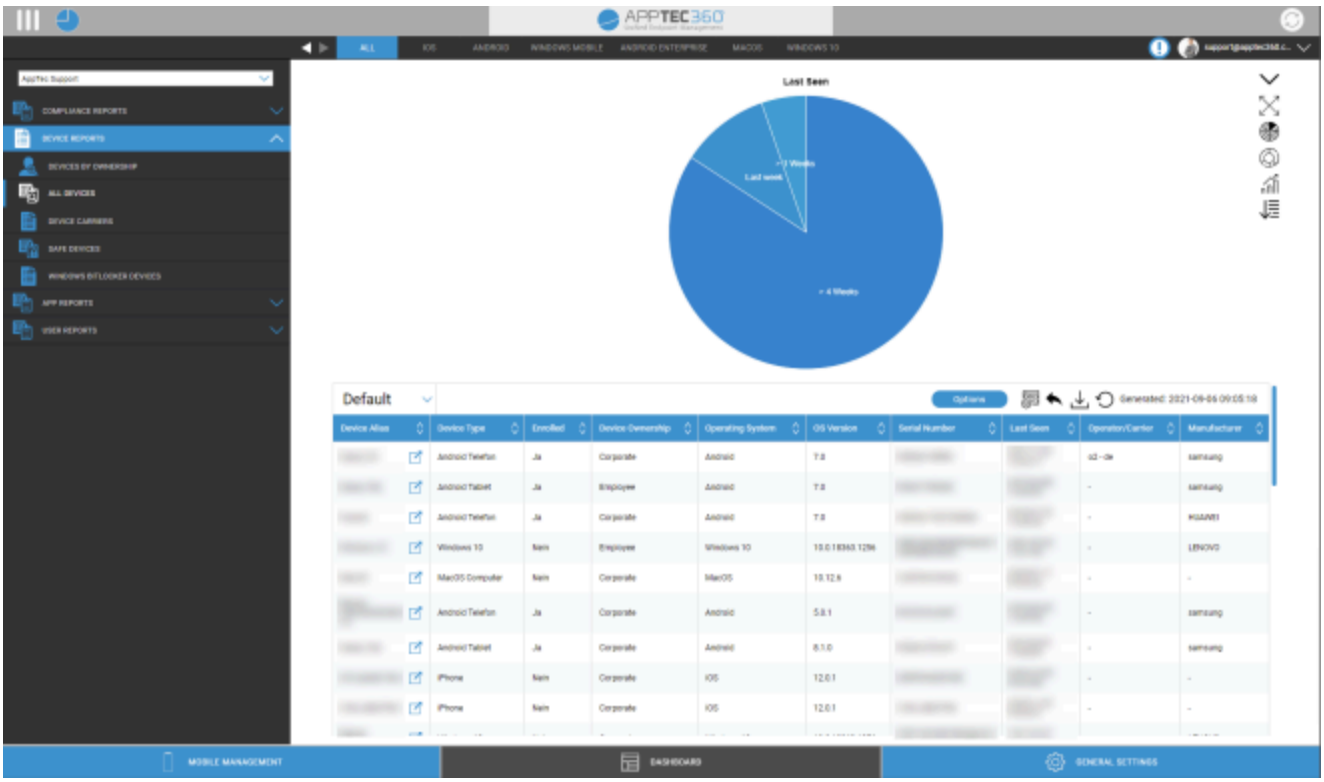
Reporting esteso

Il "Reporting esteso" offre panoramiche e grafici dettagliati sulle informazioni relative a dispositivi e utenti.

Ci sono alcuni Report predefiniti, ma tutti possono essere modificati manualmente per aggiungere o rimuovere dati da mostrare.

Tieni presente che puoi modificare solo manualmente i dati visualizzati. La categoria di report selezionata definisce i dati su cui si basa. Ad esempio, non sarai mai in grado di vedere i dispositivi Android nel rapporto iOS in Rapporti dispositivi Tutti i dispositivi iOS

In alto a sinistra puoi limitare i dati del report a un determinato gruppo (e a tutti i suoi sottogruppi). Per impostazione predefinita è impostato sul nodo principale, quindi tiene conto di TUTTI i dispositivi e gli utenti.



Controllo esteso dei rapporti

In ogni panoramica puoi utilizzare le seguenti funzioni per modificare il report nel modo che desideri:

	Nascondi il grafico (se il grafico è visualizzato)
	Mostra il grafico (se il grafico è nascosto)
	Espandi il grafico (se il grafico è chiuso)
	Chiudi il grafico (se il grafico è espanso)
	Cambia il tipo di grafico in grafico a pilastri
	Cambia il tipo di grafico in grafico a torta
	Cambia il tipo di grafico in grafico a ciambella
	Cambia il tipo di grafico in grafico ad area polare
	Cambia l'ordine di ordinamento
	Modifica le seguenti parti della panoramica visualizzata: • Aggiungi/rimuovi colonne • Specificare l'ordine di visualizzazione delle colonne • Mostra/nascondi il grafico sopra la tabella • Seleziona la colonna da utilizzare per il grafico • Filtra i dati della tua tabella
	Apri il gestore delle configurazioni per salvare e caricare diversi report
	Riporta il Report attualmente aperto al valore predefinito
	Esporta il rapporto corrente come file .csv
	Rigenerare i dati e ricaricare il rapporto corrente

Puoi trovare un elenco di tutti i report predefiniti nelle pagine successive.

Rapporti di conformità

Dispositivi radicati

Panoramica dei dispositivi che sono stati rooted/jailbroken.

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Sistema operativo
Numero di telefono
Ultimo visto
Produttore

Dispositivi in roaming

Panoramica di tutti i dispositivi in roaming

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Tipo di dispositivo
Sistema operativo
Numero di telefono
Ultimo visto

Dispositivi abilitati al roaming

Panoramica di tutti i dispositivi che hanno attivato il roaming ma che non sono necessariamente in roaming.

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Tipo di dispositivo
Sistema operativo
Numero di telefono
Ultimo visto

Dispositivi supervisionati

Panoramica di tutti i dispositivi supervisionati in modalità supervisionata (solo iOS)

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Tipo di dispositivo
Ultimo visto

Dispositivi inattivi

Panoramica di tutti i dispositivi che non si sono connessi al server negli ultimi 7 giorni

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Tipo di dispositivo
Sistema operativo
Ultimo visto

Rapporti sui dispositivi

Dispositivi per proprietà

Qui puoi vedere quanti dispositivi sono stati attualmente distribuiti come dispositivi aziendali (dispositivi aziendali) e dipendenti (dispositivi privati).

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
Tipo di dispositivo
Proprietà del dispositivo
Sistema operativo

Tutti i dispositivi

Qui puoi vedere una panoramica di tutti i dispositivi con le informazioni più importanti.

Colonne predefinite di questo report:

Alias del dispositivo
Tipo di dispositivo
Iscritta
Proprietà del dispositivo
Sistema operativo
Versione OS
Numero di serie
Ultimo visto
Operatore/Vettore
Produttore

Portatori di dispositivi

Qui puoi vedere una panoramica sull'operatore (provider di telefonia mobile).

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Sistema operativo
Versione OS
Operatore/Vettore

Dispositivi SAFE

Qui puoi vedere una panoramica dei dispositivi che utilizzano la versione SAFE.

Poiché la panoramica e/o SAFE è disponibile solo per i dispositivi Samsung, non vedrai le solite schede sotto questo punto.

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail
Tipo di dispositivo
Ultimo visto
Versione SAFE

Dispositivi Windows BitLocker

Qui puoi vedere una panoramica dei dispositivi Windows che utilizzano BitLocker.

Colonne predefinite di questo report:

Alias del dispositivo
Proprietario del dispositivo
E-mail

Stato di BitLocker

Rapporti sulle app

Qui puoi trovare una serie di panoramiche sulle app. In tutti questi rapporti puoi cliccare su una voce per vedere quali versioni sono installate sui dispositivi e con quale frequenza. In questa vista puoi cliccare nuovamente su una versione specifica per vedere quali dispositivi hanno installato questa versione specifica.

Nota: potrebbe essere necessario un po' di tempo prima che il sistema riceva informazioni aggiornate dal dispositivo. Inoltre, i rapporti non vengono aggiornati ogni minuto. Potresti dover pazientare per vedere lo stato attuale se hai appena assegnato una nuova applicazione o versione. Ricaricando manualmente il report, questo mostrerà i dati più aggiornati disponibili.

Applicazioni installate

Qui puoi avere una panoramica di tutte le app installate.

Colonne predefinite di questo report:

Nome	Nome della rispettiva applicazione e/o servizio
Identificatore	ID app/servizio definito
Conteggio totale	Con quale frequenza questa applicazione/servizio è stata installata sui dispositivi dell'utente finale

Le applicazioni più installate

Qui puoi avere una panoramica delle app che sono state installate di più.

Colonne predefinite di questo report:

Nome	Nome della rispettiva applicazione e/o servizio
Identificatore	ID app/servizio definito
Conteggio totale	Con quale frequenza questa applicazione/servizio è stata installata sui dispositivi dell'utente finale

Applicazioni obbligatorie

Qui trovi una panoramica delle app obbligatorie (richieste per legge).

Colonne predefinite di questo report:

Nome	Nome della rispettiva applicazione e/o servizio
Identificatore	ID app/servizio definito
Fonte dell'applicazione	Quale AppStore è coinvolto: • Google PlayStore (Android) • AppStore di iTunes (iOS)
OS	Sistema operativo

Applicazioni nella lista nera

Qui puoi avere una panoramica di tutte le app definite nella lista nera.

Colonne predefinite di questo report:

Nome	Nome della rispettiva applicazione e/o servizio
Identificatore	ID app/servizio definito
Fonte dell'applicazione	Quale AppStore è coinvolto: • Google PlayStore (Android) • AppStore di iTunes (iOS)
OS	Sistema operativo

Rapporti degli utenti

Tariffa

Qui puoi avere una panoramica delle tariffe telefoniche e delle schede SIM dei tuoi utenti.

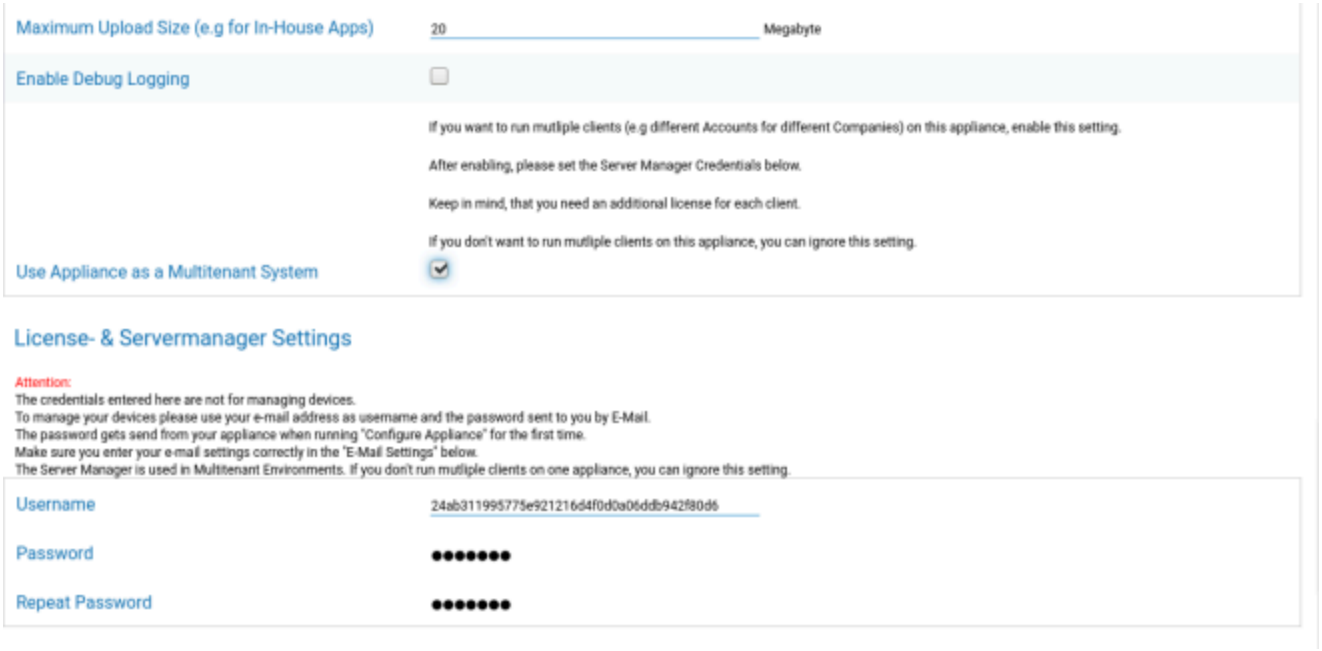
Colonne predefinite di questo report:

E-mail
Nome
numero di telefono
vettore
tariffa
opzione
prezzo
contrattoAnnullato
contrattoInizio
duringTime
mobileAndData
datiVolume
multiSIM
tipo
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Nota

Gestione dei multiaffittuari

AppTec360 EMM è in grado di ospitare più tenant separati, ognuno con i propri utenti e gruppi, autorizzazioni e impostazioni globali.

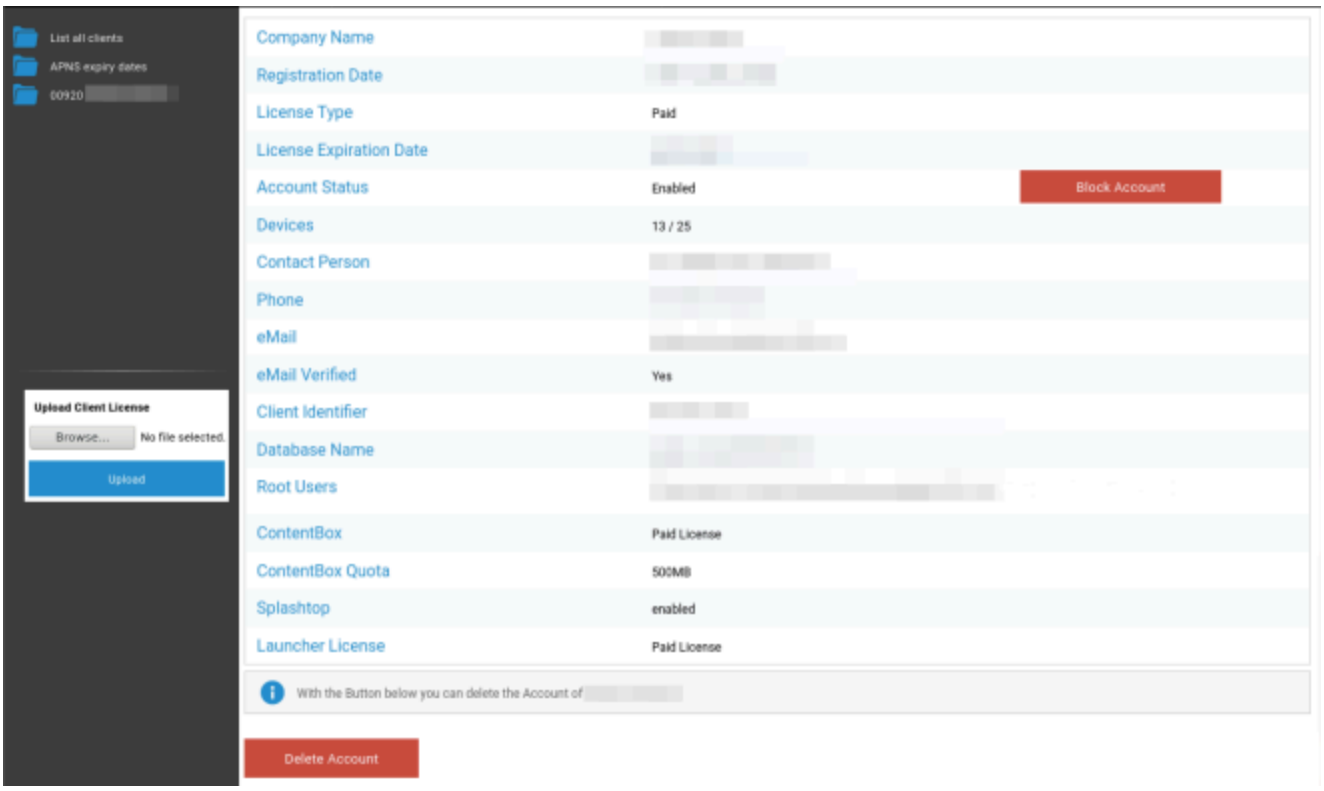
Per abilitare le funzionalità Multitenant, devi attivarle nell'interfaccia di configurazione della periferica al "Passo 3 - Impostazioni del server".



Nel nuovo menu imposta un nome utente e una password per il Servermanager. Salva le impostazioni ed esegui "Configura la periferica" in "Passo 5 - Contratto di licenza" per applicare le impostazioni.

Una volta terminata la configurazione, potrai effettuare il login con le credenziali impostate attraverso la normale interfaccia di Mobile Management.

Dopo l'accesso potrai vedere la seguente vista.



A sinistra puoi vedere tutti gli inquilini (in questo caso solo uno con id 920) e a destra le informazioni su questo cliente. Hai anche la possibilità di bloccare l'accesso all'account e di eliminare il cliente (ATTENZIONE: questo rimuoverà tutti i dati relativi a quel cliente).

A sinistra puoi caricare una nuova licenza per il cliente, che può essere un aggiornamento della licenza per un cliente esistente o una nuova licenza che crea automaticamente un nuovo cliente. Quando viene creato un nuovo cliente, un'e-mail contenente la password di accesso viene inviata automaticamente all'indirizzo e-mail per il quale è stata rilasciata la licenza.

Per ottenere una licenza client nuova o aggiornata (ad esempio, se hai bisogno di più licenze per i dispositivi) contatta il tuo rappresentante di vendita.

Ulteriori punti di vista

Elenco di tutti i clienti

Mostra una panoramica di tutti i clienti del sistema.

ID cliente	ID cliente
Identificatore	Identificatore del cliente
Database	Database
Nome dell'azienda	Nome della società
eMail	Contatto eMail
Verificato	Se l'e-mail della persona di contatto è verificata o meno
Paese	Paese
Dispositivi	Numero di dispositivi registrati
Data di registrazione	Momento dell'assegnazione della licenza
Ultimo accesso	Ultimo accesso all'account amministratore
Licenza	Visualizzazione del tipo di licenza (Free|Paid)
Licenza CB	Tipo di licenza di ContentBox (Free|Paid)
Stato	Stato attuale di AppTec-Client
Scaduto	Visualizza, se la licenza è scaduta
iOS	Numero di dispositivi iOS
Android	Numero di dispositivi Android
Windows Mobile	Numero di dispositivi Windows Mobile
MacOS	Numero di dispositivi MacOS
Windows 10	Numero di dispositivi Windows 10
Android Enterprise	Numero di dispositivi aziendali Android
IOS BYOD (iscrizione dell'utente)	Numero di dispositivi IOS BYOD (iscrizione dell'utente)
IoT	Numero di dispositivi IoT

Date di scadenza APNS

Mostra una panoramica delle date di scadenza dei certificati APNS di tutti i client.

ID cliente	ID cliente
Nome dell'azienda	Nome dell'azienda
Data di scadenza	Data di scadenza del certificato Apple APNS
Info	Informazioni sulla scadenza

Contatto

Altre domande? Basta contattarci al seguente indirizzo:

Per domande tecniche generali

support@apptec360.com

+41 61 511 3210

Per domande relative all’installazione di un dispositivo virtuale

consulting@apptec360.com

+41 61 511 3214

Esclusione di responsabilità

© AppTec GmbH

Questa documentazione è protetta da copyright. Tutti i diritti restano di AppTec GmbH. È vietato qualsiasi altro utilizzo, in particolare il trasferimento a terzi, la memorizzazione all'interno del sistema di dati, la distribuzione, la modifica, l'esecuzione, la visualizzazione e la trasmissione. Questo non vale solo per l'intero documento, ma anche per alcune parti. Le modifiche possono essere apportate in qualsiasi momento.

Altri nomi di aziende, marchi e prodotti sono marchi di fabbrica o marchi registrati e che non sono stati nominati esplicitamente in questo punto, sono protetti dalle leggi sui marchi di fabbrica e appartengono al rispettivo proprietario. Modifiche e correzioni possono essere apportate in qualsiasi momento.