Ghid de utilizare pentru administratori

Vodafone Secure Device Manager

Ghidul tău pas cu pas pentru a lucra cu

Vodafone Secure Device Manager v5.17

power to you

Vodafone Secure Device Manager

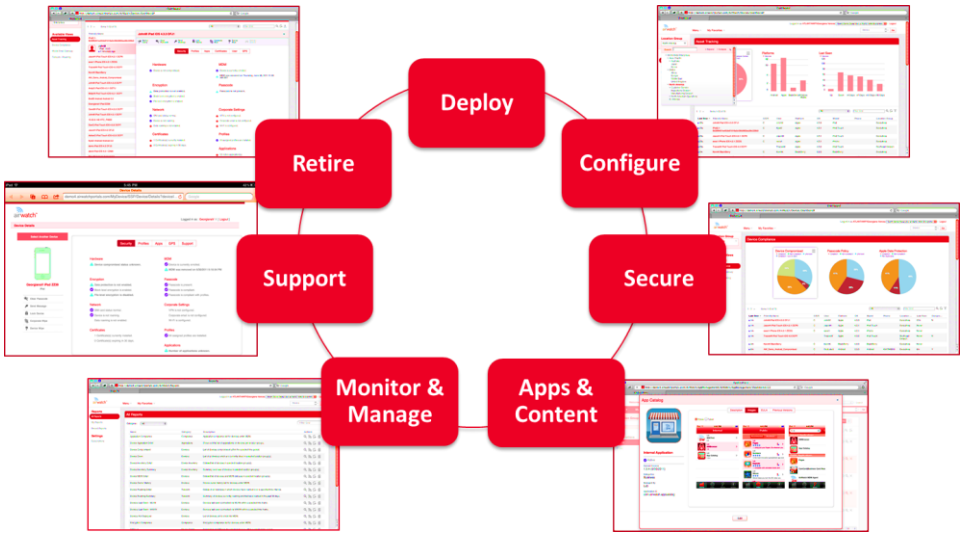
Cuprins

Vodafone Secure Device Manager

1.0 Privire generală asupra sistemelor

Privire generală asupra soluției Vodafone

Vodafone oferă **o gestionare completă a mobilității** permițând organizațiilor să controleze şi să asigure o tehnologie de ultimă oră a dispozitivelor mobile, prin furnizarea unei soluții cuprinzătoare pentru mai multe platforme în vederea gestionării acestor dispozitive.



Vodafone Secure Device Manager **(VSDM)** oferă o locație centrală pentru ca administratorii să gestioneze grupuri de dispozitive smart, indiferent de sistemul de operare, transmițător, rețea sau locație.

Din VSDM, administratorii pot gestiona cele mai multe dispozitive smart phone de oriunde în lume.

Cerințe de sistem

Următoarele cerințe de sistem ar trebui să fie îndeplinite înainte de a utiliza soluția Vodafone Secure Device Manager.

1.1.1 Browsere acceptate

Vodafone este certificat să lucreze cu următoarele browsere web:

- Internet Explorer 8+
- Firefox 3.x+
- Google Chrome 11+
- Safari 5.x

Testarea cuprinzătoare a platformei a fost efectuată pentru a asigura funcționalitatea în timpul utilizarării acestor browsere Web. VSDM poate funcționa totuşi şi cu browsere necertificate.

1.1.2 Dispozitive acceptate

VSDM acceptă în prezent următoarele dispozitive:

- Versiunea Android 2.2 şi cele superioare
- Versiunea Blackberry 5 şi cele superioare
- Versiunea iOS 4.0 şi cele superioare
- Symbian OS ^3 şi S60 (9.3 FP2)
- Windows Mobile 5/6 şi Windows CE 4/5
- Windows Phone 7 şi 7.5 Mango

Notă: Un suport limitat ar putea fi disponibil pentru alte dispozitive / sisteme de operare. Contactați Asistența Vodafone pentru mai multe informații.

1.1.3 Cerințe tehnice

Cerințele tehnice variază în funcție de utilizarea SaaS Vodafone sau soluții la locul la locul de muncă. Pentru mai multe detalii privind cerințele tehnice, te rugăm să consulți documentele Cerințele Vodafone pentru instalare şi implementare.

Privire generală asupra consolei VSDM Admin

1.1.4 Conectarea la Consola VSDM Admin

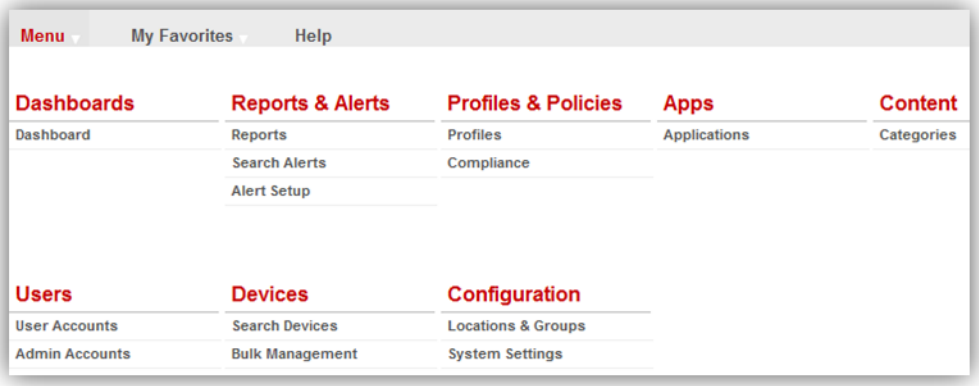
Vodafone oferă administratorilor un URL, nume de utilizator şi o parolă pentru VSDM Admin. Dacă nu ai aceste informații, te rugăm să contactezi Vodafone asistență. Odată ce ai informațiile corespunzătoare, conectează-te la VSDM:

- Navighează pe adresa furnizată **URL**.
- Introdu **Numele de utilizator** şi **Parola**.

1.1.5 Navigarea

Gestionarea dispozitivului smart cu Vodafone este centralizată în VSDM. Aici, administratorii au capacitatea de a gestiona, monitoriza si a asigura că dispozitivele lor prin orice browser, oriunde în lume, fără a trebui să descarce sau să instaleze vreun software suplimentar.

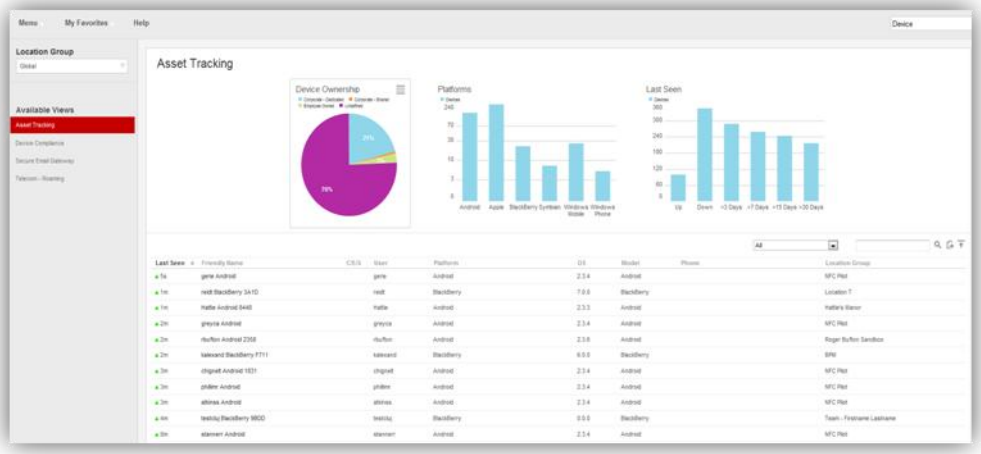
Paginile Consolei VSDM Admin sunt clasificate în funcție de scopul specific de gestionare al dispozitivului. Paginile pot fi găsite în meniul derulant din colțul din stânga sus a Consolei VSDM Admin.



Din acest meniu (arătat mai sus), administratorii pot naviga cu rapiditate la toate paginile cheie descrise mai jos.

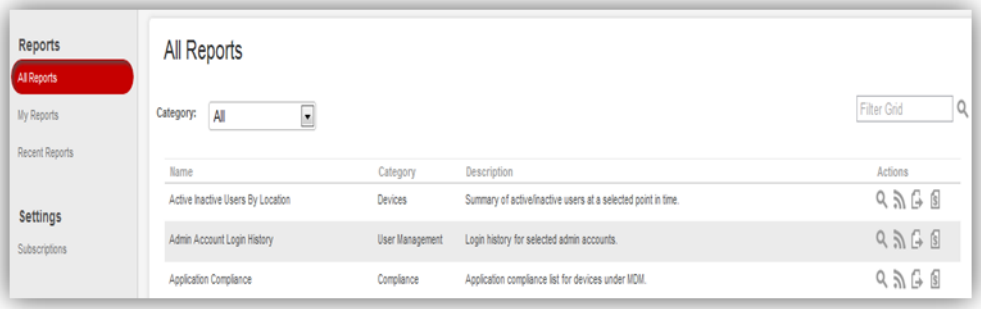
1.1.6 Bordul

Pagina cu **Bordul** este utilizat pentru a gestiona şi monitoriza dispozitivele de la grupurile de nivel înalt la dispozitivele individuale.



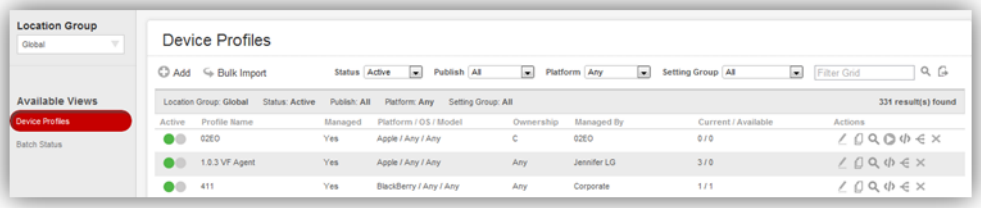
1.1.7 Rapoarte şi Alerte

Pagina de raportare permite administratorilor să genereze rapoarte personalizate cu privire la starea grupului de dispozitive, să configureze abonamente automate de raportare şi să păstreze rapoartele comune pentru utilizarea în viitor. Administratorii pot crea, de asemenea, politici de alertă unice pentru o notificare imediată atunci când un dispozitiv este compromis sau intră într-o condiție nefavorabilă.



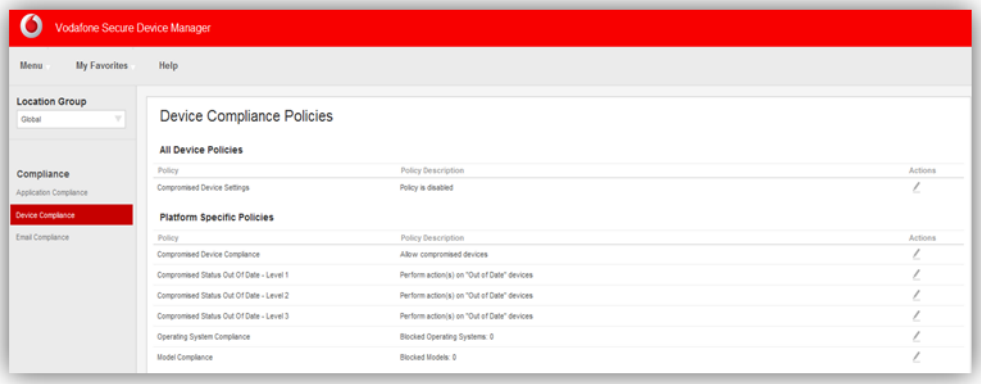
1.1.8 Profile şi Politici - Profile

Pagina de profile permite administratorilor să creeze, să editeze şi să elimine toate profilurile corporative care sunt trimise over-the-air în grupul de dispozitive smart. Aceste profiluri permit dispozitivelor să recepționeze în mod automat date corporative cum ar fi conexiuni Wi-Fi, codul de acces şi politicile de restricții, e-mailuri corporative şi calendare, catalogul Vodafone App precum şi alte date personalizate.



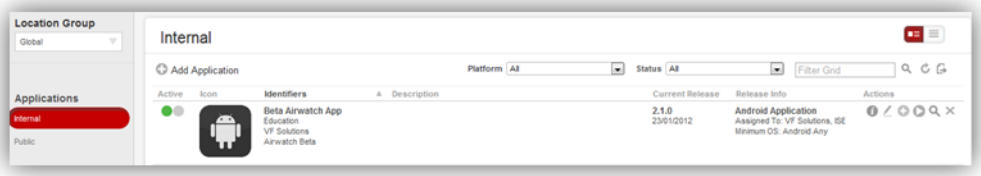
1.1.9 Profiluri şi Politici - Conformitate

Pagina de conformitate este pagina în care administratorii pot desemna politici de securitate detaliate pentru dispozitivele lor, astfel încât acțiunile specifice să poată avea loc atunci când dispozitivele nu respectă normele de conformitate. Există trei tipuri de reguli de reguli de conformitate care pot fi selectate: Aplicația, dispozitivul şi emailul.



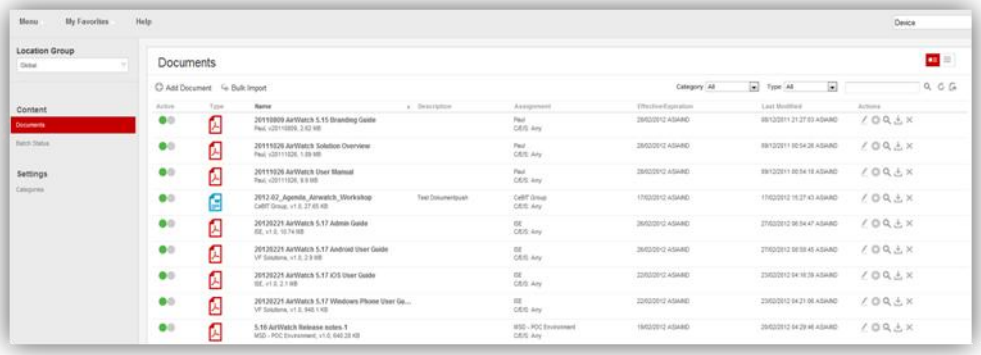
1.1.10 Aplicații

Pagina de aplicații oferă o interfață centralizată pentru ca administratorii să recomande aplicațiile publice şi să implementeze aplicații interne pentru grupul de dispozitive smart.



1.1.11 Vodafone Secure Content Locker

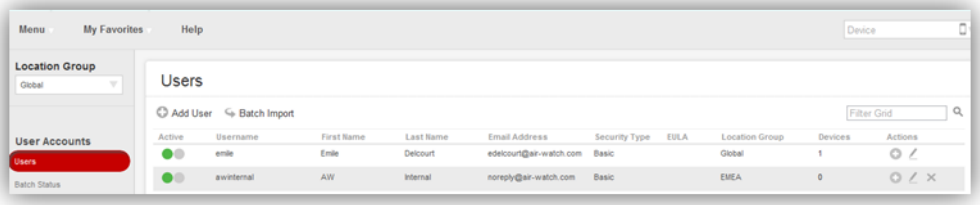
Paginile de gestionare a conținutului permit administratorilor să încarce şi să gestioneze conținutul pentru implementarea sigură a grupului de dispozitive smart.



1.1.12 Utilizatorii

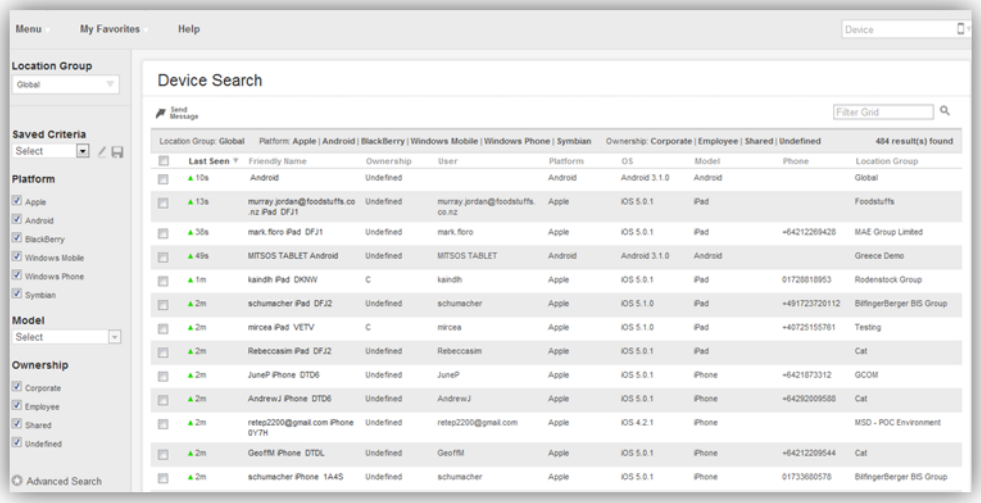
Paginile **Conturi de utilizatori** şi **Conturi administrative** furnizează instrumente pentru dezvoltarea grupului de dispozitive smart.

- Pagina **Conturi administrative** este utilizată pentru a adăuga, modifica sau şterge administratorii Vodafone care utilizează Consola VSDM Admin pentru a gestiona grupul de dispozitive.
- În cele din urmă, pagina **Conturile de utilizator** este utilizată pentru a adăuga, modifica sau şterge utilizatorii finali ai dispozitivelor gestionate.



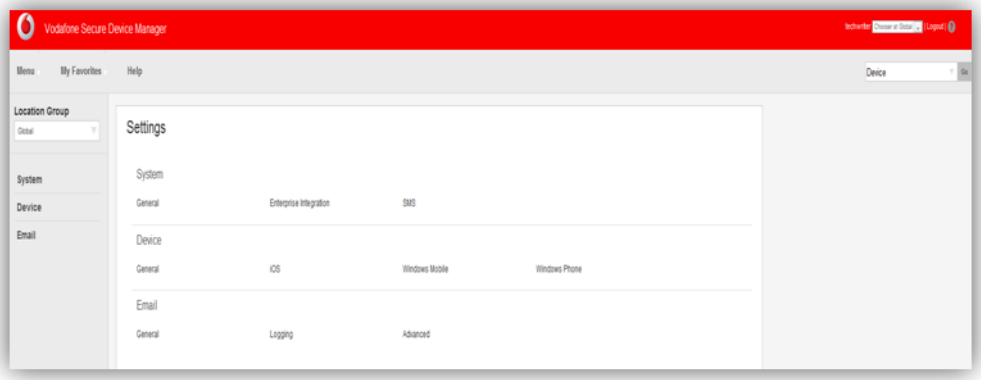
1.1.13 Dispozitivul

Paginile **Căutare dispozitiv** şi **Gestionare în grup** îţi permit să găseş ti rapid un dispozitiv sau să gestionezi grupuri de dispozitive în funcţie de nume, platformă, grup sau în funcţie de alte criterii.



1.1.14 Configurare

Paginile **Configurare** oferă o pagină **Locaţie şi grupuri** în care administratorul poate adăuga, şterge sau modifica structura de grupare a dispozitivelor, după cum este necesar. Pagina **Setări de sistem** oferă o locaţie centralizată pentru toate setările configurabile. Aici pot fi realizate configurările iniţiale şi personalizarea continuă pentru utilizatorii finali şi pentru VSDM.



2.0 Setarea mediului pentru Vodafone Secure Device Manager

Prezentare generală

Există câteva acțiuni administrative ce trebuie efectuate înainte ca utilizatorii finali să își înscrie dispozitivele în cadrul VSDM, pentru a oferi acces la Consola Admin VSDM tuturor administratorilor din grupul dispozitivelor smart.

- **Conturi de utilizatori** pentru a asocia utilizatorii corporativi cu dispozitivele lor gestionate.

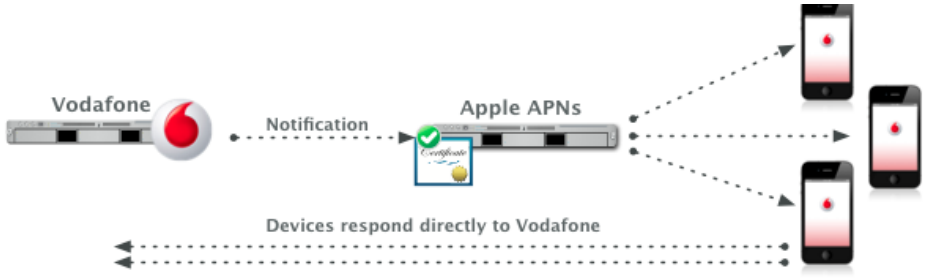
Activarea asistenței iOS VSDM

În scopul gestionării dispozitivelor iOS sub orice platformă Vodafone Secure Device Manager, compania ta trebuie să genereze mai întâi un certificat APN înainte de a începe.

- Serviciul de Notificare Automată de la Apple (APN) este folosit pentru a permite Vodafone sau oricărui furnizor al Vodafone Secure Manager să comunice în siguranță cu dispozitivele dvs. over-the-air. (OTA)
- Fiecare organizație are nevoie de propriul certificat APN pentru a asigura un mecanism sigur pentru ca dispozitivele lor să comunice în rețeaua Notificări Automate Apple.

Vodafone Secure Device Manager folosește certificatul APN pentru a trimite notificări către dispozitivele tale când Administratorul solicită informații sau în timpul unui program definit de monitorizare.

Notă: Numai notificările sunt trimise prin serverul APN.

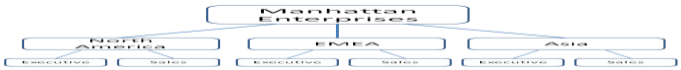


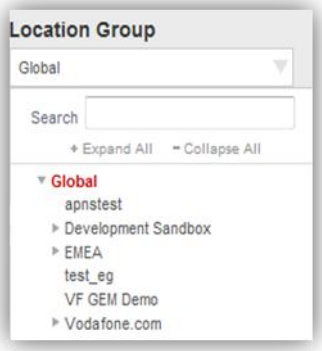
Pentru a afla mai multe despre modul în care compania ta poate genera şi încărca un certificat APN pentru administrarea dispozitivelor iOS mobile, te rugăm să contactezi organizația locală de sprijin a Vodafone.

Grupuri de locații

În cadrul companiilor mari, departamentele IT trebuie să îndeplinească cerințele utilizatorilor din diferite grupe funcționale, organizatorice sau geografice. Soluția Vodafone la această cerință referitoare la diverse scopuri, sunt **Grupurile de locații** şi **Locațiile**.

Administratorii pot crea structuri cu grupuri de locații care se aliniază cu structura ierarhică a companiei pentru a oferi soluții personalizabile şi scalabile VSDM pentru utilizatorii individuali şi companii.

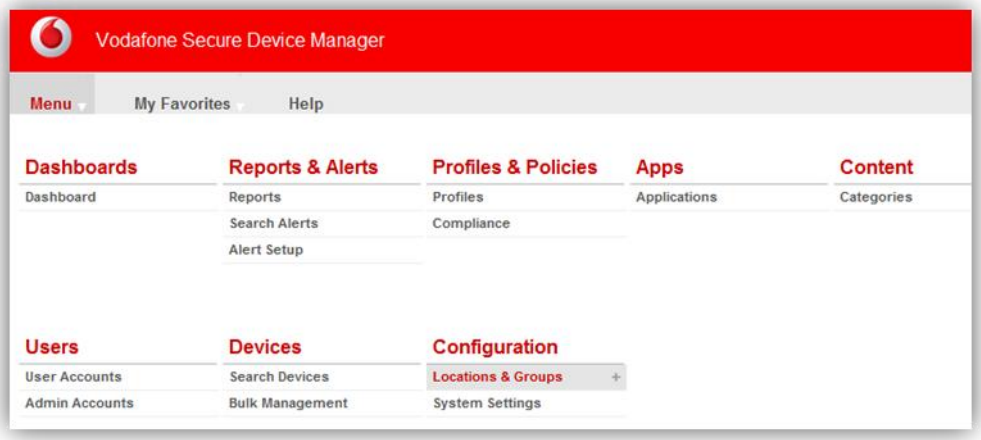




Prin urmare, odată cu evoluarea structurii corporative, vine şi nevoia de a crea grupuri şi locații suplimentare. Paşii de mai jos descriu procesul de creare a unui grup de locație şi o locație asociată:

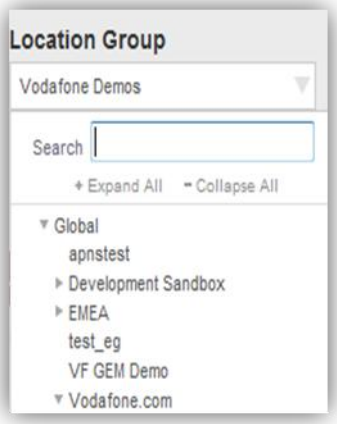
2.1.1 Crearea grupurilor de locații

▶ Navighează la **Configurare→Locații & Grupuri.**



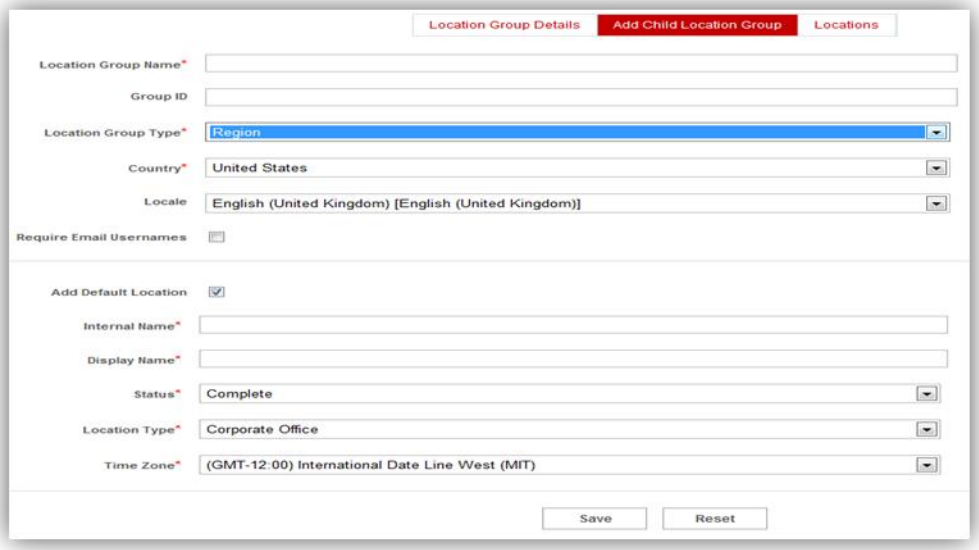
▶ Selectează un **Grup de locații părinte** din listă.

- Grupul locație părinte este grupul care este cu un nivel ierarhic mai sus de unul care este adăugat. Odată complet, noul grup este listat un nivel mai jos de grupul părinte.



- Selectează **Adăugare grup de locație copil** pentru a deschide formularul unui nou grup de locație.

- Completează informațiile necesare referitoare la grupul de locație.



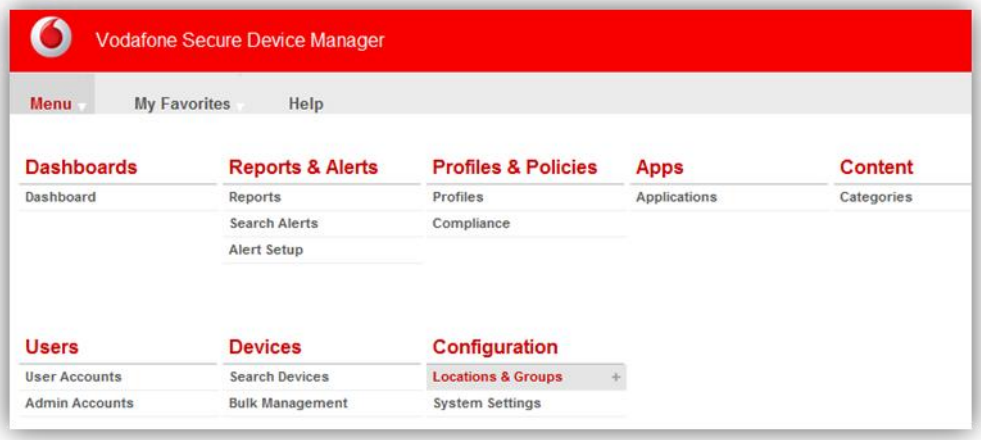
  - **Numele Grupului de Locație** – Numele afișat pentru grupul de locație care este afișat în Consola Admin VSDM.
  - **ID Grup** –Codul de activare folosit de dispozitiv pentru a se înscrie în acest grup de locație. Acesta dictează ce profiluri, aplicații şi politici sunt moştenite de dispozitiv bazat pe ceea ce este configurat la acest grup de locație. Administratorul trebuie să furnizeze utilizatorilor finali ID-ul grupului lor, în scopul de a finaliza procesul de înscriere.

- **Bifează** caseta **Adăugare locație implicită** şi completează informațiile cerute privind locația:
  - **Numele intern** –Numele unic care este folosit intern pentru a defini o locație.
  - **Numele de afișare** –Numele afișat pentru grupul de locație care este afișat în Consola Admin VSDM.
- Când ai terminat, da click pe **Salvare.** Noul grup de locație şi locația sunt acum create.

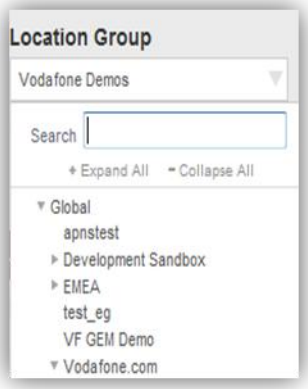
2.1.2 Modificarea şi ştergerea grupurilor de locaţie

Pagina **Detalii grup de locaţie** oferă abilitatea de a modifica şi şterge informaţiile privind grupul de locaţie, inclusiv ID-ul grupului.

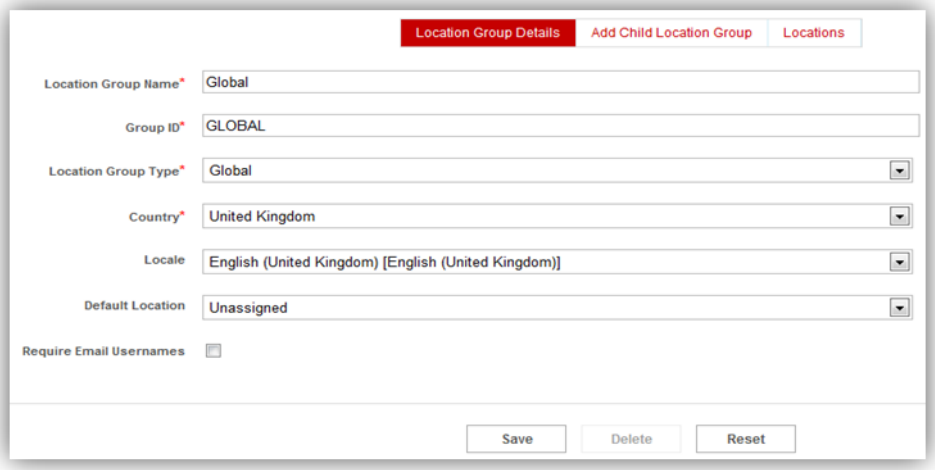
- Navighează la **Configurare→Locaţii & Grupuri.**



- Alege **Grupul de locaţie** pe care doreş ti să-l modifici sau ştergi.



- Asigură-te că ai selectat **Detalii grup locaţii** şi apoi modifica oricare din câmpurile listate mai jos.



- **Numele Grupului de Locaţie** – Numele afişat pentru grupul de locaţie care este afişat în Consola Admin VSDM.

- **ID Grup** – Codul de activare folosit de dispozitiv pentru a se înscrie în acest grup de locație. Acesta dictează ce profiluri, aplicații şi politici sunt moştenite de dispozitiv bazat pe ceea ce este configurat la acest grup de locație. Administratorul trebuie să furnizeze utilizatorilor finali ID-ul grupului lor, în scopul de a finaliza procesul de înscriere.
- **Tipul grupului de locație /țara/localitatea** – Folosit numai pentru clasificarea internă.
- **Locație implicită** – Locația implicită este locația ce se alocă dispozitivelor în mod automat atunci când sunt înscrise în grupul de locație.
  - ▶ Pentru a salva modificările, dă click pe **Salvare**.
  - ▶ Pentru a şterge grupul de locație, fă click pe **Ştergere.**

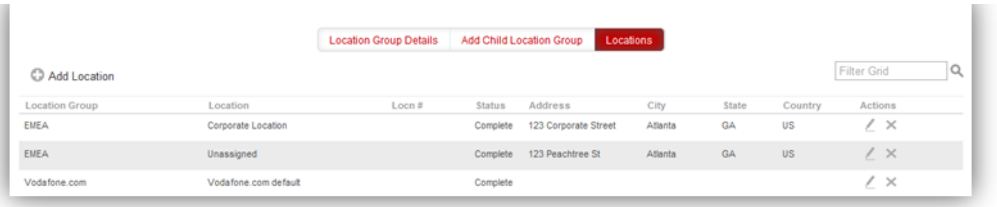
Notă: Pentru a şterge un grup de locație nu trebuie să existe niciun grup de locație copil sub el. Dacă există, şterge toate grupurile copil create de la cel de jos la cel de sus până vei putea şterge grupul original.

2.1.3 Detalii suplimentare privind grupurile de locație

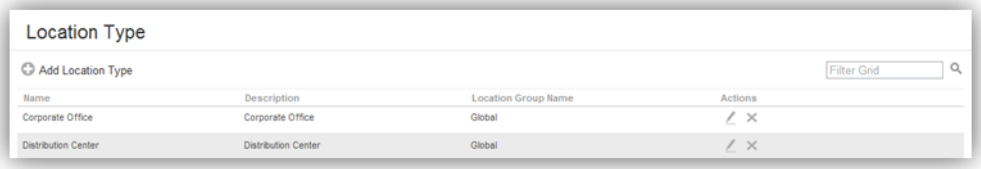
Administratorul poate stabili, de asemenea, mai multe câmpuri adiționale pentru a furniza informații suplimentare pentru grupurile de locație. Aceste domenii nu au niciun efect asupra funcționării grupurilor de locație dar pot fi folosite pentru a oferi informații suplimentare detaliate în scopul logării.

Locațiile reprezintă o unitate organizațională în care dispozitivele înscrise sunt plasate. În mod implicit, fiecare grup de locație are cel puțin o Locație, cunoscută **Locație implicită**.

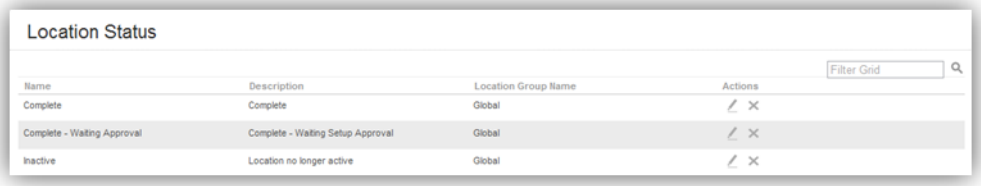
Notă: Fără o locație implicită nu pot fi înscrise dispozitiele în acel grup de locație specific.



Tipurile de locații oferă posibilitatea de a clasifica Locațiile pe baza structurii corporative (pentru uz intern în VSDM).



Statutul locației oferă posibilitatea de a clasifica statutul unei Locații. Acesta afişează dacă o Locație este activă sau va fi activă în viitor (pentru uz intern în VSDM).

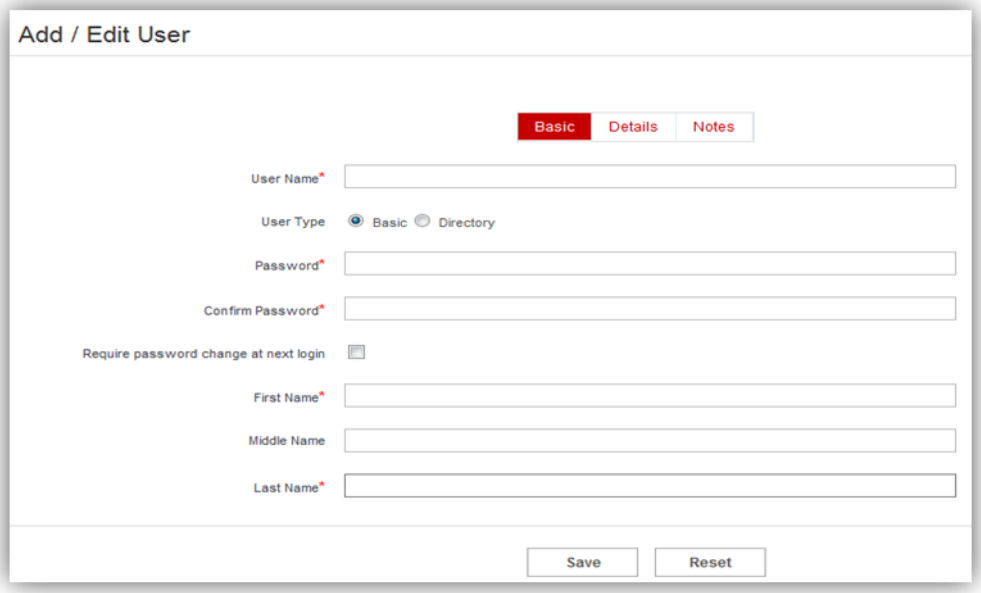


Conturi Admin

Gestionarea grupului de dispozitive smart de multe ori necesită ca mai mulți administratori să aibă acces la VSDM, şi ar putea fi necesar să adaugi sau să elimini conturi administrative. Consola de administrare VSDM oferă un mod simplu de a crea şi gestiona mai multe conturi administrative.

2.1.4 Crearea conturilor administrative

- Navighează la **Utilizatori →Conturi Administrative.**
- Selectează **Grup de locație** din colțul de sus stânga. Acesta este grupul locației implicite pentru acest cont de administrator.
    - Selectează cel mai înalt nivel de acces de care ar putea avea nevoie de administratorul. Odată conectați, ei pot avea acces la toate grupurile de locații care sunt enumerate mai jos cel selectat.
- Dă click pe Add User şi completează câmpurile cerute.

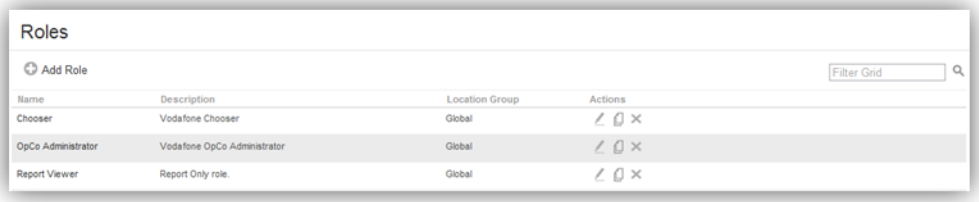


- Introdu **Numele utilizatorului** şi **Parola** pentru contul administrativ.
- Bifează caseta **Solicită schimbarea parolei la următoarea logare** pentru a determina administratorul să schimbe parola la următoarea lor logare.
- Completează câmpurile **Informații de bază** suplimentare:
    - **Prenume Nume & E-mail** – Numele şi adresa de e-mail a administratorului.
    - **Rolul primar** –Rolul primar determină nivelul de acces pe care noul administrator il are. De exemplu, dacă administratorul este un operator helpdesk, atunci rolul **Helpdesk** cu acces limitat poate fi cel mai potrivit. Rolurile sunt configurate separat de conturile administrative.
    - **Pagina de destinație implicită** –Prima pagină pe care un administrator o vede după autentificarea în Consola VSDM Admin. Pentru a modifica acest câmp, şterge conținutul şi începe să introduci numele oricărei pagini a Consolei VSDM Admin.
- Completează orice **Detalii** sau **Note** care doreş ti să fie vizibile în Consola VSDM Admin.
- Când ai terminat, dă click pe **Salvare.** Noul cont administrativ este acum creat.

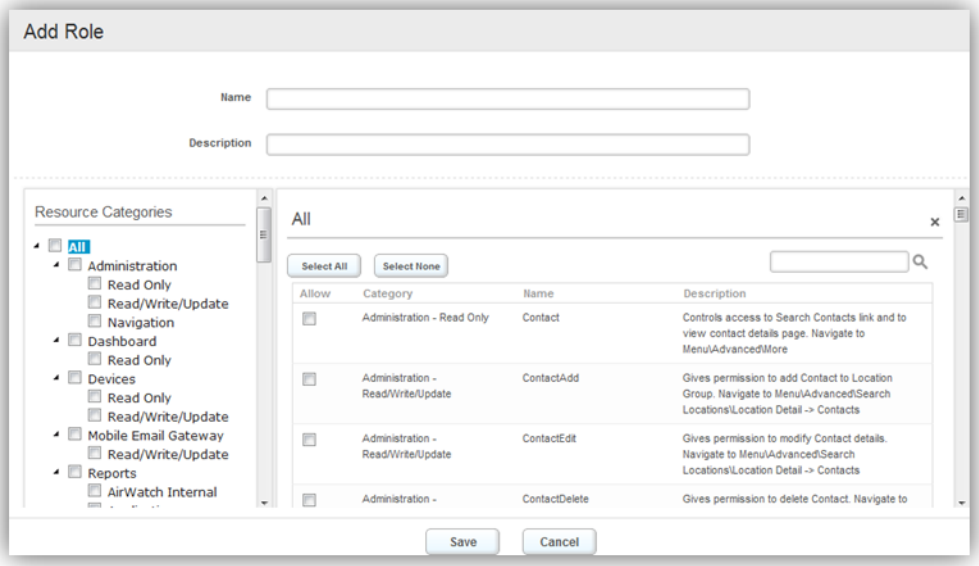
2.1.5 Crearea rolurilor pentru conturile de administratori

Rolurile administratorilor permit companiei tale să controleze securitatea şi permisiunile acordate de Vodafone Secure Manager administratorilor prin limitarea accesului la componente ale VSDM. Poți controla direct accesul administratorului prin crearea unui rol nou sau editarea unui rol existent. Pentru a crea sau edita roluri ale administratorilor:

- Navighează la **Utilizatori →Conturi Administrative.**
- Selectează **Roluri** din colțul de jos stânga pentru a edita un rol existent sau a crea unul nou.



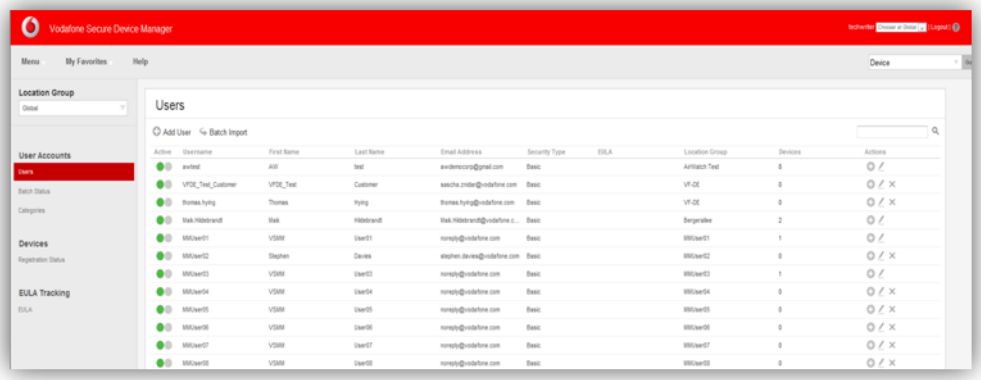
- Dă click pe **Adăugare rol** şi completează formularul.



- **Nume/Descriere** – Alege un nume descriptiv pentru ca rolul să fie uşor atribuit unui utilizator.
- Pe panoul din stânga poți selecta **Categorii resurse** pentru a defini nivelele de acces pentru diferite componente ale VSDM.
- Poți, de asemenea, să dai click pe numele Categoriei de resurse pentru a vizualiza o **listă de resurse** disponibile pentru fiecare categorie din dreapta.
- Pentru a localiza rapid resursele de un anumit tip, utilizează **bara de căutare** din colțul de sus dreapta.
- Când ai terminat, dă click pe **Salvare.** Noul rol este acum disponibil pentru atribuire de către administratori.

Conturile de utilizator

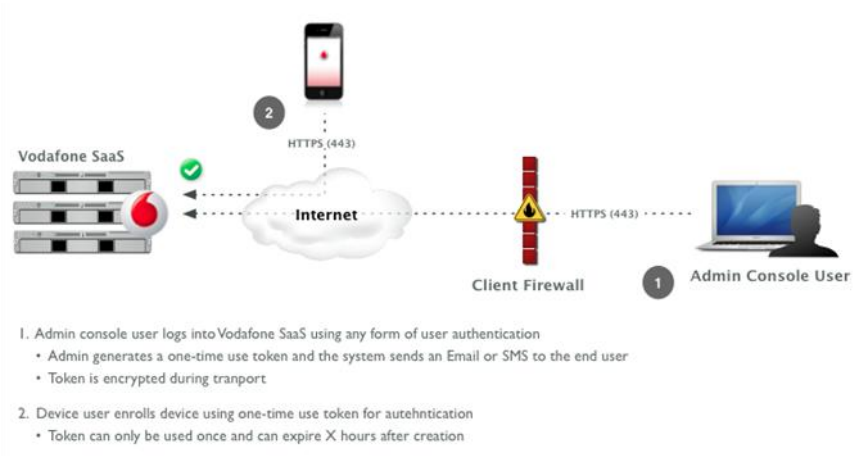
Conturile de utilizator sunt utilizate de către utilizatorii finali pentru a asocia dispozitivele la utilizatorii respectivi ai companiei. Vodafone recomandă ca pentru fiecare utilizator final să fie creat un cont asociat de utilizator pentru o scalabilitate completă. Prin urmare, deoarece grupurile de dispozitive smart ale companiilor se extind, administratorii trebuie să creeze în mod regulat conturi de utilizator suplimentare. Administratorii pot configura şi gestiona rapid conturile de utilizatori direct în VSDM pe pagina **Conturi de utilizatori** .



2.1.6 Tipuri de conturi de utilizatori

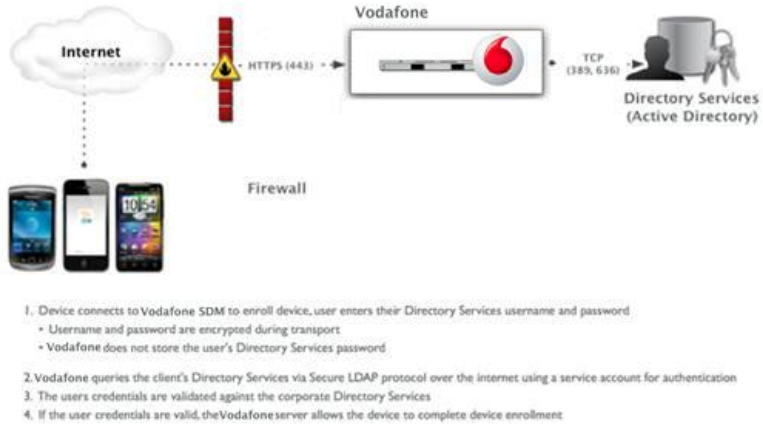
Conturile de utilizator pot fi configurate în diferite moduri, în funcție de cerințele companiei, modelul de implementare şi infrastructura companiei. Secțiunea următoare descrie configurații diferite iar în secțiunile de mai jos este detaliat modul de a crea conturi de utilizator de fiecare tip.

- **Autentificarea de bază** poate fi utilizată de orice arhitectură Vodafone Secure Device Manager dar nu oferă integrare în conturile de utilizatori existente.



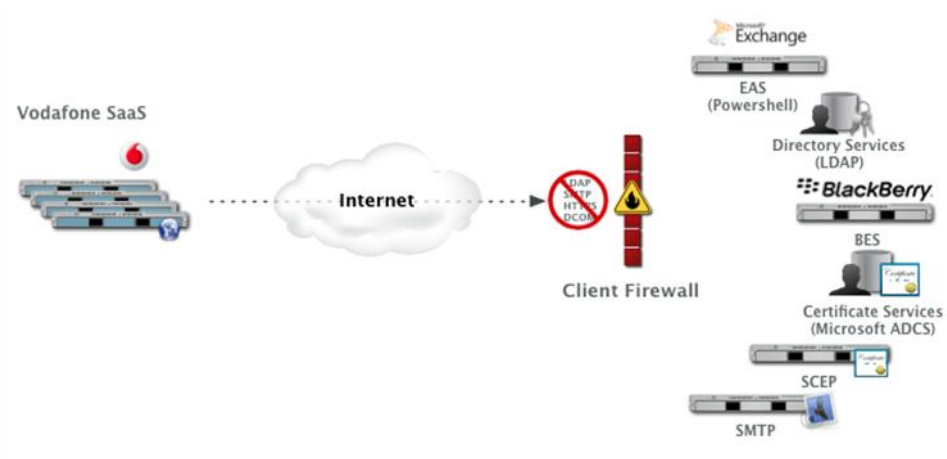
- **Puncte forte:** Poate fi utilizată pentru orice metodă de implementare, nu necesită integrare tehnică şi nici infrastructură de companie.
- **Puncte slabe:** Informațiile de acces există numai în Vodafone si nu se potrivesc neapărat informațiilor de acces corporative. Nu oferă securitate federală sau un singur sign-on. Vodafone stochează toate numele de utilizatori şi parolele.

- **Directorul activ / autentificarea LDAP** este utilizat pentru a integra conturile de utilizator şi de administrator ale VSDM în conturile corporative existente. Cu toate acestea, deoarece acest lucru necesită ca serverul VSDM să fie în contact direct cu un controlor de domeniu corporativ, acesta este recomandată pentru implementările on-premise.



- **Puncte forte:** Utilizatorii finali se pot autentifica cu informațiile corporative existente. Aceasta este o metodă sigură de integrare cu LDAP / AD pentru implementările on-premise şi este o practică standard de integrare.
- **Puncte slabe:** Necesită un AD sau alt server LDAP. Acesta este folosit folosit numai pentru implementările on-premise.

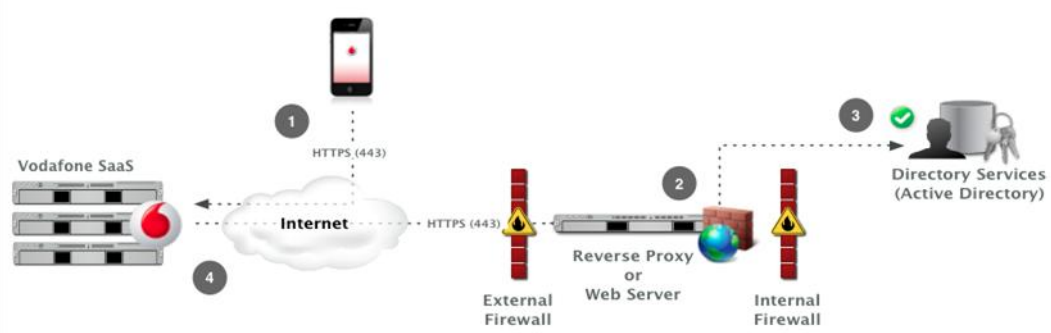
  ▶ **Directorul activ / autentificarea LDAP cu Serviciul de Integrare Vodafone Enterprise** oferă aceeaşi funcționalitate ca autentificarea AD / LDAP tradițională dar permite ca acest model să funcționeze across the cloud pentru implementări SaaS. Serviciul de Integrare Exterprise oferă, de asemenea, o serie de capabilități de integrare aşa cum se arată mai jos.



- **Puncte forte:** Utilizatorii se autentifică prin informațiile corporative existente. Necesită doar un singur port de firewall-ul deschis între serverul EIS şi Vodafone SaaS (port 443). Transmisia informațiilor de acces este criptată şi sigură. Oferă, de asemenea, configurare sigură pentru alte infrastructuri cum ar fi BES, Microsoft ADCS, SCEP şi servere SMTP.
- **Puncte slabe:** Necesită ca Serviciul de integrare Enterprise să fie instalat în spatele firewall-ului sau într-un DMZ. Este necesară o configurare suplimentară.

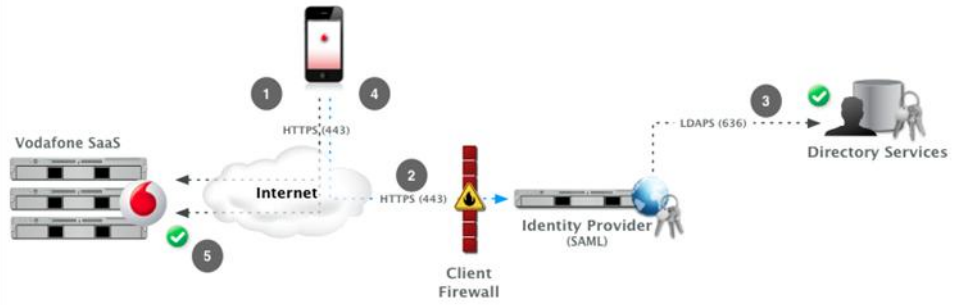
  Notă: Disponibilitatea EIS poate varia în funcție de piețele locale.

  ▶ **Proxy de autentificare** este o soluție de proprietate ce furnizează integrarea serviciului across the cloud sau în rețele interne dure. În acest model, serverul Vodafone Secure Device Manager comunică cu un server Web public sau un server de schimb ActiveSync care este capabil să autentifice utilizatorii conform controlorului de domeniu. Această metodă poate fi utilizată numai atunci când organizațiile au un server cu web public, cu legături în controlatorul de domeniu corporativ.



1. Device connects to Vodafone SDM to enroll device, user enters their Directory Services username and password
   - Username and password are encrypted during transport
   - Vodafone does not store the user's Directory Services password
2. Vodafone relays the username and password to a configured Authentication Proxy endpoint that requires authentication (e.g. Basic Authentication)
3. The users credentials are validated against the corporate Directory Services
4. If the user credentials are valid, the Vodafone server allows the device to complete device enrollment

- **Puncte forte:** Oferă o metodă sigură de inrtegrare cu AD/LDAP across the cloud. Utilizatorii finali se pot autentifica cu informațiile corporative existente. Acesta este un modul uşor care necesită configurare minimă.
- **Puncte slabe:** Necesită un server cu web public sau un server de schimb ActiveSync cu legături într-un server AD / LDAP. Fezabil numai pentru machete de arhitectura specifice. Este o soluție mult mai robustă decât EIS.
  - **Autentificarea SAML 2.0** este o soluție nouă care oferă asistență la conectarea unică şi autentificarea federală, Vodafone nu primeşte nicio informație corporativă. Dacă o organizație are un server Furnizor de identitate SAML, integrarea SAML 2.0 este recomandată.



1. Device connects to Vodafone to enroll device, Vodafone server redirects the device to the client specified identity provider
2. Device securely connects via HTTPS to client provided identity provider and user enters credentials
   - Credentials are encrypted during transport directly between the device and SAML endpoint
3. Credentials are validated against Directory Services
4. The identity provider returns a signed SAML response with the authenticated username
5. The device responds back to the Vodafone server and presents the signed SAML message; the user is authenticated

- **Puncte forte:** Oferă capacități de logare unică, autentificare cu informațiile existente ale companiei, iar Vodafone nu primeşte niciodată informații corporative în text simplu.
- **Puncte slabe:** Necesită o infrastructură SAML de Furnizare Identitate.

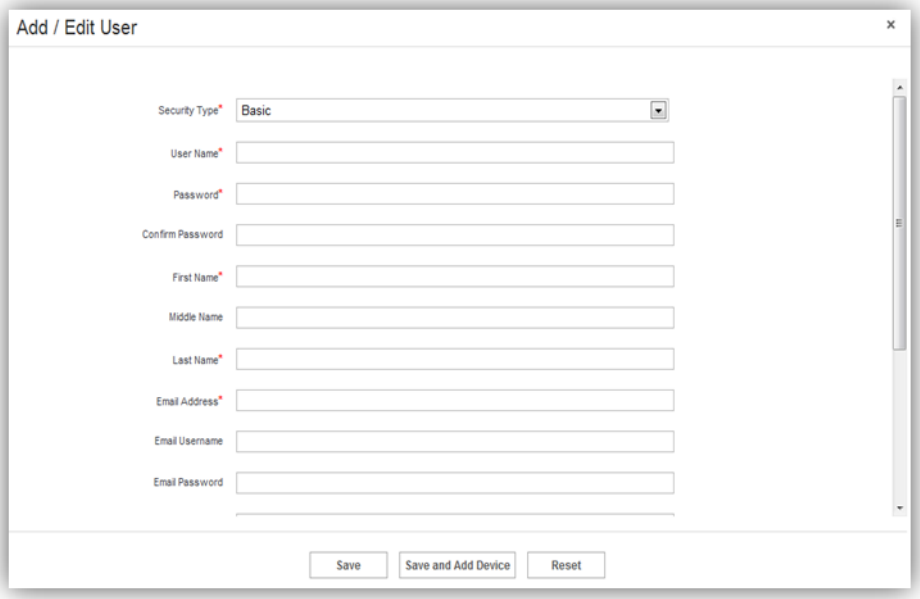
2.1.7 Crearea utilizatorilor finali de bază

1. Navighează la Utilizatori →Conturi utilizatori.
2. Selectează un Grup de locație din colțul de sus stânga.

- Selectează grupul de locație de la nivelul cel mai înalt în care utilizatorul trebuie să se înscrie. Ei se pot înscrie în toate grupurile de locație listate mai jos de acest grup dacă utilizatorul introduce ID-ul grupului (ID-ul grupului este configurat în **Configurare** -→**Locații & Grupuri** →**Detalii Grup de locație**) în timpul procesului de înscriere.

  ▶ Selectează Add User.

  ▶ Completează câmpurile necesare şi opționale din **Adăugare/Editare Formular de utilizator.**



- **Tipul securității** – Tipul de autentificare ce va fi utilizat pentru acest utilizator particular.

  ▶ **De bază** – Opțiunea de autentificare implicită care foloseşte un nume de utilizator de bază şi o combinație de parole aşa cum este determinat de acest formular.

  ▶ **Proxy de autentificare** – Autentificare cu informațiile pe bază de director, prin validarea înr-un server proxy în loc de un controler de domeniu corporativ. Aceasta este soluția recomandată pentru autentificarea pe bază de director across the cloud pentru clienții SaaS.

  ▶ **Director** –Autentificarea cu informațiile de acces LDAP sau AD corporative prin validarea într-un controler de domeniu corporativ.

  ▶ **SAML** –Autentificarea prin folosirea informațiilor de acces de tip Security Assertion Markup Language (SAML).

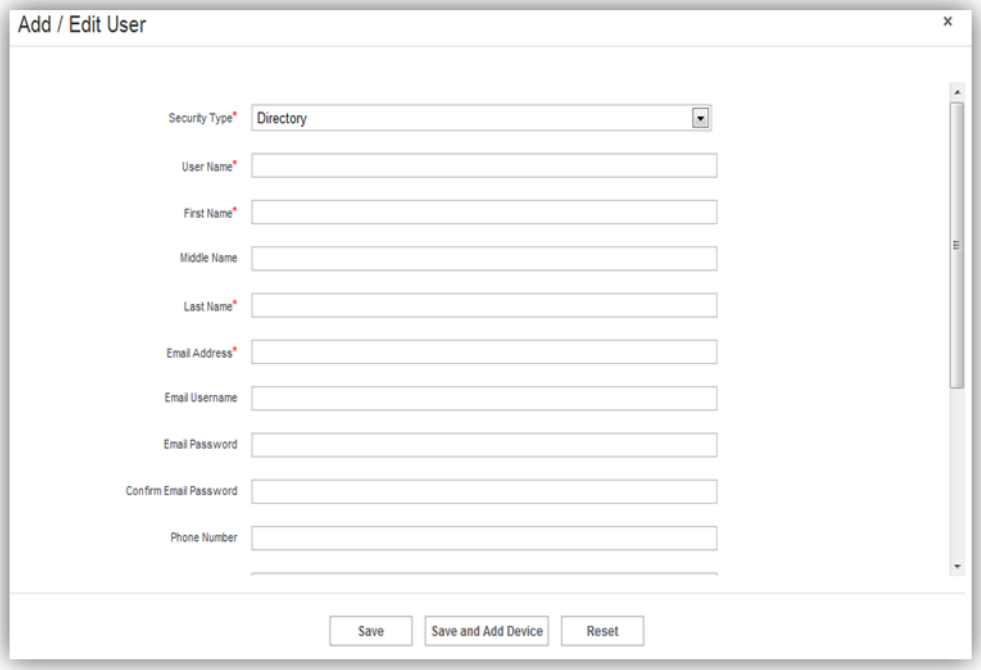
- **Nume de utilizator & Parolă** - Informațiile de acces de tip nume de utilizator şi parola pe care utilizatorul le introduce în timpul procesului de înscriere a dispozitivelor lor corporative. Administratorul trebuie să furnizeze utilizatorilor finali aceste informații.
- Selectează **Activare etapizare dispozitiv** - Un utilizator care a activat etapizarea dispozitivului poate organiza înscrierea pentru alți utilizatori astfel încât John Doe să se înscrie el însuşi, şi apoi personal să înscrie dispozitivele lui Jane Doe şi ale lui John Smith.
- Selectează **Tipul de mesaj** pentru ca utilizatorul să primească notificarea că acum îşi poate înscrie dispozitivele lor în Vodafone Secure Device Manager. De obicei, acum administratorii oferă utilizatorilor finali informațiile de acces (acreditările) necesare pentru înscriere (URL-ul de Înscriere, ID-ul grupului, numele de utilizator şi parola).
- Dă click pe **Salvare** pentru a finaliza contul de utilizator sau **Salvare şi Adăugare dispozitiv** pentru a finaliza contul de utilizator şi a intra în detaliile de bază pentru dispozitivul utilizatorului (înregistrare dispozitiv).

2.1.8 Crearea utilizatorilor finali prin LDAP / Directorul activ

Pentru a crea utilizatorii finali prin intermediul LDAP / Directorul Activ, Vodafone Secure Device Manager trebuie să fie configurat şi integrat în serverul LDAP / AD. Pentru a face acest lucru, te rugăm să consulți Contul de utilizator & Autentificarea dispozitivului.

După ce autentificarea directorului a fost configurată, administratorii pot crea conturi de utilizatori pe bază de Directoare.

- Navighează la **Utilizatori→Conturi de utilizatori**.
- Selectează Add User pentru a deschide Formularul de Adăugare utilizator.
- Selectează **Director** ca tip de securitate.



- Introdu detaliile de bază:

- Asteriscurile roşii denotă un câmp obligatoriu.
- Completează câmpul **Domeniu** dacă utilizatorul face parte dintr-un alt domeniu decât domeniul implicit, sau în cazul în care niciun domeniu implicit nu a fost specificat.
- Completează **Numele principal al utilizatorului** dacă Setarea de căutare a utilizatorului descrisă în Configurarea de autentificare pe bază de director nu rezolvă acest cont de utilizator.
- În mod implicit, aceste două domenii nu trebuie să fie configurate decât în circumstanțe speciale.

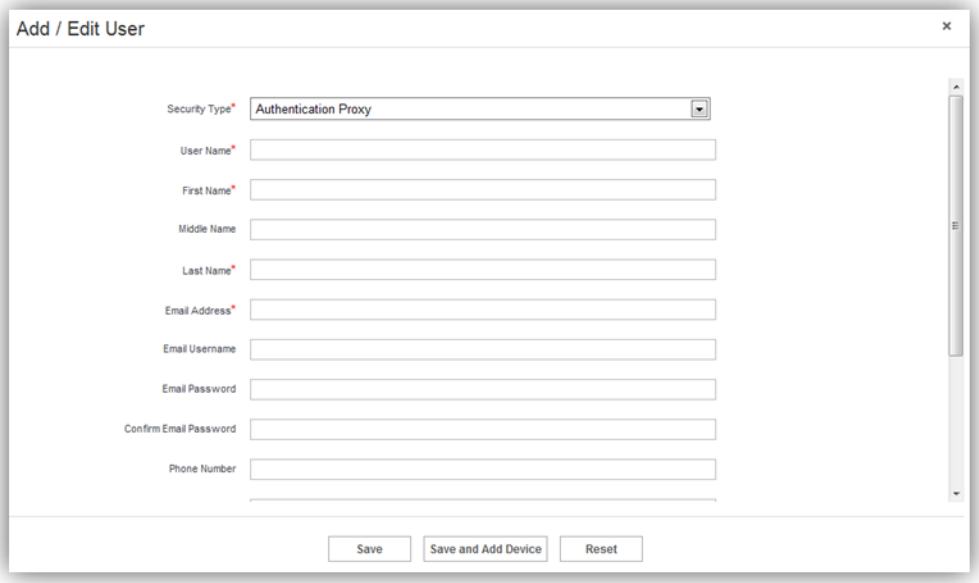
- Selectează **Salvare** pentru a completa procesul.

2.1.9 Crearea utilizatorilor finali prin Proxy de autentificare

Pentru a crea utilizatorii finali prin proxy de autentificare, Vodafone Secure device Manager trebuie să fie configurat şi integrat în serverul de web public sau în serverul EAS. Pentru a face acest lucru, te rugăm să consulți Contul de utilizator & Autentificarea dispozitivului.

După ce autentificarea proxy a fost configurată, administratorii pot crea conturi de utilizatori pe bază de proxy.

- Navighează la **Utilizatori→Conturi de utilizatori**.
- Selectează Add User pentru a deschide formularul **Adăugare utilizatori** .
- Selectează **Proxy de autentificare** ca tip de securitate.



- Introdu detaliile de bază:

- Asteriscurile roşii denotă un câmp obligatoriu. Completează câmpul **Domeniu** dacă utilizatorul face parte dintr-un alt domeniu decât domeniul implicit, sau în cazul în care niciun domeniu implicit nu a fost specificat.

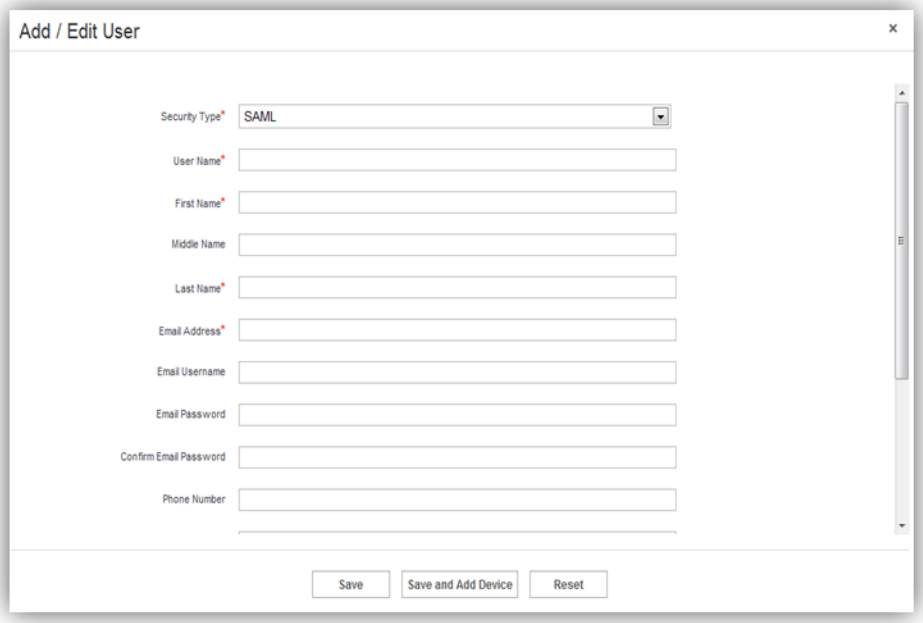
- Selectează **Salvare** pentru a finaliza procesul.

2.1.10 Crearea utilizatorilor finali prin SAML

Pentru a crea utilizatori finali prin intermediul SAML2.0, Vodafone Secure Device Manager trebuie să fie configurat şi integrat în serverul SAML de Furnizare Identitate. Pentru a face acest lucru, te rugăm să consulți Contul de utilizator & Autentificarea dispozitivului.

După ce autentificarea SAML a fost configurată, administratorii pot crea conturi de utilizatori securizate pe bază de SAML.

- Navighează la **Utilizatori→Conturi de utilizatori**.
- Selectează Add User pentru a deschide formularul **Adăugare utilizatori** .
- Selectează **SAML** ca tip de securitate.



- Introdu detaliile de bază:

- Asteriscurile roşii denotă un câmp obligatoriu.
- Completează câmpul **Domeniu** dacă utilizatorul face parte dintr-un alt domeniu decât domeniul implicit, sau în cazul în care niciun domeniu implicit nu a fost specificat.
- În mod implicit, aceste domenii nu trebuie să fie configurate decât în circumstanțe speciale.

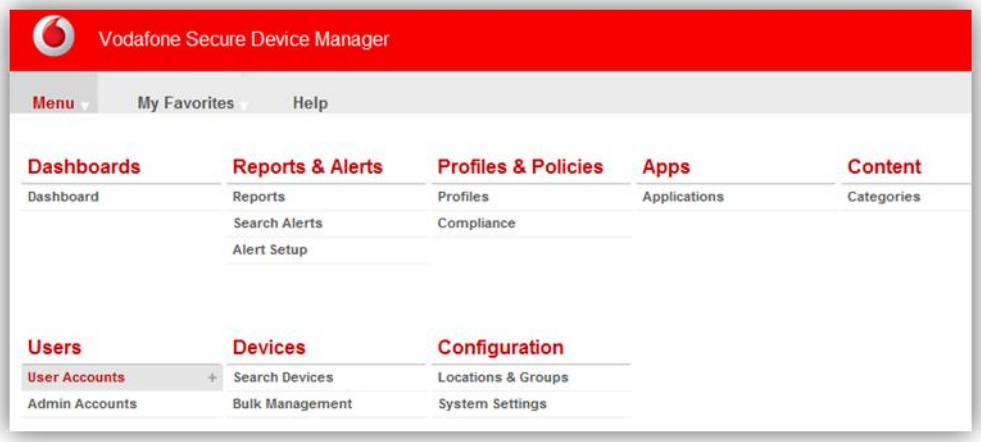
- Selectează **Salvare** pentru a finaliza procesul.

2.1.11 Crearea utilizatorilor finali în grup

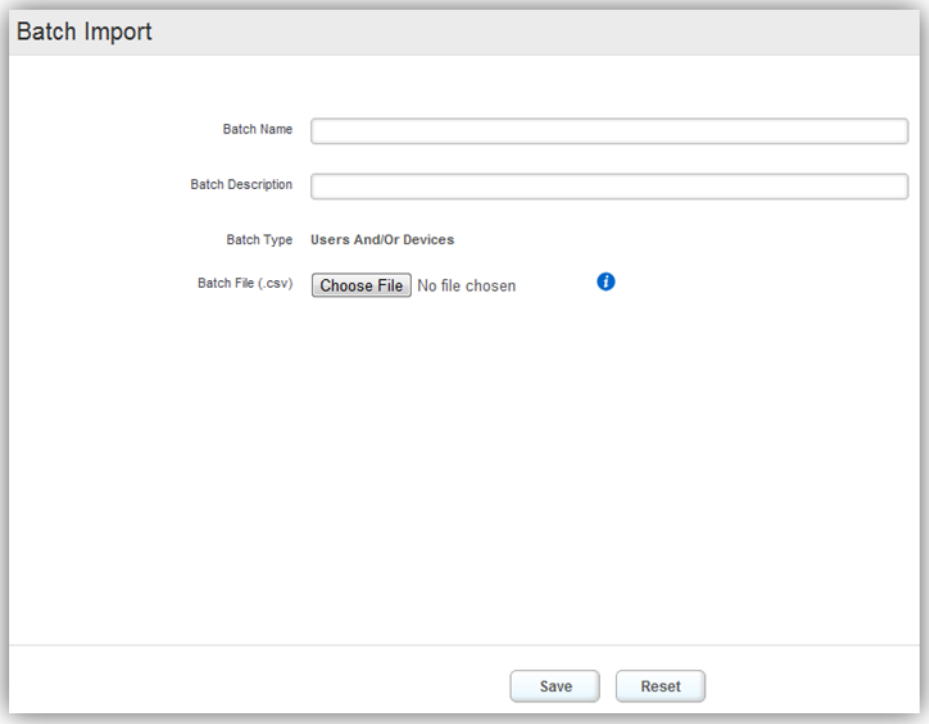
Pentru a economisi timp şi efort în importarea utilizatorilor tăi finali în VSDM, administratorii pot încărca utilizatori finali în grup, prin import de utilizatori finali în grup.

Pentru a crea conturi de utilizator de orice tip (de bază, pe bază de director sau proxy de autentificare), în grup:

▶ Navighează la **Utilizatori→ Conturi de utilizatori**.



▶ Da click pe Batch Import pentru a deschide **Formularul de import în grup.**



▶ Introdu toate detaliile de bază:

- **Nume grup** - Numele utilizatorului/dispozitivului pentru referință în Consola VSDM Admin.
- **Descriere grup**- O descriere a utilizatorului particular /dispozitivului pentru referință în Consola VSDM Admin.

▶ Da click pe pentru a deschide Formularul de import în grup.

- ▶ De aici, selectează **Descărcare şablon** pentru a descărca **Şablonul de import în grup.**
- ▶ Introdu toate informațiile relevante pentru fiecare utilizator în şablon. Trei utilizatori de eşantionare (unul din fiecare Tip de securitate) au fost adăugați în partea de sus a şablonului ca referință pentru ce tip de informații se pun în fiecare coloană.
- ▶ Toate câmpurile din şablon sunt identice cu câmpurile care sunt folosite în timpul procesului de Creare a conturilor de utilizator şi procesul individual de înregistrare a dispozitivului .

- Câmpurile obligatorii sunt desemnate cu un asterisc *
- Coloana E, **Tipul de securitate**, este folosită pentru a determina ce tip de securitate (de bază, pe bază de director sau Proxy de autentificare) ar trebui utilizată pentru a crea contul de utilizator.
- Pentru a înregistra un dispozitiv, Coloana T**, Înregistrare numai pentru utilizator** trebuie să fie setată la **Nu**.
- Pentru a înregistra un dispozitiv suplimentar pe acelaşi cont de utilizator, asigura-te că toate informațiile din **Coloanele A–T** sunt aceleaşi. Coloanele rămase sunt folosite pentru a înregistra fiecare dispozitiv suplimentar.
- Pentru a stoca informații avansate de înregistrare, Coloana AA **, Stocare informații avansate dispozitiv** trebuie să fie setată la **Da**.
  - ▶ Odată ce ai terminat, salvează şablonul ca un fişier **.CSV**, selectează **Browse** din **Formularul Import în grup** şi selectează fişierul **.csv** pe care tocmai l-ai creat.
  - ▶ Când ai terminat, dă click pe **Salvare** pentru a înregistra toți utilizatorii enumerați şi dispozitivele corespunzătoare.

Înregistrarea dispozitivului

Înregistrarea dispozitivului permite atât administratorilor cât şi utilizatorilor finali posibilitatea de a introduce informații despre dispozitivele specifice care sunt înscrise în cadrul gestionării dispozitivului mobil. Această caracteristică oferă, de asemenea, un nivel suplimentar de autorizare sigură, astfel încât numai dispozitivele autorizate se pot înscrie. Există mai multe moduri în care înregistrarea se poate realiza pentru a se acomoda diferitelor nevoi şi cerințe.

- **Administratorul poate înregistra dispozitive individuale** pentru a adăuga un dispozitiv important şi informații despre articol cum ar fi numele prietenos (numele dispozitivului creat de administrator pentru recunoaşterea uşoară în VSDM), modelul, sistemul de operare, numărul de serie, UDID şi numărul articolului. Acest proces poate urma direct crearea Contului de utilizator selectând **Salvare şi Adăugare dispozitiv.**

- **Administratorii pot înregistra o listă de dispozitive** (din motive similare precum cele listate mai sus) în grup. Acest proces are loc în timpul Creării Contului de Utilizator.

- **Administratorii pot invita utilizatorii finali să se înregistreze** pentru ca ei înşişi să poată introduce detalii despre dispozitivele lor şi să inițieze înregistrarea dispozitivului de la terminalul lor. Acest proces are loc pe dispozitivul utilizatorului final în Portalul Self Service.

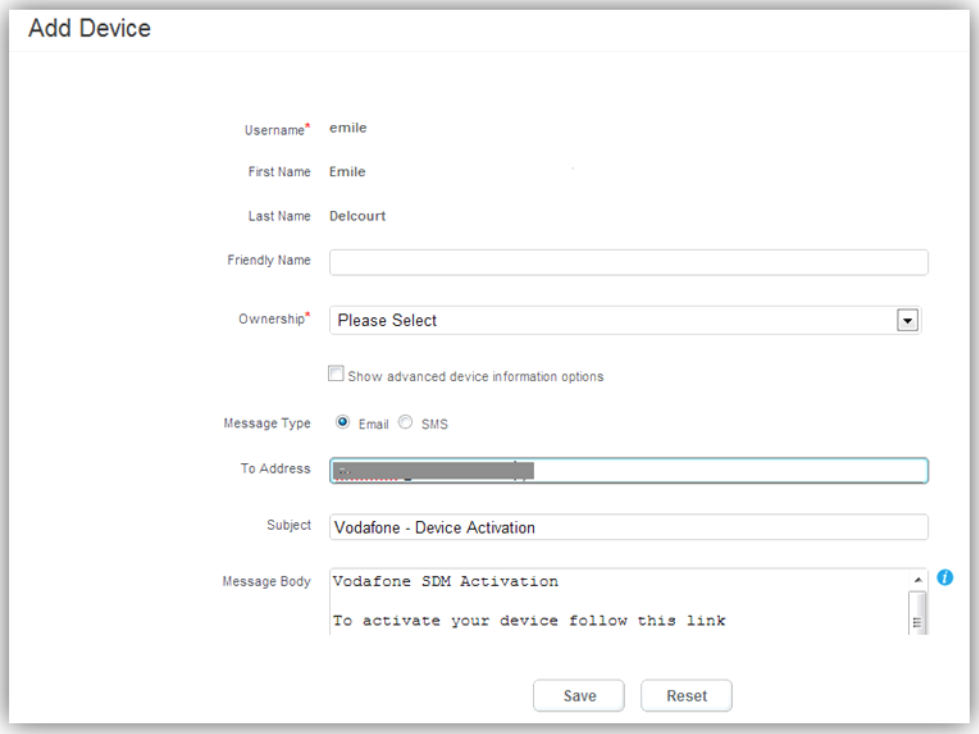
2.1.12 Admin înregistrează un singur dispozitiv

Pentru a înregistra un dispozitiv individual:

- Navighează la **Utilizatori→Conturi de utilizatori** şi selectați **Adăugare dispozitiv** de lângă contul de utilizator existent pe care doreș ti să-l asociezi la dispozitiv.

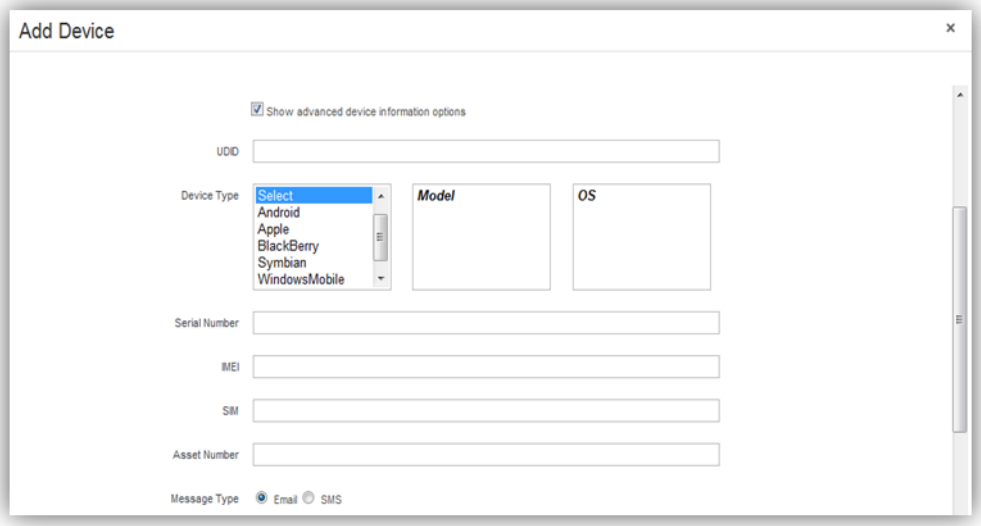
SAU

- Completează Procesul de Creare a unui Nou Utilizator şi selectează **Salvare şi Adăugare dispozitiv** la sfârşit.
- Aceasta deschide formularul **Adăugare dispozitiv**. Completează informațiile de bază.



- **Numele prietenos** - Numele dispozitivului ce va fi afişat în Consola VSDM Admin pentru o recunoaştere uşoară.
- **Tipul de proprietate**-Specificarea unui tip de proprietate (Corporativ-dedicat, Corporativ-Divizat sau Proprietatea angajatului), pentru a face distincția între dispozitive corporative şi cele deținute de angajat. Acest lucru permite administratorului să personalizeze politicile VSDM în funcție de tipul de proprietate pentru a permite maximum de intimitate şi protecție.
- **Tipul mesajului**- Specifică dacă mesajul de activare va fi trimis prin SMS sau e-mail.
- **Adresa / Subiect/ Corp mesaj** - textul mesajului care este trimis la adresa furnizată după ce dispozitivul este înregistrat. Acest mesaj conține de obicei linkul de înscriere şi ID-ul grupului.

- Bifează **Afişează opțiuni avansate de informații despre dispozitiv** pentru a introduce manual informații suplimentare despre dispozitiv pentru a fi afişate în VSDM.



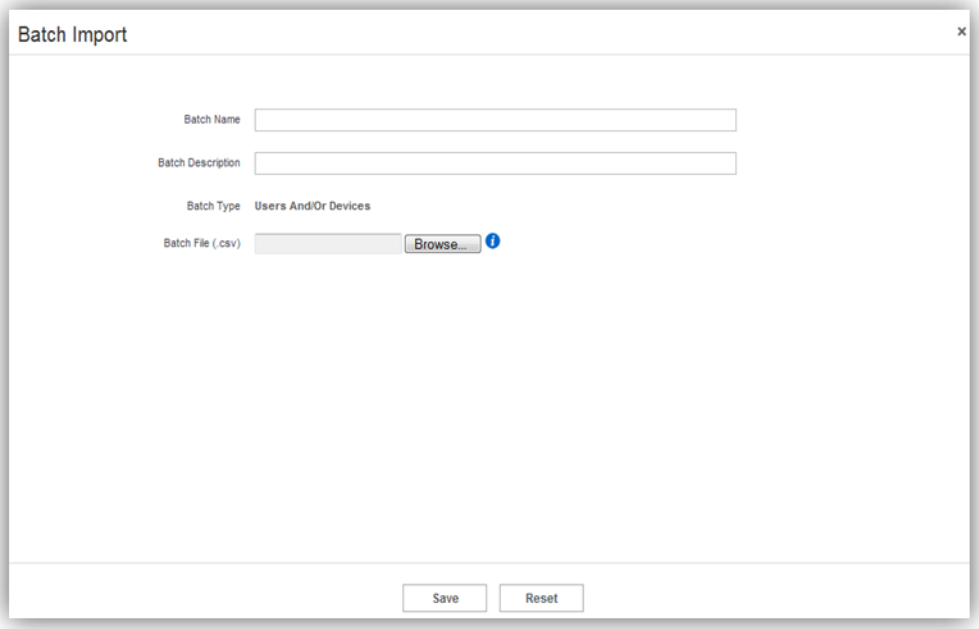
- **UDID** - Universal Device Identifier - Identificator Dispozitiv Universal
- **Platformă / Model / OS** - Informații specifice privind dispozitivul
- **SN / IMEI / SIM / Număr articol** - numerele de referință specifice ale dispozitivului pentru a distinge acest dispozitiv specific.

▶ Când ai terminat dă click pe **Salvare** pentru a finaliza formularul şi a trimite mesajul specificat utilizatorilor finali.

▶ Utilizatorul final primeşte mesajul şi continuă cu înscrierea.

2.1.13 Administratorul înregistrează o listă de dispozitive

1. Dă click pe Batch Import pentru a deschide **Formularul de import în grup.**



▶ Introdu informațiile de bază:

- **Nume grup** - Numele grupului utilizatorului/dispozitivului pentru referință în Consola VSDM Admin.
- **Descriere grup**- O descriere a grupului utilizatorului /dispozitivului respectiv pentru referință în Consola VSDM Admin.

▶ Dă click pe  pentru a deschide Formularul de import în grup.

De aici, selectează **Descărcare şablon** pentru a descărca Şablonul de import al grupului.

▶ Introdu toate informațiile relevante pentru fiecare dispozitiv în şablon. Trei utilizatori de eşantionare au fost adăugați în partea de sus a şablonului ca referință pentru ce tip de informații se introduc în fiecare coloană.

- Toate câmpurile din şablon sunt identice cu câmpurile care sunt folosite în timpul procesului de Creare Contului de utilizator şi a procesului individual de înregistrare a dipozitivului.
- Pentru a înregistra un dispozitiv, **coloana T, Înregistrare numai pentru utilizator** trebuie să fie setată la**Nu**.
- Pentru a înregistra un dispozitiv suplimentar pe acelaşi cont de utilizator, asigură-te că toate informațiile din **Coloanele A–T** sunt aceleaşi. Coloanele rămase sunt folosite pentru a înregistra fiecare dispozitiv suplimentar.
- Pentru a stoca informații avansate de înregistrare, coloana AA **, Stocare informații avansate despre dispozitiv** trebuie să fie setată la **Da**.

▶ Odată ce ai terminat, salvează şablonul ca un fişier .CSV, selectează **Browse** din Formularul de Import în grup şi selectează fişierul .csv file pe care tocmai l-ai creat.

▶ Când ai terminat, selectează **Salvare** pentru a înregistra toți utilizatorii enumerați şi dispozitivele corespunzătoare.

2.1.14 Administratorul invită utilizatorii să se înregistreze

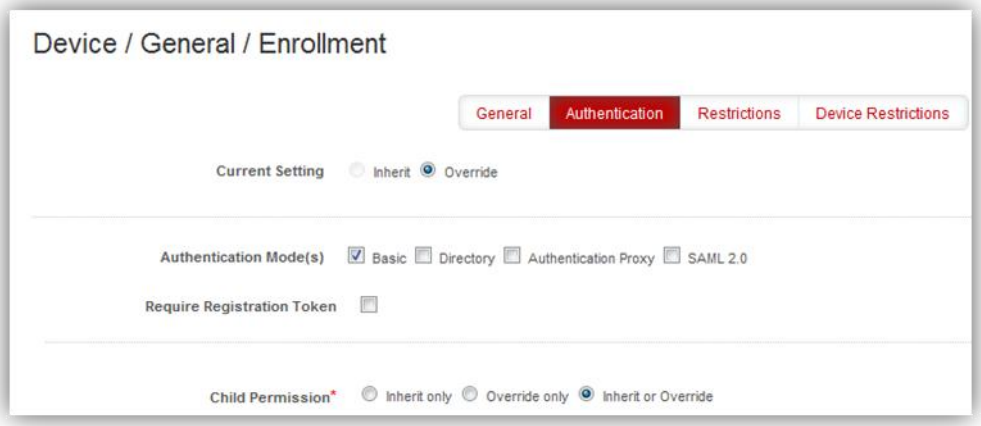
În cazul în care un administrator doreşte ca utilizatorii finali să-şi înregistreze propriile dispozitive, administratorul trebuie să informeze utilizatorii finali că trebuie să finalizeze procesul de înregistrare şi să le ofere un URL de înregistrare şi acreditări (te rugăm să consulți Crearea utilizatorilor finali de bază).

Există mai multe moduri de a notifica utilizatorii finali:

▶ Administratorul trimite un e-mail sau notificări intranet întregului grup de utilizatori din afara Vodafone cu instrucțiunile de înregistrare.

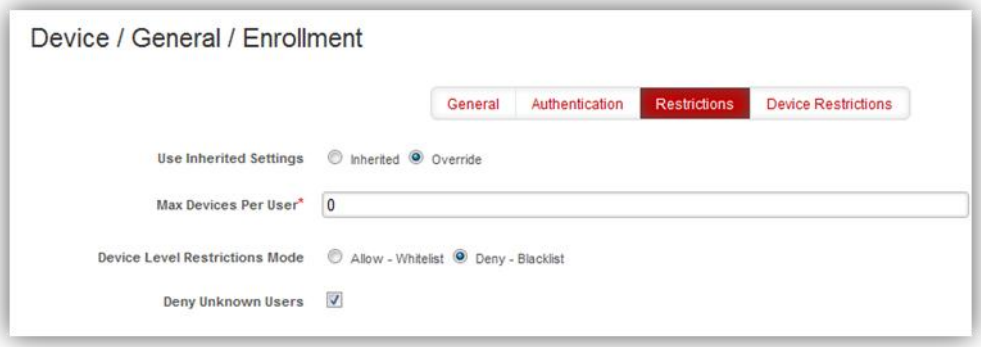
- Această metodă este folosită în general în cazul în care administratorii nu au niciun utilizator deja creat pentru utilizatorii finali şi doresc ca aceştia să poată să se poată înscrie şi înregistra fără asistență. Pentru ca utilizatorii să îşi poată înscrie dispozitivele fără eforturi administrative:

▶ Autentificarea înscrierii trebuie activată pentru fiecare Director Activ sau Proxy de autentificare (editați aceste setări în **Configurare →Setări de sistem→Dispozitiv→General→Înscriere→Autentificare**)



ŞI

- Repinge utilizatorii necunoscuți în Restricții de înscriere (editează aceste setări în **Configurare→Setări de sistem→Dispozitiv→General→Înscriere→Restricții**) nu pot fi bifate.



- Alternativ, administratorii pot crea mai întâi conturi de utilizator pentru toți utilizatorii finali pentru a-şi înregistra dispozitivele şi apoi trimite mesaje de activare a contului de utilizator pentru fiecare utilizator, conținând instrucțiunile de înregistrare.

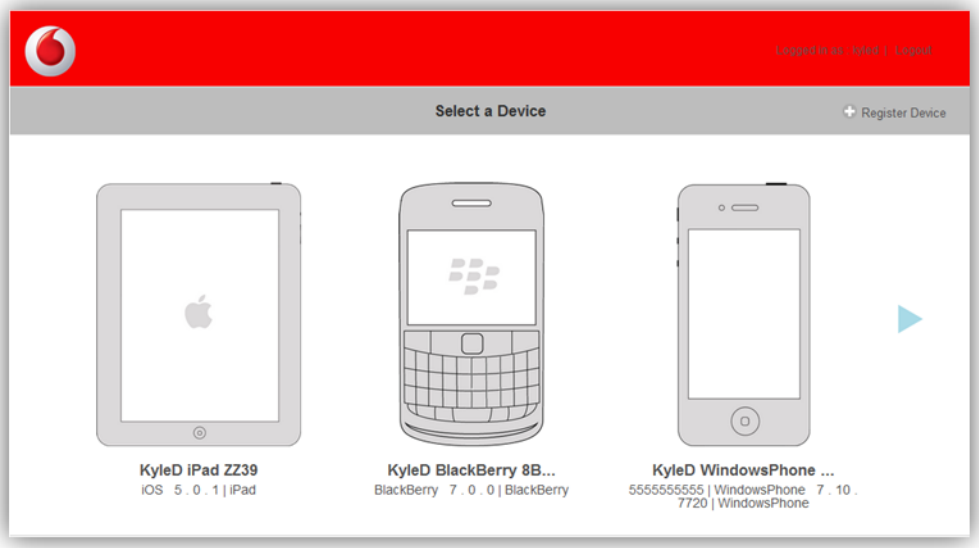
În orice caz, administratorul trebuie să anunțe utilizatorul final cu privire la două lucruri:

- **Unde să se înregistreze** – Utilizatorii finali se pot înregistra navigând la **URL-ul portalului de Self-Service**.
  - Acest URL are forma **https://<VodafoneEnvironment>/MyDevice** în care **<VodafoneEnvironment>** este URL-ul de înscriere.
- **Cum să te autentifici în Portalul de Self-Service** – această informație include un **Grup de locație (ID Grup)**, **Utilizatorul** şi **Parola** pe care utilizatorii trebuie să le folosească pentru a-şi înregistra dispozitivul.

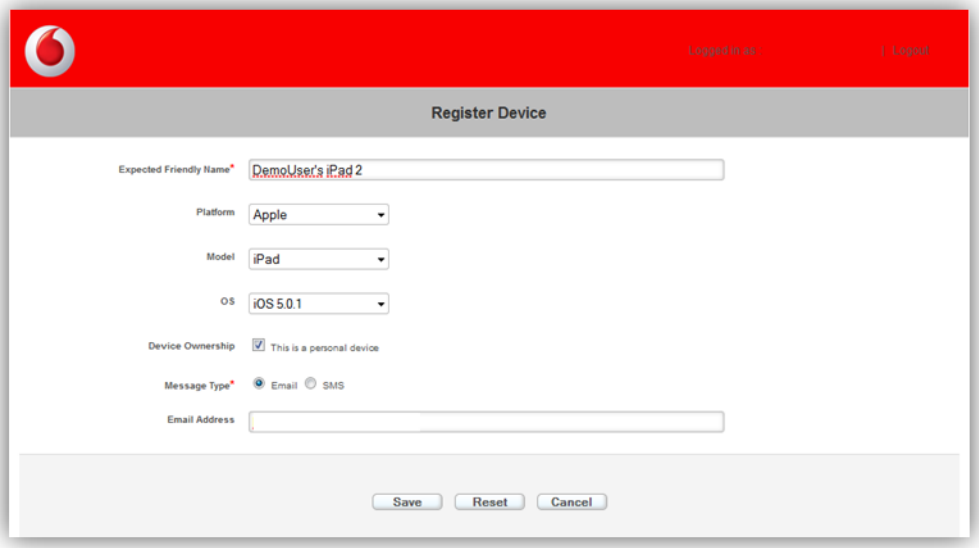
2.1.15 Înregistrarea utilizatorilor finali

După ce administratorul trimite notificarea de înregistrare utilizatorului (cu excepția cazului în care administratorul înregistrează dispozitivele în numele utilizatorilor), utilizatorii finali trebuie să îşi înregistreze dispozitivul. Utilizați următorii paşi meniți să ghideze utilizatorii finali în procesul de înregistrare.

- Navighează la **URL-ul portalului de Self-Service** (fie în browserul dispozitivului, fie din orice browser de internet).
- Introdu numele de utilizator şi parola furnizate.
- Din pagina următoare, selectează **Înregistrare dispozitiv** pentru a deschide **Formularul de înregistrare a dispozitivului.**



- Completează câmpurile de informare privitoare la dispozitiv.



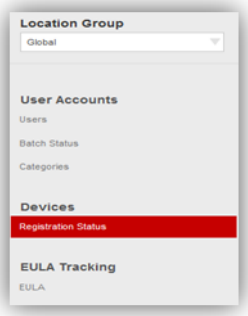
- **Numele prietenos** - Numele dispozitivului care este afişat în Consola de Admin VSDM (numele prietenos poate fi de asemenea folosit pentru a urmări statusul de înregistrare al dispozitivului). De exemplu, “iPad-ul lui John Smith”.
- **Platforma / Modelul / sistem de operare** - Detaliile dispozitivului specific.
- **Proprietatea asupra dispozitivului** - Selectează dacă dispozitivul este unul personal.

- **Tipul mesajului** - Selectează formatul mesajului pentru confirmarea înregistrării utilizatorului final.
- **Adresă email / Număr de telefon** - Adresa sau numărul de telefon al recipientului acestui mesaj.

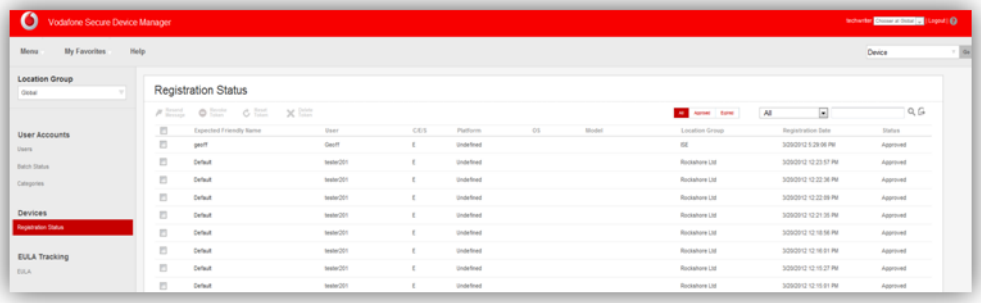
▶ Când ai terminat, dă click pe **Salvare** pentru a finaliza procesul de înregistrare al Utilizatorului final.

2.1.16 Statutul de înregistrare al dispozitivului

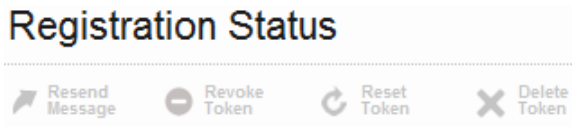
Vodafone permite administratorilor să urmărească statutul de înregistrare al dispozitivului, indiferent dacă utilizatorul a înscris sau nu dispozitivul. După ce înregistrarea dispozitivului a fost realizată prin oricare din procesele descrise mai sus (Administratorul înregistrează un singur dispozitiv , o listă de dispozitive , sau administratorul permite utilizatorilor finali să își înregistreze propriile dispozitive), administratorii pot vizualiza înregistrarea și statutul de înscriere al dispozitivului din **Statutul înregistrării** de pe pagina **Conturi de utilizatori**.



De aici, administratorii pot vizualiza detaliile de înregistrare, data și statutul mesajului de înregistrare trimis la utilizatorii finali.



În plus, administratorii pot gestiona procesul de înregistrare prin cele patru butoane ale acțiunii de înregistrare din partea de sus a paginii.

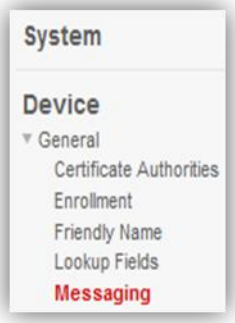


- **Retrimitere mesaj -** Retrimiterea mesajului de înregistrare dispozitivelor selectate, cu o bifă în dreptul numelui lor prietenos.
- **Revocare Token -** Forțează statutul de înregistrare al dispozitivelor selectate mai jos pentru expirare. Acest lucru împiedică în esență, înscrierea acestor dispozitive din cauza unui token expirat.
- **Resetare Token –**Dacă un dispozitiv de înregistrare a fost revocat sau a expirat, administratorii pot da click pe "Resetare Token" pentru a reactiva tokenul de înregistrare, astfel încât să se poată efectua înscrierea.
- **Ştergere Token -** Această comandă şterge permanent tokenul de înregistrare pentru dispozitivele selectate de mai jos, astfel că acestea trebuie să se re-înregistreze pentru a se înscrie.

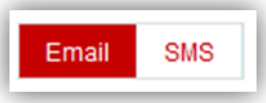
2.1.17 Personalizarea mesajelor de înregistrare

Pentru a personaliza mesajul de înregistrare trimis către utilizatorii finali după ce îşi înregistrează dispozitivele:

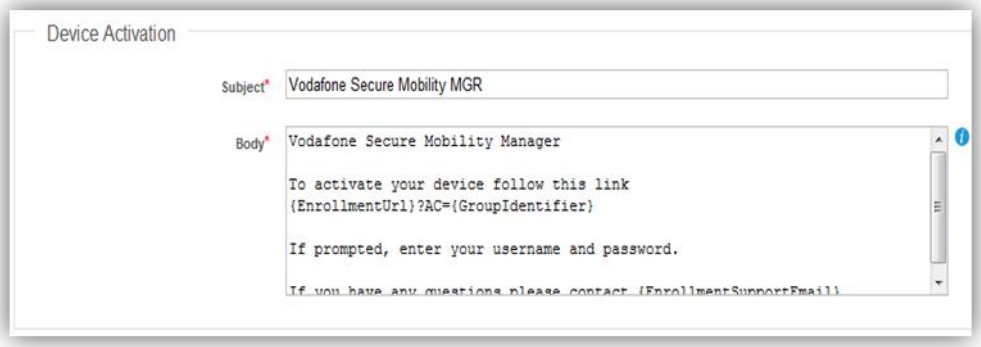
- Navighează la **Configurare→Setări sistem→Dispozitiv→General→Mesaje** pentru a deschide formularul mesajului de activare a Utilizatorului şi a Dispozitivului.



- Pentru a modifica **Şabloanele de mesaje e-mail** pentru activarea utilizatorului şi a dispozitivului, selectează **E-mail** din partea de sus a paginii. Alternativ, selectează **SMS** pentru a modifica mesajele text de tip trimise dispozitivelor.



- Din fiecare tab, administratorii pot modifica mesajul **Activarea contului utilizatorului** sau mesajul de **Activare dispozitiv**. Derulează în jos la secțiunea **Activare dipozitiv** .



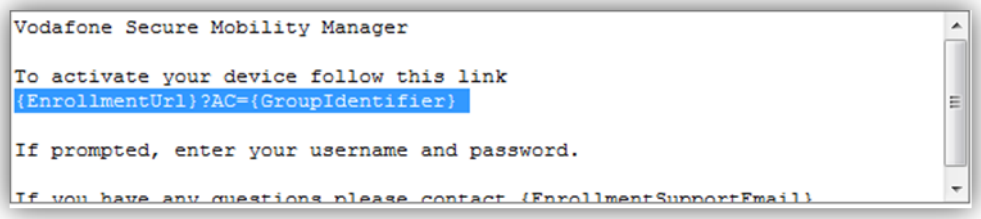
- Introdu **subiectul** mesajului de email sau SMS şi **corpul mesajului**.
- Când ai terminat, dă click pe **Salvare.**

Folosirea variabilelor în mesajele de înregistrare

În timpul creării şablonului de mesaj pentru activarea dispozitivului descris în secțiunea anterioară, administratorii pot pune în funcțiune **Valorile de căutare** pentru a adăuga conținut dinamic mesajului de activare care este special pentru fiecare destinatar.

▶ Din formularul arătat mai sus dă click pe pentru a deschide o listă de posibile **valori de căutare** şi descrieri.

▶ Administratorii pot introduce oricare din valorile de căutare listate în corpul mesajului cu aceste simboluri: **{}**



- De obicei utilizatorii finali trebuie să obțină următoarele din mesajele lor de înregistrare:
  - ▶ URL de înscriere: {EnrollmentURL}
  - ▶ Identificator grup: {GroupIdentifier}
  - ▶ Nume utilizator & parolă: {EnrollmentUsername} & {EnrollmentPassword}
  - ▶ Tokenul (dacă este folosit tokenul pentru înscriere): {EnrollmentToken}
- Pentru a încorpora un URL de înscriere în identificatorul grupului de utilizatori, utilizează următoarea valoare de căutare:
  - ▶ {EnrollmentUrl}?ac={GroupIdentifier}

▶ Când ai terminat, dă click pe **Salvare**.

Valori de căutare curente

- **Domeniu email** – Domeniul căruia îi aparține contul de utilizator respectiv.
- **EmailUserName** – Numele de utilizator pentru e-mail, fără partea "@companie.com". Numele de utilizator asociat cu e-mailul unui utilizator corporativ.
- **EmailAddress –** Adresa completă de email a contului de utilizator.
- **EnrollmentUser –** Numele contului de utilizator.
- **EnrollmentUserId –** ID-ul unic al contului de utilizator.
- **DeviceUid** – Identificatorul unic al dispozitivului.
- **DynamicScepChallenge** – Un câmp utilizat în şabloanele certificat pentru a permite serverelor SCEP să se integreze în mod corespunzător în soluție pentru configurații certificate dinamice.
- **GroupIdentifier** – Identificatorul grupului al grupului de locație în care un utilizator sau un dispozitiv se înscrie.
- **SessionToken** – Tokenul unic care este folosit în timpul procesului de înregistrare pentru a asocia un dispozitiv ce se înscrie cu un dispozitiv care a fost recent înregistrat.
- **DeviceFriendlyName** – Nume prietenos afişat în Consola VSDM Admin pentru un dispozitiv.
- **DeviceSerialNumber** – Numărul serial al dispozitivului.
- **UserPrincipalName** – Numele principal al utilizatorului atunci când utilizatorii sunt integrați în serviciile directoare. Folosit potențial pentru integrarea certificatului.
- **DeviceSerialNumberLastFour –** Ultimele patru caractere alfanumerice ale numărul serial al dispozitivului.
- **DevicePlatform** – Platforma dispozitivului specific.
- **DeviceModel** – Modelul unui dispozitiv specific.
- **DeviceOperatingSystem** – Sistemul de operare al dispozitivului specific.
- **DeviceUidLastFour** – Ultimele patru caractere alfanumerice ale Identificatorului unic.
- **DeviceReportedName** – Numele raportat al unui dispozitiv care s-a înregistrat dar nu a fost încă înscris.
- **EmailPassword** – Parola unui utilizator pentru a pentru a recupera mailul individual corporativ.

Cele mai bune practici

- Acordă atenție ierarhiei grupului de locație atunci când creezi şi editezi conturilor administrative. Este important să activezi opțiuni la grupul cu locația cea mai înaltă, pentru a te asigura că administratorul are capacitățile adecvate de editare.
  - Grupul de locație selectat poate fi întotdeauna afişat în colțul din stânga sus colțul al VSDM.
- Există trei informații pe care administratorul trebuie să le comunice utilizatorilor finali:
  - URL-ul de Înscriere Vodafone (oferit de Vodafone) care este acelaşi URL folosit pentru accesarea Consolei VSDM Admin.
  - ID-ul grupului pentru a identifica grupul de locație original (ID-ul grupului este determinat în **Configurare→Locații & Grupuri→Detalii Grup de locație**)
  - Numele de utilizator şi parola unică a utilizatorului final (Numele şi parola sunt determinate în **Utilizatori→Conturi utilizator→Adăugare utilizator** sau **Editare utilizator**)
    - În funcție de **Tipul de securitate**, utilizatorul şi parola pot fi create de administrator (**de bază**) sau integrate în **Director**, **Proxy de autentificare**,or **SAML**.

Dacă compania ta utilizează înregistrarea dispozitivului şi are nevoie de asistență, te rugăm să contactezi biroul local de asistență Vodafone.

3.0 Gestionarea dispozitivului

Prezentare generală

Gestionarea dispozitivului smart este centralizată în consola Vodafone Secure Device Manager. De aici, administratorul este în măsură să creeze următoarele caracteristici VSDM:

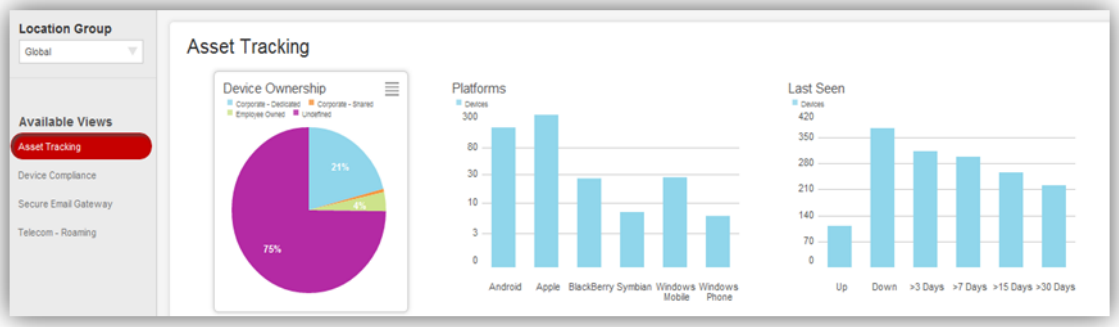
- Particularizarea urmăririi articolelor în forma datelor în timp real a grupului de sispozitive mobile, indiferent de tipul de dispozitiv, transportator sau locație.
- Navigarea printr-un bord de date mobile şi de telecomunicații pentru a ajuta organizația să ia decizii mai informate pe baza utilizării reale a telecomunicațiilor mobile.
- Efectuarea acțiunilor de la distanță pe dispozitive.
- Generarea unui set de rapoarte.
- Activarea de alerte proactive atât pentru pentru utilizatori cât şi pentru administratori atunci când pragurile

Notă: Această secțiune se referă la dispozitive iOS, Android, Blackberry, Symbian şi Windows Phone 7. Pentru mai multe informații despre gestionarea dispozitivelor Windows Mobile, consultați *Ghidul de administrare Windows Mobile*.

Următoarele secțiuni descriu modul în care administratorii pot activa anumite pagini în VSDM pentru a gestiona în mod efectiv şi eficient dispozitivele smart.

Navigare Bord

Pagina **Bord** centralizează monitorizarea dispozitivelor smart oferind administratorilor situații la nivel înalt a grupurilor de dispozitive smart, cu capacitatea de a detalia la nivel de dispozitiv individual. Pentru a accesa **Pagina de bord**, navigați la **Borduri→Bordul**



De aici, administratorii pot vedea o imagine de ansamblu de grafice şi statistici pentru un grup de locație sau de flota întregul dispozitiv, sau localiza rapid informații cu privire la un anumit dispozitiv, făcând clic pe numele prietenos.

3.1.1 Bara laterală grup de locație

Bara laterală a grupului de locație de pe partea stângă a ecranului permite administratorilor să vizualizeze dispozitivele care aparțin unui grup de locație specific şi toate grupurile sale copii, în mod eficient. Există, de asemenea, mai multe instrumente care pot fi folosite pentru a găsi grupuri de locație specifice:

- **Structura arborescentă extensibilă** - Găsirea grupurilor de locație şi afişarea legăturilor de la grupurile părinte la grupurile copil.
- **Caseta de căutare** - Căutarea unor grupuri specifice de locație în funcție de nume.
- **Capacitatea de extindere / restrângere** - extinde sau restrânge ierarhia grupurilor de locație.
- **Capacitatea de prindere** - Prinderea barei laterale a grupului înapoi pe bara laterală a Bordului.

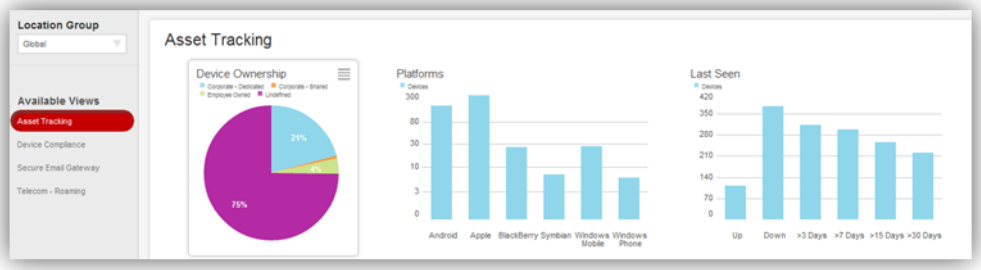
3.1.2 Ecrane disponibile

Există, de asemenea, mai multe **Ecrane disponibile** pe pagina de Bord care oferă administratorilor posibilitatea de a vizualiza liste întregi de dispozitive pe baza indicatorilor listați mai jos:

- **Monitorizare terminal** –Vizualizarea dispozitivelor pe baza tipului de proprietate, platformă şi ultimele măsurători văzute.
- **Conformitate dispozitiv** –Vizualizarea dispozitivelor pe baza conformității acestora la normele privind dispozitivele compromise, politicile privind codul de acces şi Protecția Datelor instituită de Apple.
- **Poartă de email securizată** –Vizualizarea dispozitivelor care încearcă să obțină acces corporativ la e-mail prin Email Secure Gateway şi a statutului lor. Aceasta este o caracteristică opțională care impune ca componentele să fie implementate la fața locului.

3.1.3 Miniporturi grafice

Miniporturile grafice de pe pagina de **Bord** furnizează date statistice relevante şi oferă o modalitate uşoară de a selecta un grup de dispozitive în funcție de o serie de categorii (exemplul de mai jos este din ecranul **Monitorizare terminal**).



Pentru a schimba ecranul la un grup selectat de dispozitive (de la un miniport grafic):

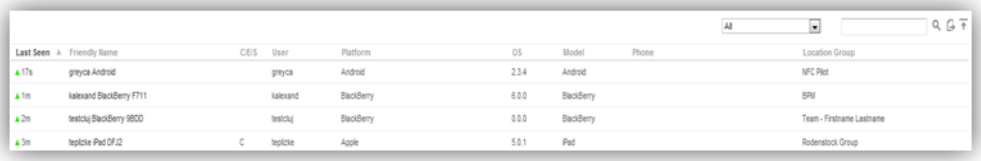
▶Dă click pe grafic pentru a **evidenția** miniportul.

▶Dă click pe **Grup de date** în colțul din dreapta sus a miniportului pentru a comuta miniportul la alt ecran.

▶Selectează un **Grup de date.** Aceasta modifică lista dinamică de dispozitive pentru a afişa numai dispozitivele care aparțin grupului de specificat de date.

3.1.4 Lista dispozitivelor dinamice

Lista dispozitivelor dinamice de pe pagina **Bord** conține o listă flexibilă a dispozitivelor şi datelor care aparțin fiecărui ecran:

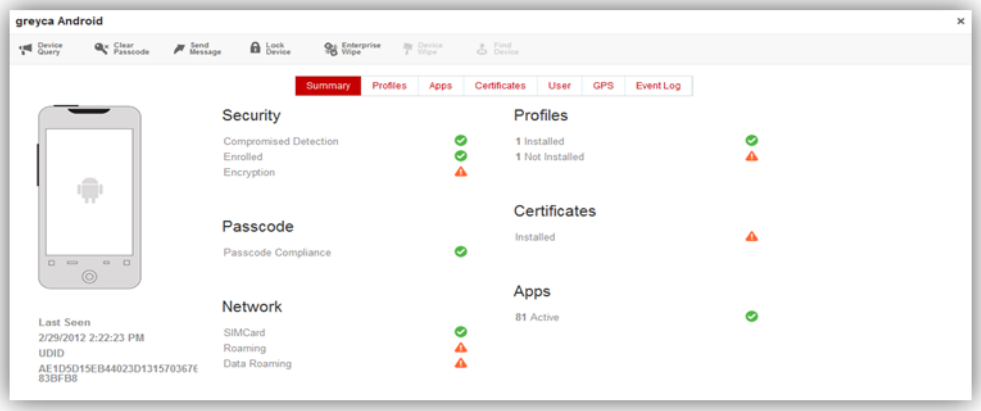


Există multe moduri prin care un administrator poate selecta, ordina şi identifica dispozitive specifice din Lista de dispozitive dinamice:

- Selectează oricare din **Ecranele disponibile**.
- Dă click pe oricare dintre Grupurile de date din miniporturile grafice.
- Dă click pe oricare din **Categoriile din coloană** (cum ar fi "Ultimul vizualizat" sau "Nume prietenos") pentru a reordona lista.
- Utilizarea oricăror instrumente suplimentare de căutare şi vizualizare din colțul din dreapta sus a listei:

Panoul de control al dispozitivului

Când administratorii doresc să vadă informații detaliate sau să efectueze acțiuni de la distanță la nivel de dispozitiv individual, ei pot acționa **Panoul de control al dispozitivului** disponibil din pagina de **Bord**. Pentru a deschide **Panoul de control al dispozitivului**, localizează un dispozitiv individual pe pagina de Bord utilizând oricare din instrumentele disponibile de căutare şi apoi selectează-l. Vor apărea informațiile din **Panoul de control al dispozitivului**:



Panoul de control al dispozitivului conține două meniuri primare:

- O listă de informații a dispozitivului pentru a vizualiza informații detaliate şi statistici.

- O **Listă a acțiunilor de la distanță** pentru a efectua acțiuni administrative over the air.

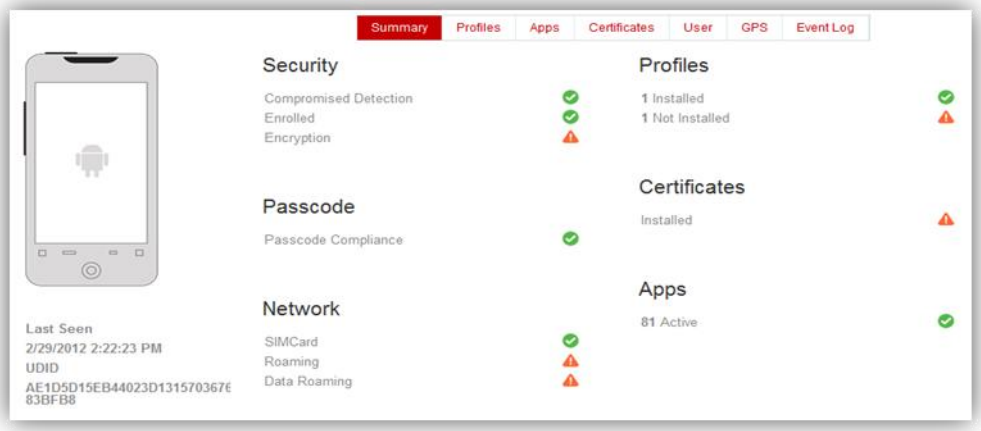
Notă: Informațiile şi acțiunile din Panoul de control al dispozitivului respectă regulile de disponibilitate ale setărilor de confidențialitate şi compatibilitatea platformei.

3.1.5 Lista de informații a dispozitivului

Lista de informații a dispozitivului afişează informații detaliate referitoare la fiecare dintre categoriile enumerate. Mai multe informații despre fiecare categorie de informații ale dispozitivului sunt prezentate mai jos.

Rezumat

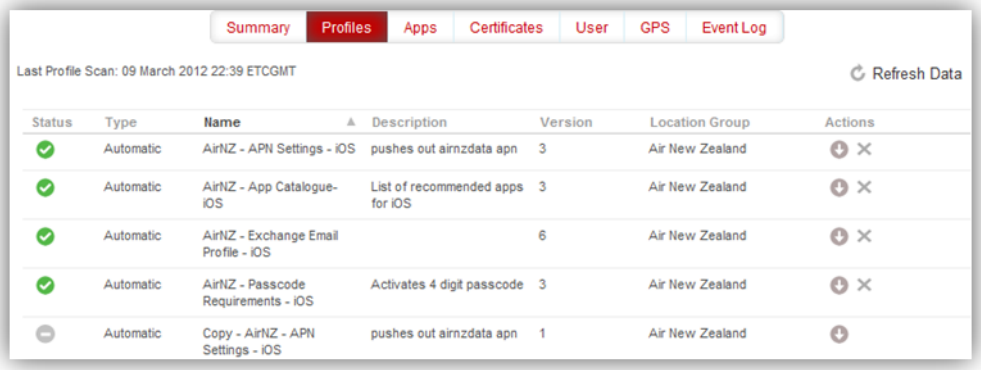
Secțiunea rezumat afişează conformitatea componentei hardware, a VSDM, criptării şi a codului de acces, pe lângă alte informații generale.



- **Hardware** –Afişează informații privind componenta hardware a dispozitivului.
- **Securitate**–Afişează date compromise ale dispozitivului şi date de la nivelul criptării.
- **Codul de acces** –Afişează dacă un cod de acces este prezent sau nu sau dacă îndeplineşte cerințele codului de acces.
- **Rețeaua** –Afişează informații legate de rețea, cum ar fi cartela SIM şi de statutul roaming.
- **Profiluri** –Afişează toate profilurile şi oferă un statut de instalare a profilului.
- **Certificate** –Afişează certificatele instalate şi statutul expirat sau aproape de expirare.
- **Aplicații** –afişează numărul de aplicații instalate pe dispozitiv.
- **Conținut**– Afişează numărul de documente instalate şi numărul de documente atribuite.

Profiluri

Secțiunea **Profiluri** prezintă toate profilurile VSDM care au fost trimise dispozitivului şi statutul fiecărui profil.



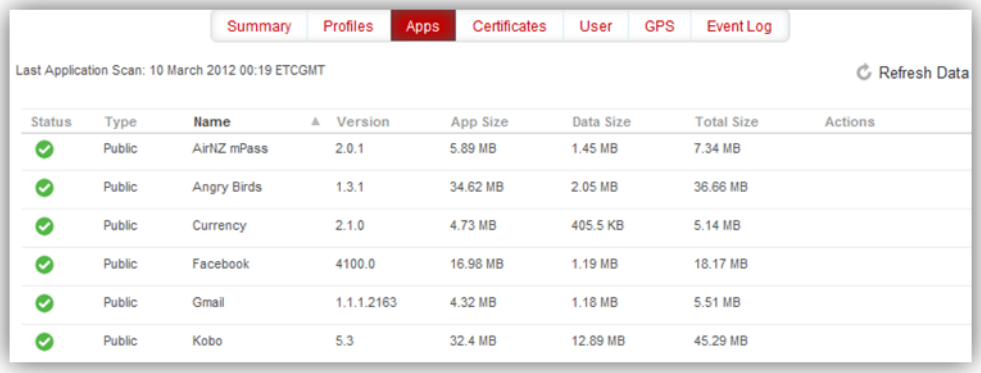
- **Statut** –Afişează statutul de instalare a profilului:

- Instalat
- Instalare în aşteptare
- Neinstalat
- Eliminare în ateptare
- Eliminat

- **Tip** –Afişează tipul profilului: automat, opțional sau interactiv.
- **Versiunea** –Afişează versiunea profilului (de câte ori profilul a fost actualizat).
- **Grupul de locație**–Afişează grupul de locație în care profilul este atribuit.
- **Acțiuni**–Oferă posibilitatea de a instala de la distanță sau elimina profilul.

Aplicații

Secțiunea de aplicații afișează toate aplicațiile care au fost instalate pe dispozitiv (sub rezerva setărilor de confidențialitate specificate în **Configurare→Setări sistem→Dispozitiv→General→Confidențialitate**).



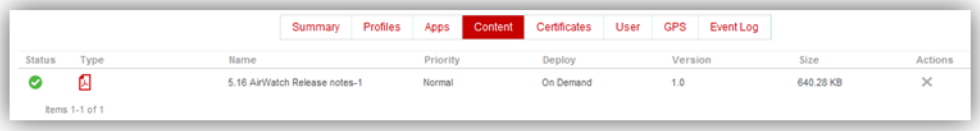
Reține următoarele descrieri de domeniu:

- **Statut** –Afişează statutul de instalare a aplicației:
  - Instalat
  - Instalare în aşteptare
  - Neinstalat
  - Eliminare în ateptare
  - Eliminat
- **Tip** –Afişează este o aplicație internă sau publică.
- **Acțiuni**–Oferă posibilitatea de a instala sau elimina de la distanță aplicația.

Notă numai pentru iOS5: Tab-ul de apllicații pentru dispozitivul iOS5 oferă administratorilor abilitatea de a instala sau revoca aplicațiile gestionate către sau de la dispozitiv over the air.

Conținutul

Aplicabil numai dispozitivelor echipate cu Blocarea securizată a conținutului.

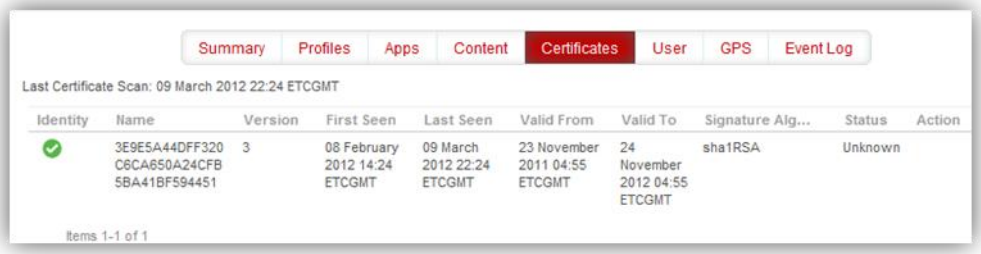


Secțiunea **Conținut** are următoarele detalii și acțiuni privitoare la conținut:

- **Statut** –Afișează statutul de instalare a aplicației:
  - Instalat
  - Instalare în așteptare
  - Neinstalat
  - Eliminare în ateptare
  - Eliminat
- **Tip** –Formatul documentului. Treceți peste pictogramă pentru a afișa tipul de format.
- **Nume** –Numele documentului așa cum apare în Consola VSDM Admin Console și Secure Content Locker.
- **Prioritate** –Prioritatea documentului așa cum este specificată de câmpul Importanță din Conținut→Gestionarea Conținutului→Adăugare sau Editare Document.
- **Implementare** –Există două opțiuni pentru tipul de implementare:
  - **La cerere** –Utilizatorul final trebuie să descarce documentul.
  - **Automat** –Documentul este descărcat automat în dispozitivul utilizatorului final.
- **Versiune**–Afișează documentului (pe baza numărului de actualizări a documentului).
- **Acțiuni**–Oferă posibilitatea de a instala sau elimina conținutul.

Certificate

Secțiunea Certificate prezintă toate certificatele stocate în prezent în dispozitiv și oferă informații de bază de sprijin.

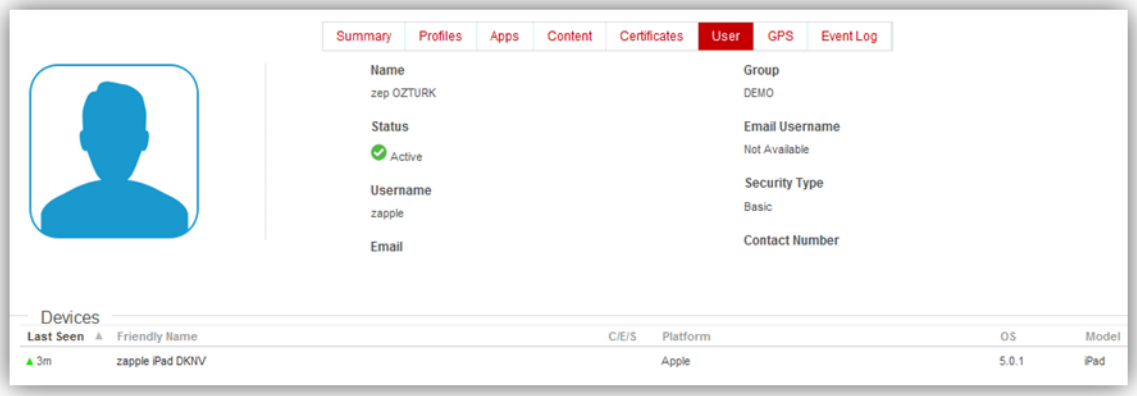


- Dispozitivele iOS trebuie să arate întotdeauna cel puțin un certificat curent care să indice faptul că și-au înscris dispozitivele.

Utilizatorul

Secțiunea **Utilizator** afișează informații specifice (atunci când sunt disponibile și sub rezerva setărilor de confidențialitate așa cum este specificat în **Configurare→Setări sistem→ Dispozitiv →General →Confidențialitate**) inclusiv Numele, Statutul, Numele de utilizator,

Email, Grup, Nume utilizator Email, Tip de securitate şi număr de contact. Afişează, de asemenea, o listă cu toate dispozitivele pe care utilizatorul le-a înscris.

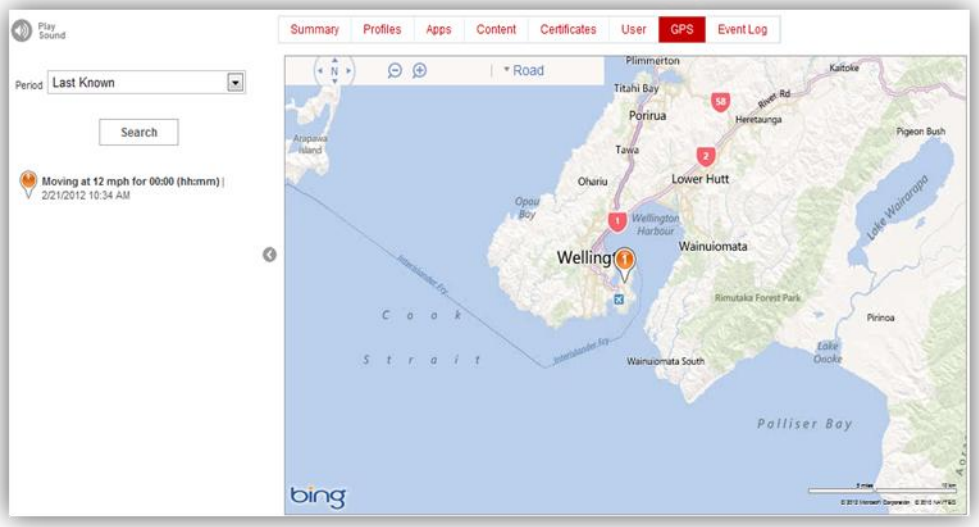


GPS

Secțiunea **GPS** afişează coordonatele GPS ale dispozitivului (subrezerva setărilor de confidențialitate aşa cum este specificat în **Setările sistemului → Dispozitiv →General →Confidențialitate**). Afişajul implicit este "Ultimul cunoscut" (coordonatele cele mai recent primite). Pentru a vizualiza coordonatele GPS pe o perioadă anume de timp:

- Selectează perioada de timp pentru care ați dori coordonatele GPS din **Perioadă**, meniul derulant.
- Dă click pe **Căutare**.

Rezultatele căutării returnează întregul traseu disponibil (breadcrumbs) al coordonatelor GPS pe perioada solicitată.

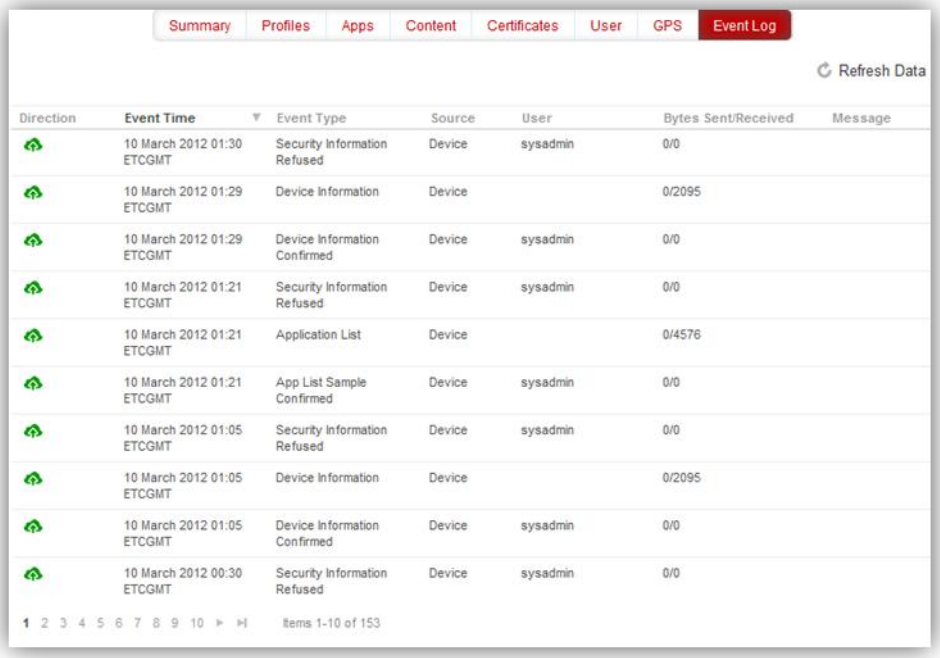


- În plus, pictograma **Redare sunet** este disponibilă pentru a localiza un dispozitiv pierdut. Dă click pe pictogramă pentru a reda un sunet pe dispozitiv.

Jurnal evenimente

Jurnalul de evenimente conține un jurnal cuprinzător al tuturor interacțiunilor dintre VSDM şi dispozitiv. Dă click pe Refresh Data pentru a actualiza instant Jurnalul de evenimente. Câmpuri importante de notat în Jurnalul de evenimente includ următoarele:

- **Direcția**–Afişează direcția evenimentului(☐dispozitiv către server' sau ☐server către dispozitiv')
- **Tipul evenimentului**– Oferă o clasificare scurtă/rezumat al evenimentului. Exemple de evenimente includ:
  - Lista profilului confirmată
  - Check In
  - Statut compromis raportat



3.1.6 Acțiuni de la distanță

Lista de acțiuni de la distanță este afişată mai jos. Cu această listă, administratorii pot efectua oricare dintre următoarele acțiuni listate pe dispozitivul selectat over-the-air.

Interogare dispozitiv

Solicită manual dispozitivului la distanță să trimită un set cuprinzător de informații VSDM la Consola VSDM Admin. Aceasta suprascrie check-in-urile dispozitivului cu o cerere imediată.

Şteregere cod de acces

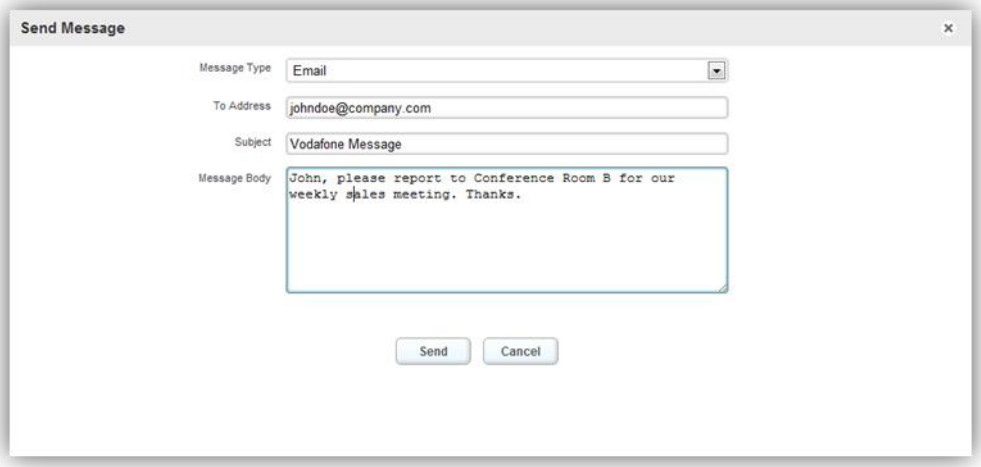
Aceasta şterge codul de acces de pe dispozitivul la distanță. Aceasta poate fi acționată ori de câte ori utilizatorii finali îşi uită codul de acces sau accesul la dispozitiv este blocat.

Trimitere mesaj

Acesta permite administratorilor să trimită diferite tipuri de mesaje dispozitivelor, over-the-air.

- **Email** – Când setările SMTP corporative au fost corect configurate, administratorii au posibilitatea de a trimite e-mailuri de la distanță oricărei adrese.
- **SMS** – Dacă o societate a setat un cont de serviciu pentru SMS-uri cu Cell Trust, şi dacă informațiile de acces au fost corect configurate, administratorii au posibilitatea de a trimite mesaje text SMS de la distanță către orice număr de telefon.

- **APN-uri** – Pentru dispozitivele iOS care au de agentul Vodafone instalat, administratorii pot trimite mesaje automate de notificare Apple, unui utilizator final care afişează corpul mesajului în notificare.



Blocarea dispozitivului

Aceasta blochează dispozitivul, astfel încât utilizatorul trebuie să deblocheze aparatul cu codul de acces corespunzător pentru a continua utilizarea acestuia.

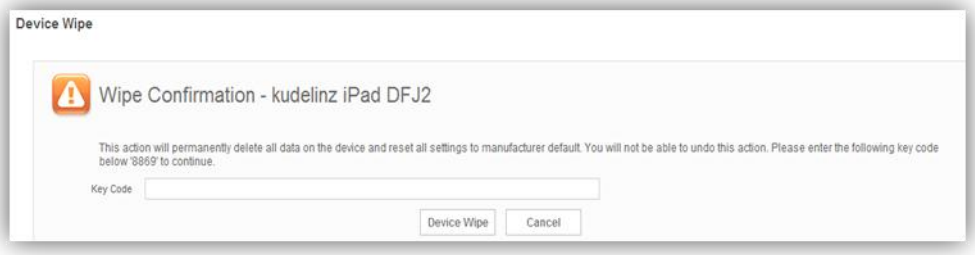
Ştergere totală

Aceasta elimină dispozitivul din Vodafone Secure Device Manager ştergerea dispozitivului şi ştergerea selectivă a datelor conținute pe dispozitiv, în profiluri VSDM, politici şi aplicații interne.

Ştergere dispozitiv

Aceasta efectuează o ştergere completă a aparatului (sub rezerva setărilor de confidențialitate, specificate în **Configurare→ Setări sistem→Dispozitiv→General→Confidențialitate**).

- ▶ Ca o măsură de securitate, un mesaj de confirmare îți va aminti tipul de proprietate al dispozitivului pentru a fi şters. ☐
- Trebuie să introduci codul furnizat înainte de efectuarea ştergerii dispozitivului.
- ▶ Ştergerea dispozitivului va înlătura toate datele, e-mailul, profilurile şi capacitățile VSDM iar telefonul revine la setarea implicită din fabrică.



Găsirea dispozitivului

Această funcționalitate obligă dispozitivele iOS să facă un set de tonuri de notificare sonoră, astfel încât utilizatorii finali să poată localiza aparatul lor.

Vizualizare de la distanță

Acesta oferă o vedere de la distanță a dispozitivelor şi aplicațiilor selectate. Butonul de captură ia o captură de ecran pentru a păstra toate ecranele de eroare sau alte probleme.

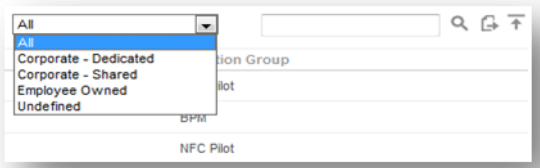
Control de la distanță

Acesta permite unui administrator să controleze de la distanță dispozitivele Windows Mobile din VSDM pentru asistență imediată de la distanță.

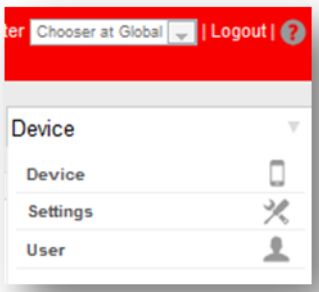
Căutare dispozitive

Aceasta permite unui administrator să localizeze rapid de la distanță un dispozitiv sau un grup de dispozitive, în conformitate cu următoarele opțiuni de căutare:

- **Bara laterală a grupului de locație**–Dă click pe un grup de locație pentru a vizualiza dispozitivele care aparțin acelui grup şi de toate grupurile-copii.
- **Domenii sortate**–Sortează oricare dintre coloanele de rețea dând click pe numele coloanei.
- **Criterii rețea**–Filtrează rețeaua în conformitate cu criteriile dispozitivului, prin selectarea criteriilor de la meniul derulant.



- **Căutare rețea**–Caută rețeaua selectată în mod curent prin tastarea unui termen de căutare (cum ar fi numele prietenos al dispozitivului, modelul, platforma, în caseta "Filtru rețea" (aşa cum se vede mai sus).
- **Căutare avansată**–Caută VSDM prin localizarea casetei de căutare din partea de sus dreaptă a ecranului.
  - Selectează una din următoarele categorii de căutare din meniul derulant: Dispozitiv, Echipament, Locație, Setări sau Utilizator.
  - Introdu cuvântul cheie de căutare.
  - Dă click pe **Căutare**.

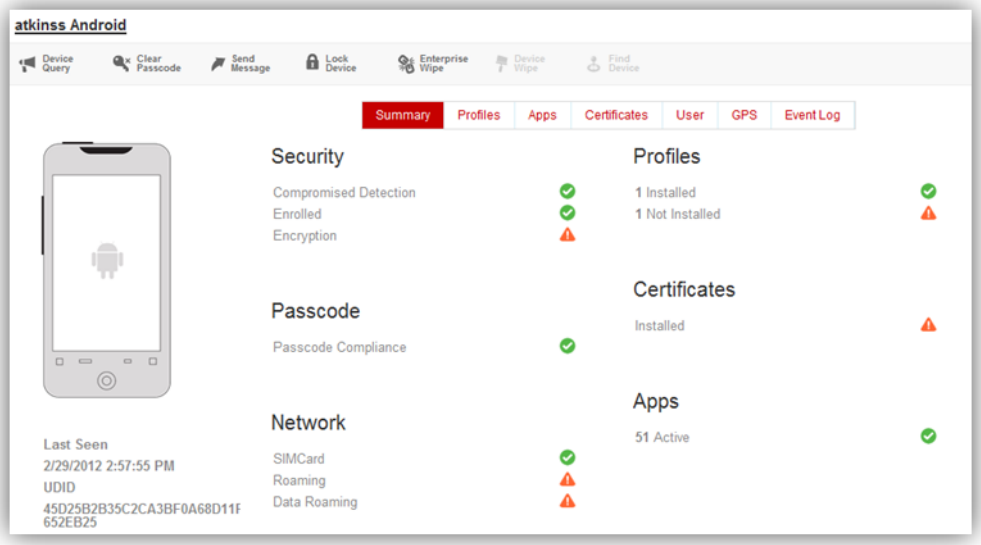


Cuvântul cheie al căutării este evidențiat în rezultate. Când efectuezi o căutare avansată, dând click pe numele dispozitivului se afişează pagina **Detaliile dispozitivului** în locul **Panoului de control a dispozitivului**.

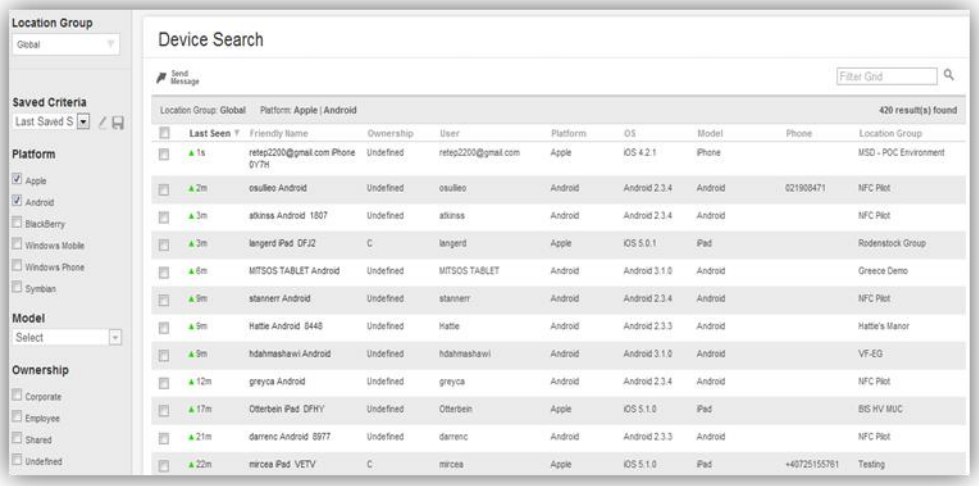
Detalii dispozitive

Administratorul poate urmări informații detaliate ale dispozitivului, pe lângă accesarea rapidă a utilizatorului şi întreprinderea de acțiuni de gestionare vizualizând Detaliile dispozitivului. Există două moduri de a vizualiza Detaliile dispozitivului.

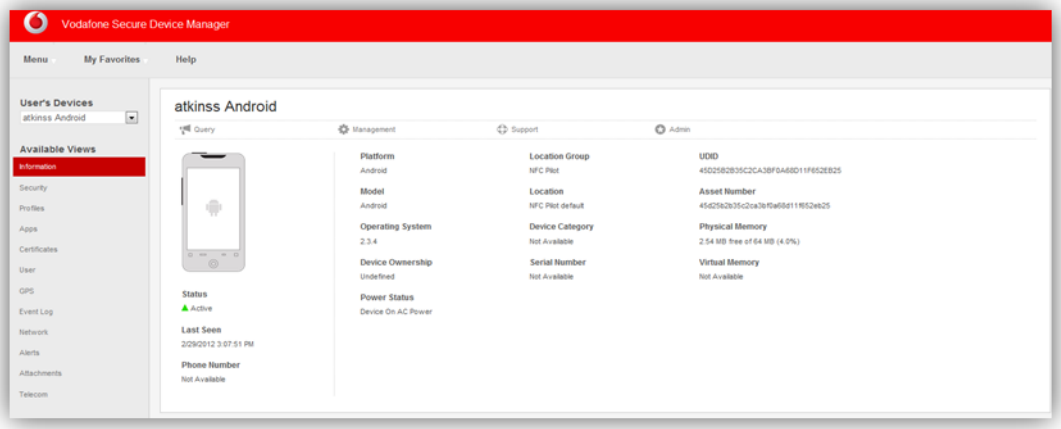
- Dă click pe **Numele prietenos** al dispozitivului din bordul acestuia. Când apare Panoul de control al dispozitivului, dă click pe nume din nou.



- Sau, folosește oricare din [instrumentele de căutare](#) pentru a căuta un dispozitiv individual.



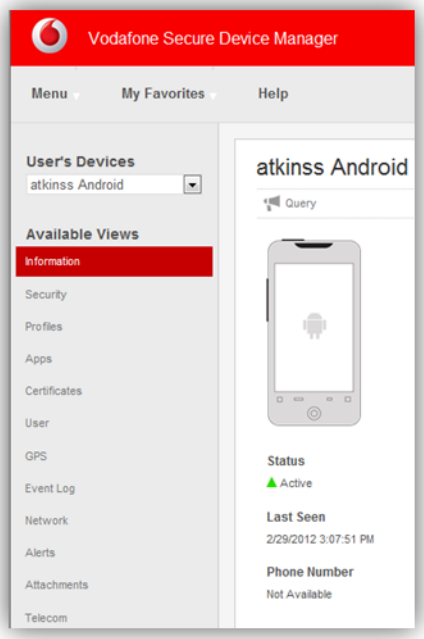
- Din pagina de rezultate ale căutării, dă click pe **Numele prietenos** al dispozitivului individual pentru a deschide pagina cu **Detaliile dispozitivului**:



Din pagina **Detalii dispozitiv**, administratorii pot vizualiza toate informațiile prezentate în **Panoul de control al dispozitivului** pe lângă alte valori mai detaliate.

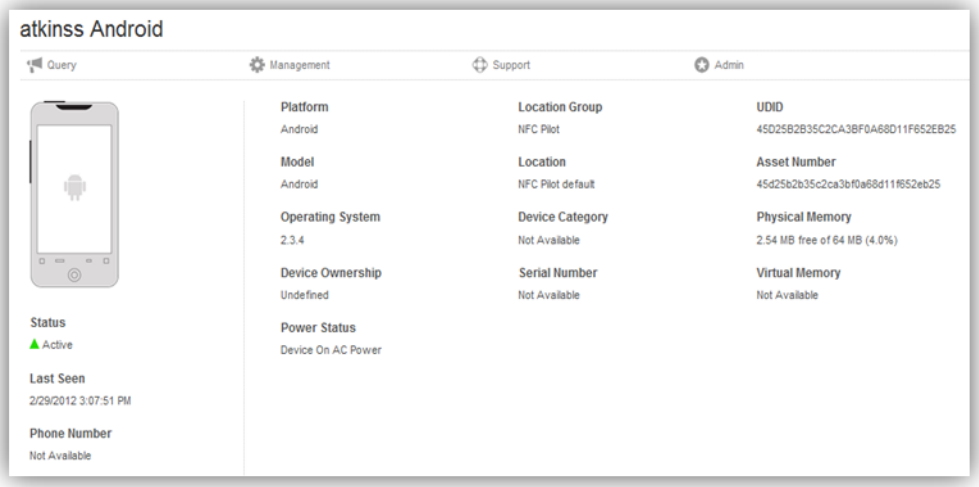
- Multe din Detaliile dispozitivului sunt identice cu informațiile din Panoul de control al dispozitivului. Pentru informații privind Securitatea, Profilurile, Aplicațiile, Certificatele sau ecranele de Jurnal evenimente, consultă Panoul de control al dispozitivului.

- Dă click pe diferite **Ecrane disponibile** în partea stângă a **Detaliilor dispozitivelor** pentru a vedea detalii individuale conform categoriilor descrise mai jos.



3.1.7 Informaţii dispozitiv

Ecranul informaţii dispozitiv este afişat în mod implicit când pagina cu **Detaliile dispozitivului** este deschisă dar poate fi afişat din nou selectând tab-ul **Informaţii** din **Ecrane disponibile**.



Din acest ecran, administratorii pot vedea o serie de statistici generale despre dispozitivul curent, inclusiv:

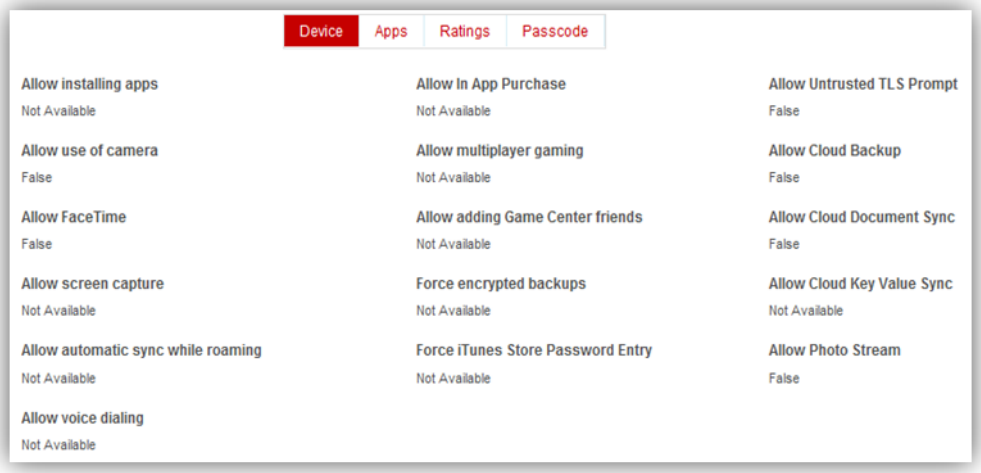
- ▶Statut dispozitiv şi Ultimul vizualizat
- ▶Numărul de telefon (atunci când este disponibil şi sub rezerva la setărilor de confidenţialitate specificate în **Configurare→Setări sistem→Dispozitiv →General →Confidenţialitate**)
- ▶Platformă/Model/OS
- ▶Proprietate dispozitiv/Categorie dispozitiv/Grup dispozitiv
- ▶Grup de Locaţie/Locaţie
- ▶Număr serial/UDID/Număr articol
- ▶Statut încărcare/Memorie fizică/Memorie virtuală

3.1.8 Restricţii dispozitiv

Pentru a afişa **Ecranul cu Restricţii ale dispozitivului**, selectează tab-ul **Restricţii** din Ecrane disponibile. De aici, administratorii pot vedea toate restricţiile de securitate care au fost plasate pe dispozitiv, prin utilizarea profilurilor de restricţii. Această informaţie este organizată în patru ecrane distincte: **Dispozitiv**, **Aplicaţii**, **Evaluări**, şi **Codul de acces**.

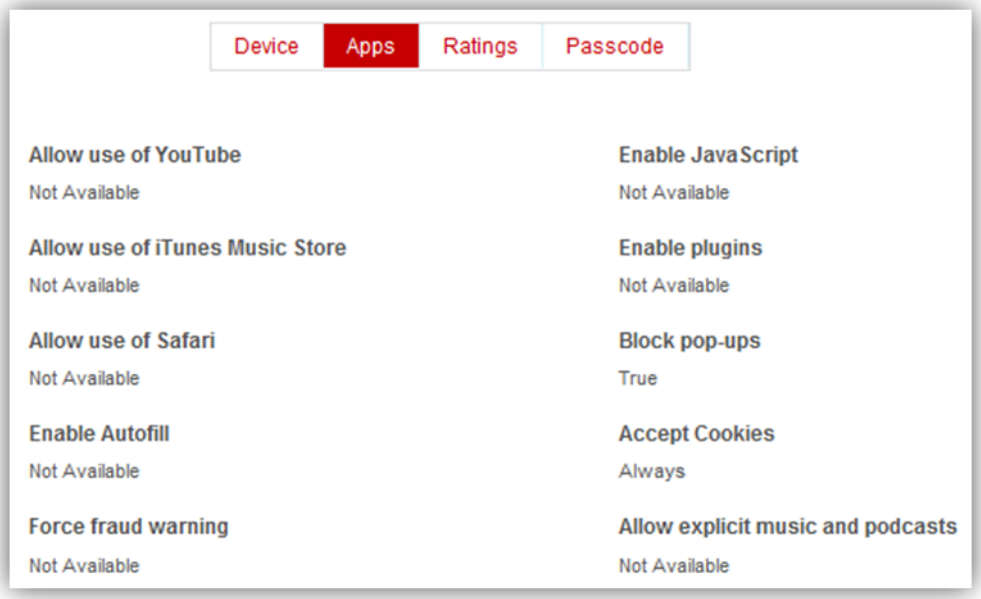
Dispozitivul

Tab-ul **Dispozitivul** afişează toate restricţiile în vigoare pentru dispozitiv de la un nivel generic de sistem. Acestea nu sunt limitate, în ceea ce priveşte domeniul de aplicare, la cereri individuale sau profiluri, ca celelalte tab-uri de restricţii.



Aplicații

Tab-ul **Aplicații** afişează restricțiile implementate privind aplicațiile în dispozitiv.



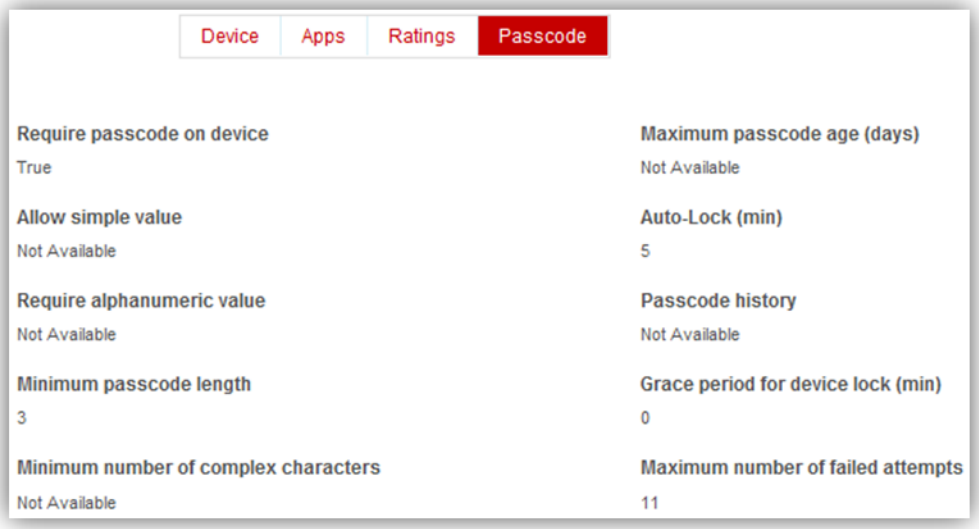
- **Permisiune utilizare YouTube** elimină aplicația YouTube din dispozitiv astfel încât utilizatorii finali nu o pot utiliza.
- **Permisiune utilizare iTunes Music Store** şi **Permisiune muzică explicită şi podcast-uri** limitează aceste caracteristici specifice din cadrul aplicațiilor iTunes.
- Permite utilizarea Safari, Enable Autofill, Force Fraud Warning, Enable JavaScript, Enable Plug-ins, Block pop-ups, şi Accept Cookies se aplică toate aplicației browser Safari Web.

Evaluări

Tab-ul **Evaluări** prezintă toate restricțiile care determină controlul de conținut al filmelor, emisiunilor TV şi aplicațiilor de la iTunes şi App Store. Daca filtrarea de conținut se aplică, numai anume mass-media specifice, care are un rating de vârstă mai mic, sunt permise pentru descărcare.

Codul de acces

Tabul **Codul de acces** prezintă toate setările curente ale codului de acces prevăzute pentru dispozitiv.



3.1.9 Locația dispozitivului

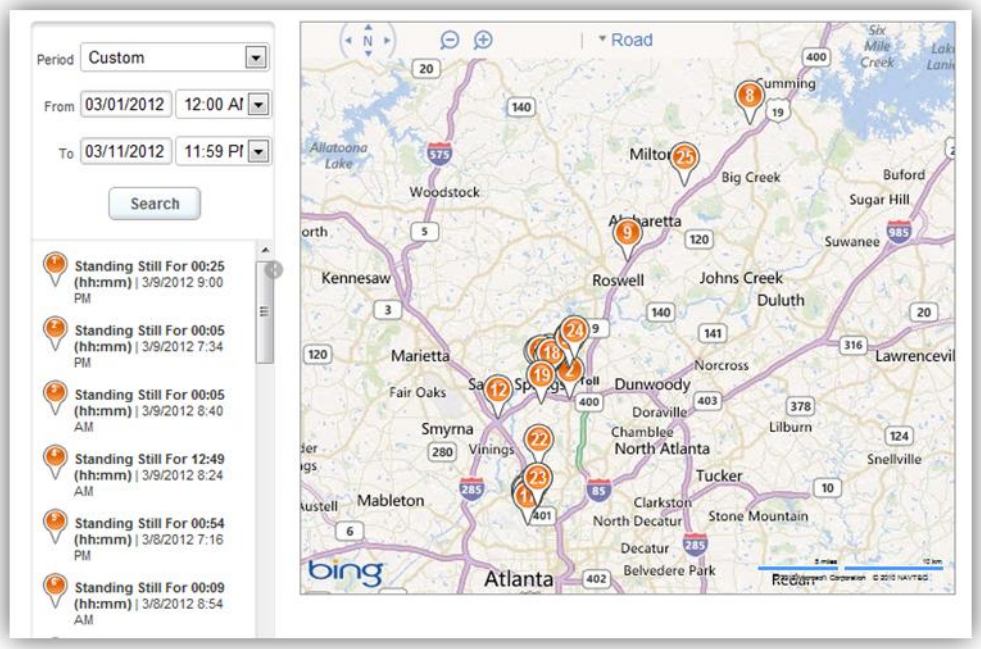
Pentru a vizualiza locația curentă sau istoria de locații a dispozitivului, selectează tab-ul **GPS** din Ecrane disponibile.

Acesta afișează coordonatele GPS ale dispozitivului (sub rezerva setărilor de confidențialitate așa cum sunt specificate în **Setări sistem→ Dispozitiv →General →Confidențialitate**). Afișajul implicit este "Ultimul cunoscut" (coordonatele cele mai recent primite).

Pentru a vizualiza coordonatele GPS pe o perioadă anume de timp:

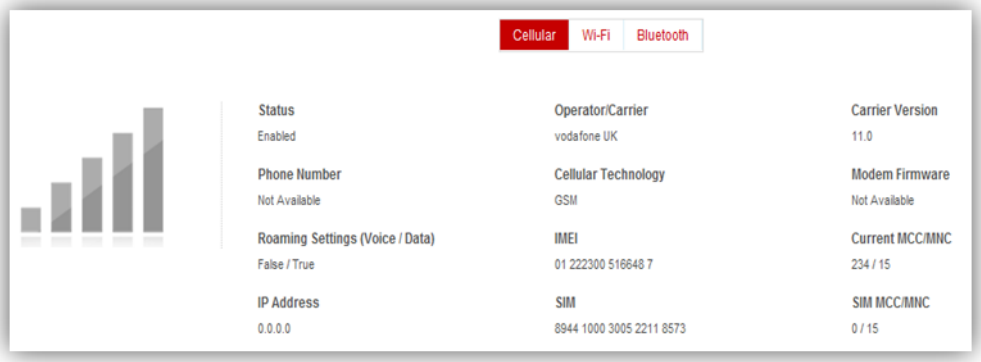
- Selectează perioada de timp pentru care ai dori coordonatele GPS din **Perioadă**, meniul derulant.
- Dă click pe **Căutare**.

Rezultatele căutării returnează întregul traseu disponibil (breadcrumbs) al coordonatelor GPS pe perioada solicitată.



3.1.10 Statutul rețelei

Pentru a vizualiza statutul curent al unui dispozitiv, selectează tab-ul **Rețeaua** din Ecrane disponibile.



De aici, administratorii pot alege oricare dintre tab-urile diferite pentru a vizualiza **Celular, Wi-Fi,** şi informații legate de rețeaua **Bluetooth**.

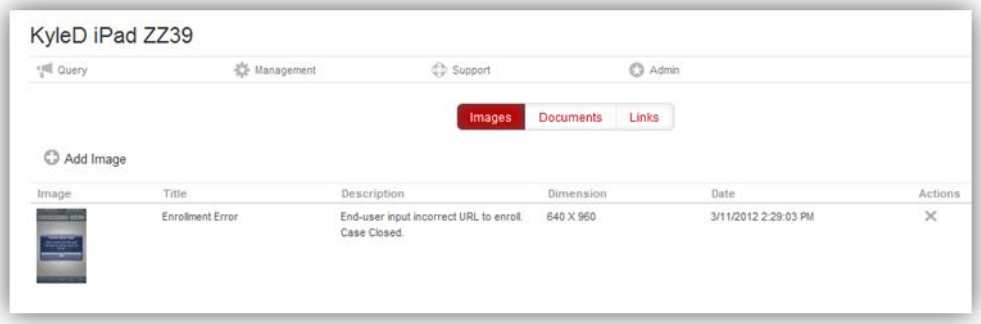
3.1.11 Alerte

Pentru a vizualiza toate alertele care au fost declanşate de către dispozitivul curent, selectați tab-ul **Alerte** din Ecrane disponibile.

De aici, administratorii pot vedea detalii specifice de alertare pentru **Severitate, Prioritate, Atribute, Valori, Durată, Dată alertă,** şi **Politică de creare**.

3.1.12 Ataşamente

Pentru a ataşa imagini, documente sau link-uri care sunt relevante pentru dispozitiv, selectează tab-ul **Ataşamente** din Ecrane disponibile.

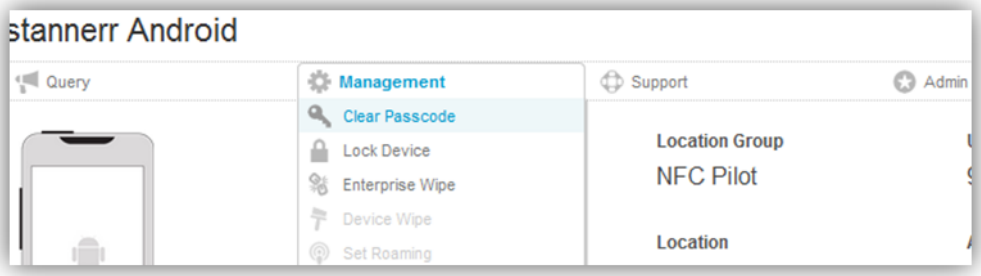


Există trei ecrane în tab-ul de ataşamente; **Imagini**, **Documente**, şi **Link-uri**. Aceste categorii sunt utilizate numai în cadrul Consolei de administrare VSDM pentru a ajuta administratorii să organizeze ataşamentele. Exemple de informații relevante pe care administratorii pot dori să le includă în acest domeniu includ:

- Copii de tichete de asistență cu privire la dispozitiv
- Capturi de ecran ale dispozitivului
- Documentație de sprijin privind dispozitivul

Gestionarea detaliilor dispozitivului

Meniul **Gestionarea detaliilor dispozitivului** (situat sub numele prietenos al dispozitivului) oferă comenzi rapide pentru gestionarea rapidă atât a dispozitivului cât şi a contului de utilizator asociat cu dispozitivul.



Mută mouse-ul pe **Interogare**, **Gestionare**, **Asistență**, sau **Admin** pentru a vizualiza opțiunile de gestionare a meniului derulant.

3.1.13 Interogare

Meniul **Interogare** permite administratorului să solicite informații de la dispozitiv. Dă click pe categorie pentru a trimite o interogare la dispozitiv. Selectați **Interogare completă** pentru a solicita tuturor categoriilor sau a trimite interogări individuale pentru următoarele informații privitoare la dispozitiv:

- Informații dispozitiv
- Securitate
- Profiluri
- Aplicații
- Certificate

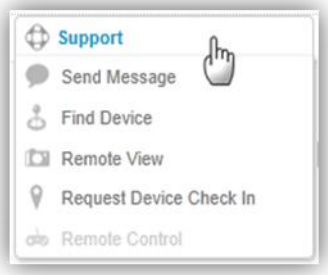
3.1.14 Gestionare

Meniul **Gestionare** permite administratorului să efectueze imediat următoarele acțiuni de la distanță pe dispozitiv (consultă secțiunea Acțiuni de la distanță pentru informații despre primele patru opțiuni):

- **Ştergere cod de acces**
- **Blocarea dispozitivului**
- **Ştergere totală**
- **Ştergere dispozitiv**
- **Setare Roaming** –Activează sau dezactivează opțiunile de roaming pentru voce şi date.

3.1.15 Asistență

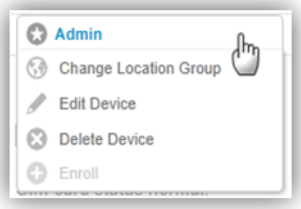
Meniul Asistență oferă opțiuni de a efectua următoarele acțiuni de la distanță (consultă secțiunea Acțiuni de la distanță pentru informații despre primele trei opțiuni):



- **Trimitere mesaj** (E-mail, SMS sau notificare automată)
- **Găsirea dispozitivului**
- **Vizualizare de la distanță**
- **Solicitare de conectare a dispozitivului**–Trimite un mesaj la dispozitiv ce solicită conectarea la Agentul Vodafone.
- **Control de la distanță** (disponibil numai pentru Windows Mobile)-control de la distanță a dispozitivului

3.1.16 Admin

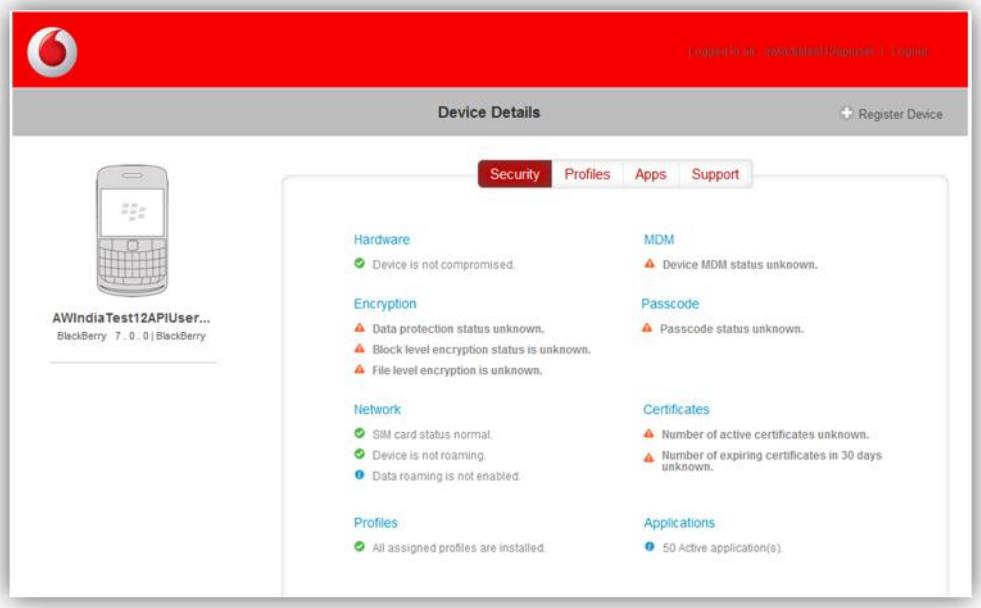
Meniul **Admin** permite administratorilor să editeze instantaneu următorul dispozitiv şi setările utilizatorului:



- **Modificare Grup locație**–editează grupul de locație al utilizatorului.
- **Editare dispozitiv**–Editează următoarele setări ale dispozitivului:
  - Nume prietenos
  - Tip de proprietate a dispozitivului
  - Grup dispozitiv
  - Categorie dispozitiv
- **Ştergere dispozitiv**
- **Înscriere** - Înscrie dispozitivul în Vodafone Secure Device Manager

Self-Service utilizator final

Portalul Vodafone de Self-Service permite utilizatorilor finali să monitorizeze şi să-şi gestioneze de la distanță dispozitivele smart.



Portalul Self-Service, prezentat mai sus, oferă administratorilor posibilitatea de a vizualiza informații relevante pentru orice dispozitiv înscris, şi să efectueze acțiuni de la distanță, cum ar Ştergere cod de acces, Blocare dispozitiv sau Ştergere dispozitiv.

3.1.17 Activarea portalului Self-Service

Utilizatorii finali ai dispozitivelor iOS şi Android pot accesa portalul de Self Service direct de pe dispozitivul lor.

▶ Avantajele accesării portalului Self-Service de pe dispozitivul gestionat includ:

- Utilizatorii finali pot vizualiza informații de conformitate importante.
- Utilizatorii finali pot descărca rapid profilurile opționale.
- Utilizatorii finali pot gestiona mai multe dispozitive gestionate de la Portalul Self-Service pe un singur dispozitiv.

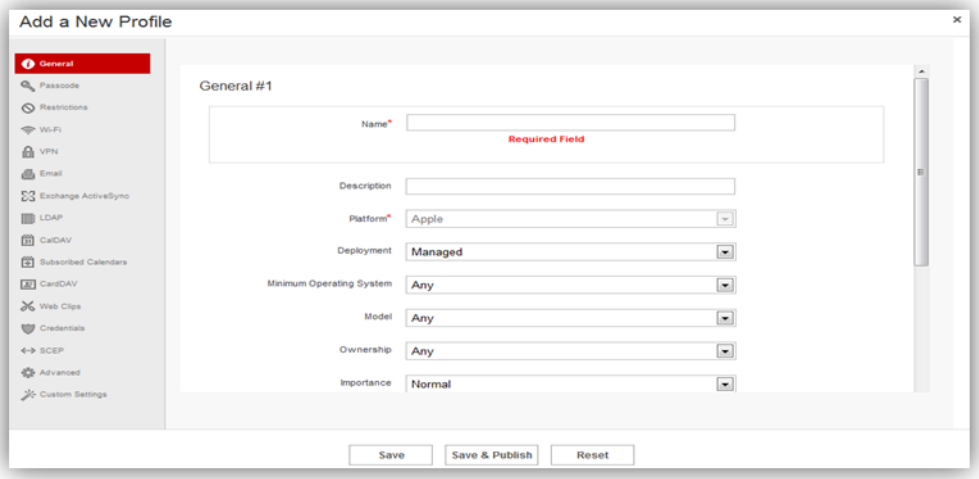
Pentru ca utilizatorii finali să acceseze portalul de Self-Service din dispozitivul lor, administratorul trebuie să implementeze mai întâi un clip Web (iOS) sau să marcheze profilul (Android) care conține profilul URL-ul pentru aplicația bazată pe web a portalului de Self-Service. Paşii de mai jos descriu procesul pentru implementarea portalului de Self-Service (a se vedea Crearea profilurilor pentru instrucțiuni privind crearea unui profil):

▶ Navighează la Profiluri & Politici→Profiluri.

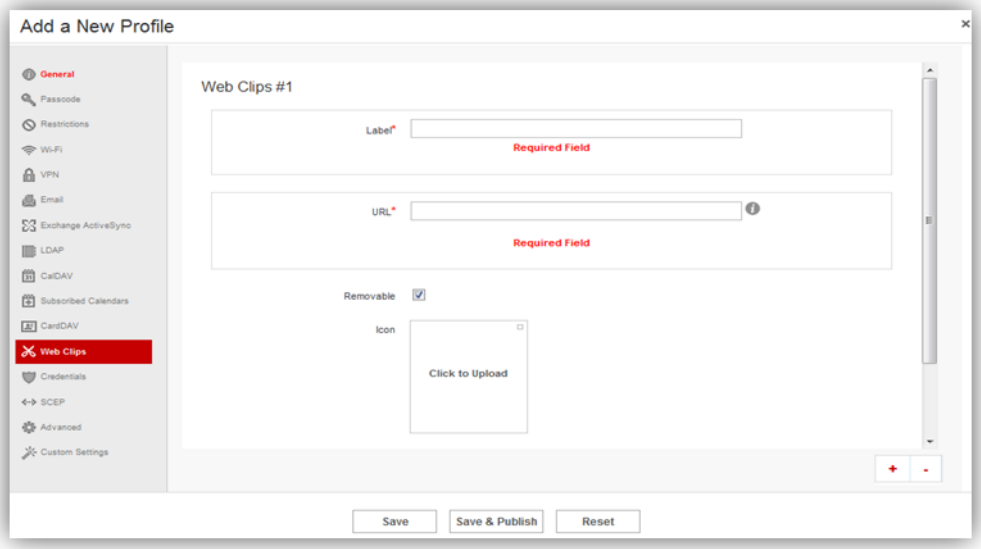
▶ Selectează **Adăugare**.

▶ Introdu în Informații profil de bază în Setări generale.

- Selectează platforma dispozitivului.
- **Numeș te** profilul. De exemplu: *Self-Service Portal Webclip pentru dispozitivele iOS*.
- Specifică grupurile de locație originale pentru a **gestiona** şi a **atribui** profilul.



- Selectează **Web Clip (iOS)** sau **Marcaj (Android)** de pe bara laterală din stânga.
- Introdu **Informațiile profilului.**



- **Eticheta** – Textul afişat sub pictograma Web clip pe dispozitivul unui utilizator final. De exemplu, Portalul Self Service Vodafone .
- **URL** – URL pe care îl afişează Web clip-ul.

1. Pentru portalul de Self-Service, folosiți următorul URL: **http://<Your Enrolment Environment>/mydevice/**.

- **Pictogramă** – Pentru a adăuga o pictogramă personalizată, selectează un fişier grafic în format .gif, .jpg, sau .png.
  - Pentru cele mai bune rezultate, oferă o imagine pătrată nu mai mare de 400 de pixeli pe fiecare parte şi mai puțin de 1 MB ca dimensiune atunci când este necomprimată. Grafica se scalează automat şi se ajustează pentru a se potrivi, dacă este necesar, şi se converteşte la formatul .png. Pictogramele Web Clip au 104 x 104 pixeli pentru dispozitivele cu un afişaj Retina sau 57 x 57 pixeli pentru alte dispozitive.

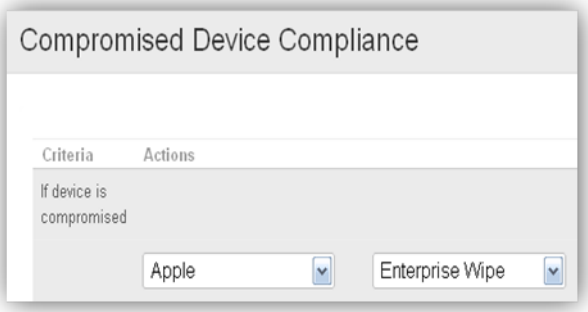
- După ce ai completat, dă click pe **Salvare şi Publicare** pentru a trimite imediat profilul la toate dispozitivele necesare.

Notă privind setările de confidențialitate: Accesul la informațiile şi acțiunile de la distanță din portalul Self-Service sunt determinate atât de setările de confidențialitate (**Configurare→Setări sistem→Dispozitiv→General→Confidențialitate**) şi setări Rol (**Utilizatori→ Conturi Admin**). Dacă mai multe setări sunt în vigoare, politica cea mai strictă se va aplica.

Retragerea dispozitivului

În cazul în care un dispozitiv trebuie să fie îndepărtat din gestionarea dispozitivelor mobile, există mai multe metode posibile pentru a şterge dispozitivul din diferite surse.

- **Ştergerea automată** – Motorul de conformitate Vodafone poate fi configurat astfel încât atunci când dispozitivele nu sunt conforme cu politicile privind **Aplicaţiile** sau **Dispozitivul** , acestea sunt automat şterse din gestionarea dispozitivelor.



- **Ştergerea administrativă** – Administratorii pot de asemenea şterge dispozitivele over the air din pagina **Bord Dispozitiv** sau pagina **Detalii dispozitiv**. Din oricare dintre aceste pagini, administratorii trebuie să selecteze **Ştergere corporativă** , iar dispozitivul este îndepărtat din gestionarea dispozitivelor mobile.

- **Ştergere utilizator final** – Dacă un utilizator final decide să renunțe la gestionarea dispozitivelor mobile, atunci el poate iniția procesul de ştergere din propriile dispozitive. Deşi procesul este diferit pentru fiecare platformă de gestionat, procesul general implică eliminarea privilegiilor administrative de către Vodafone, precum şi eliminarea oricăror agenți Vodafone din dispozitiv.

Cele mai bune practici

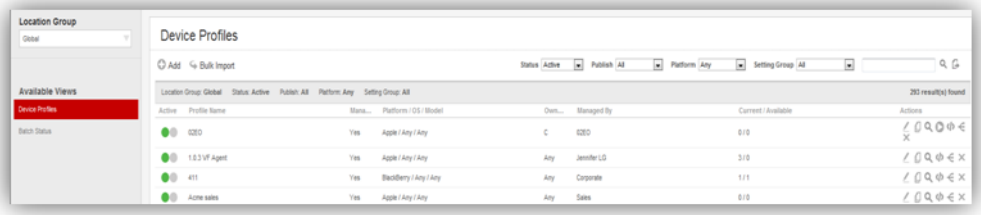
- Înainte de a efectua acțiuni de la distanță pe un dispozitiv, ia în considerare tipul de proprietate asupra dispozitivului.
  - De exemplu, ține cont de faptul că realizarea unei ştergeri complete a unui dispozitiv deținut de un angajat elimină toate datele personale din dispozitiv, pe lângă toate datele corporative.
- În plus, administratorul poate dori să utilizeze setările de confidențialitate (specificate în **Configurare→Setări sistem→ Dispozitiv →General →Confidențialitate**) şi permisiuni privind rolul (specificate în **Utilizatori→Conturi administrative→Roluri**) pentru a restricționa accesul lower-tier al administratorului la datele dispozitivului deținut de angajat.

4.0 Administrarea profilului

Vodafone permite administratorilor IT să creeze şi să implementeze **profiluri de configurare** care definesc **setări de companie**, **politici** şi **restricţii** pentru dispozitive smart, fără a necesita interacţiune cu utilizatorii. Vodafone furnizează profiluri **semnate**, **criptate** şi **blocate** over-the-air pentru a asigura faptul că nu sunt modificate, divizate sau eliminate. Un singur profil implementat este numit un profil **Payload.**

Pagina de profiluri

Pagina de **Profiluri ale dispozitivului** din Consola Admin VSDM este responsabilă pentru gestionarea şi crearea profilurilor.



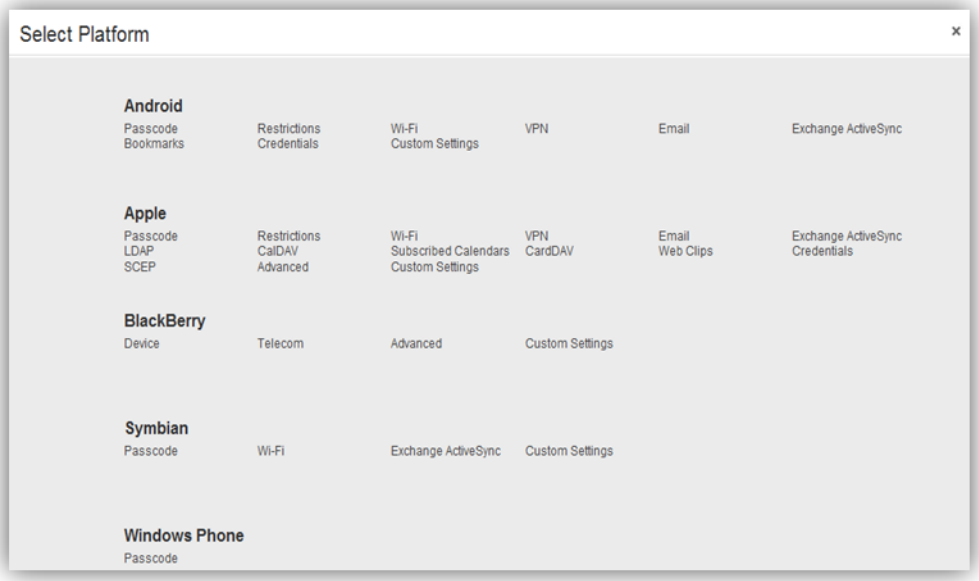
- **Bara de căutare**–Căutarea pentru un profil bazat pe atribute specifice.
- **Activ** – Dacă este verde/activ, profilul este disponibil pentru noile dispozitive. Dacă este roşu / inactiv, profilul nu este disponibil pentru dispozitive.
- **Gestionat** – Profilurile gestionate sunt asociate direct cu Vodafone, prin urmare, dacă un dispozitiv nu este înscris sau retras, profilele gestionate sunt eliminate. Profilurile negestionate rămân pe un dispozitiv chiar şi după ce au fost şterse din Vodafone.
- **Proprietate** – Arată dacă un profil este atribuit unui dispozitiv sau special pentru dispozitive deținute de corporații sau angajați.
- **Gestionat de** – Grupul de locație care are acces la editare, publicare sau ştergere a unui un profil.
- **Acțiuni** – Gestionarea unui profil utilizând următoarele opțiuni:
  - Editare Permite personalizarea unui profil existent.
  - Copiere Permite copierea unui profil existent cu un nou nume de profil.
  - Publicare Publică profilul în dispozitive care se potrivesc cu criteriile profilului.
  - Vizualizare XML Vizualizează codul XML transmis over the air spre dispozitive care descriu aplicația sau profilul.
  - Şterge profilul şi îl elimină din dispozitive.
  - Vizualizare dispozitive Afişează dispozitivele care sunt disponibile pentru acel profil şi, dacă profilul este instalat în prezent.

Crearea de profiluri

Pentru a implementa profilurile în dispozitive folosind **Pagina de profiluri a dispozitivului** în Consola VSDM Admin:

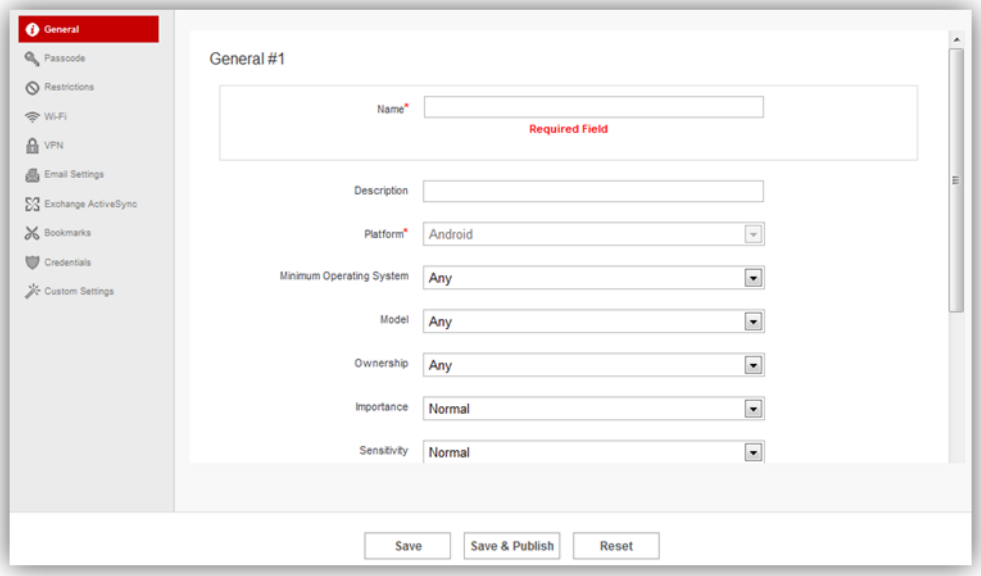
- Navighează la **Profiluri & Politici** →**Profiluri** pentru a deschide pagina de **Profiluri dispozitiv**.

- Selectează Add
- Alege Platforma pe care doreș ti să o asociezi cu profilul.



4.1.1 Setări generale

Primul pas în crearea oricărui profil este configurarea **Setărilor generale**. **Setări generale** reprezintă o modalitate de setare globală care determină cum şi cui îi este implementat profilul.



- **Nume** – Numele profilului ce va fi afişat în Consola de administrare VSDMT.
- **Descriere** – O scurtă descriere a ceea ce face profilul. Acestea sunt afişate pe dispozitive gestionate în cadrul **Detaliilor profilului**.
- **Platforma** – Platforma pentru implementarea profilului (acest câmp este pre-populat pe baza platformei selectate în pasul anterior). Asistența privind profilul variază în funcție de platformă, şi, prin urmare, alegerea platformei determină ce tipuri de profiluri pot fi utilizate.
- **Implementare**:
  - **Gestionat** înlătură profilul atunci când dispozitivul este înscris.
  - **Manual** lasă profilul instalat atunci când dispozitivul este înscris.
- **Model şi Sistem minim de operare** – Introdu modelele specifice şi sistemele de operare minime la care profilul este implementat. Profilul poate fi implementat numai în dispozitive care îndeplinesc parametrii specificați.

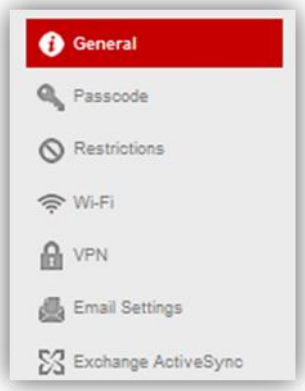
- **Proprietate** – Specificarea unui tip de proprietate (Corporativ-dedicat, Corporativ-divizat, sau Deținut de angajat), limitează implementarea profilului numai la dispozitivele care fac parte din grupul specificat de proprietate. Diferențierea între dispozitivele corporative şi cele deținute de angajat permite maxim de intimitate şi protecție.
- **Importanță şi Sensibilitate** – Acestea sunt domenii utilizate în Consola de administrare VSDM numai pentru detalii suplimentare şi capacități de filtrare a profilului. Ele nu au niciun efect asupra modului în care profilurile sunt implementate.
- **Permite eliminarea** – Un parametru de securitate care specifică ce pot face utilizatorii finali pentru a elimina profilul specific din dispozitivul lor:
  - **Întotdeauna** – Utilizatorii pot elimina profilul pe cont propriu, fără a introduce coduri de autorizare.
  - **Cu autorizare** – Utilizatorii îşi pot elimina profilul dacă introduc în mod corect un cod de autorizare aşa cum a fost creat de către un administrator de Consolă VSDM Admin.
  - **Niciodată** – Utilizatorii nu pot elimina profilul decât dacă dispozitivul este şters din Vodafone management.
- **Grup de locație original** – Grupul de locație cu care administratorii trebuie să fie asociați în scopul de a edita şi şterge acest profil. Dacă administratorii reuşesc să gestioneze grupuri de locație mai mari decât grupul de management, atunci ei pot avea, de asemenea, acces la gestionarea profilului prin moştenire.
- **Tip de atribuire** – Acesta determină modul în care profilul este trimis către dispozitive.
  - **Auto** – Trimite automat profilul la toate dispozitivele.
  - **Opțional** - Trimite manual profilul la dispozitivele selectate din grupurile de locație selectate în caseta de atribuiri.

Notă: Când un profil este setat la opțional, **niciun** dispozitiv nu-l poate primi în mod implicit. Acesta trebuie să fie atribuit manual **fiecărui** dispozitiv care are nevoie de el.

- **Grupul de locație**– Grupurile de locație (şi toate grupurile de locație copii) care sunt configurate cu acest profil. Orice dispozitive care se înscriu în aceste grupuri sau alte grupuri copii care primesc profilul.

Notă: Configurați întotdeauna la **Grupul de locație**.

Când Setările generale sunt complete, selectează oricare din tipurile de profil din lista din stânga pentru a începe crearea profilurilor.



4.1.2 Navigare

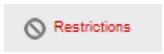
După ce Setările generale sunt configurate, poți începe crearea şi implementarea altor tipuri de profil. Aici sunt unele linii directoare generale pentru navigarea prin procesul de creare a profilului.

- Pentru a crea un profil nou, selectează tipul de profil din panoul de navigare din stânga şi dă click pe 

- Completează toate informațiile specifice ale profilului care sunt necesare.
  - Domeniile specifice utilizate pentru a configura fiecare dintre tipurile de profil specifice sunt prezentate în secțiunea de mai jos, numită Tipuri de profil.
- Odată ce ai terminat, selectează **Salvare, Salvare şi Publicare**, sau **Resetare** pentru a finaliza profilul.

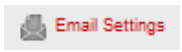
- **Salvarea profilului** salvează configurarea profilului în Consola VSDM Admin dar nu implementează profilul în dispozitive din cauza statutului **nepublicat**.
- **Salvarea şi publicarea profilului** salvează configurarea profilului în Consola VSDM Admin şi **publică** profilul pentru ca toate dispozitivele gestionate în mod corespunzător să primească imediat noul profil.
- **Resetare** nu salvează niciuna din configurațiile profilului şi şterge toate modificările.

Profilurile sunt listate în panoul de navigație **Adăugare Profil Nou** . Panoul de navigare oferă, de asemenea, un rezumat rapid al statutului profilului, utilizând următorii indicatori:

- Verde indică faptul că domeniile profilului din această categorie sunt complete.
  - Exemplu: 

- Gri indică faptul că niciun profil de acest tip nu a fost configurat.
  - Exemplu: 

- Roşu indică o eroare în câmpurile de informații ale profilului.
  - Exemplu: 

- Numerele de lângă numele profilului indică numărul de profiluri create pentru tipul de profil selectat.
  - Exemplu: 

Creați profiluri multiple de un tip

Gestionarea profilurilor de către Vodafone permite administratorului să configureze profiluri multiple pentru multe dintre categoriile profilelor (de exemplu, Wi-Fi, E-mail sau LDAP). Pentru a crea mai mult de un profil pentru un tip de profil:

- Dă click pe numele profilului pentru a deschide fereastra de editare profil (dacă este necesar, dă click pe **Configurare** pentru a adăuga profilul inițial).
- Pentru a adăuga un alt profil, dă click pe semnul plus (+). Pentru a şterge profilul selectat, dă click pe semnul minus (-).
- Pentru a derula profilurile, dă click pe săgeți. Sau, selectează o anumită pagină dând click pe cercul corespunzător. Imaginea exemplu de mai jos prezintă şase cercuri, fiecare reprezentând o pagină de profil:

Notă: Este important să facem diferența între crearea profilurilor multiple de un tip (de exemplu, diferite profiluri de E-mail), care este o practică recomandată, şi mai multe profiluri payloads (de exemplu, crearea unui profil Email şi Wi-Fi în acelaşi timp), care nu este o practică recomandată.

Capacitățile dispozitivului privind profilul

Capacitățile profilului variază în funcție de tipul dispozitivului. Tabelele de mai jos oferă o descriere pe scurt a opțiunilor profilului pentru dispozitiv / sistemul de operare:

4.1.3 Profiluri iOS

Nume profil	Descriere scurtă
Codul de acces	Profilurile cu cod de acces necesită ca utilizatorii finali să-şi protejeze dispozitivele cu coduri de acces de fiecare dată când se întorc din starea de inactivitate (idle). Acest lucru asigură protecția tuturor informațiilor corporative pe dispozitivele gestionate. În cazul în care mai multe profiluri necesită politici separate a codurilor de acces, poate intra în vigoare politica cea mai restrictivă.
Restricții	Profilurile cu restricții limitează caracteristicile disponibile utilizatorilor de dispozitive gestionate prin restricționarea anumitor caracteristici, cum ar fi YouTube, iTunes Store sau aparatul foto de pe dispozitiv.
Wi-Fi	Profilurile Wi-Fi trimit setările corporative Wi-Fi direct la dispozitivele gestionate pentru acces instantaneu. Rețineți opțiunile pentru iOS 5+.
VPN	Profilurile VPN trimit setările private virtuale corporative la dispozitivele corporative, astfel încât utilizatorii să poată accesa în siguranță infrastructura companiei din locații de la distanță.
Email	Permite administratorului să configureze conturile de e-mail IMAP/POP3.
Exchange ActiveSync	Profilurile de tip Exchange ActiveSync permit utilizatorilor finali să acceseze infrastructura corporativă privind emailul. Vă rugăm să rețineți că acestea sunt domenii de căutare şi opțiuni care se aplică numai la iOS 5 +.
LDAP	LDAP permite configurarea cu informații despre director LDAPv3. Câmpurile din această secțiune acceptă valori de căutare. Dați click pe pictogramă pentru valori şi definiții.
CalDAV	CalDAV oferă opțiuni de configurare pentru a permite utilizatorilor finali să se sincronizeze wireless cu serverul de companie CalDAV. Câmpurile din această secțiune acceptă valori de căutare. Dați click pe pictogramă pentru definiții.
Calendare subscrise	Calendare subscrise oferă configurarea calendarelor. Câmpurile din această secțiune acceptă valori de căutare. Faceți clic pe vârful instrumentului pentru definiții.
CardDAV	CardDAV - Această secțiune permite configurarea specifică a serviciilor CardDav. Câmpurile din această secțiune acceptă valori de căutare. Dați click pe pictogramă pentru definiții.
Clipuri web	Profilurile cu Clipuri Web trimit hyperlink-uri care se pot accesa către dispozitive sub unei pictograme pentru a oferi acces rapid la resurse web comune (de exemplu, ați putea adăuga versiunea online a ghidului de utilizare iPhone la ecranul de întâmpinare)
Informații de acces	Profilurile pe bază de informații de acces (acreditări) implementează certificate corporative la dispozitivele gestionate. Dacă rețeaua acceptă, şi cererile ad-hoc de certificat pot fi configurate.
SCEP	Sarcina utilă SCEP specifică setări care permit dispozitivului să obțină certificate de la un CA care foloseşte un protocol de tip Simple Certificate Enrollment Protocol (SCEP).
Setări avansate	Profilurile avansate permit o configurare avansată a punctului de acces.
Setări personalizate	Setările personalizate permit ca profilul XML particularizat să fie inclus în sarcina utilă a profilului.

4.1.4 Profiluri Android

Nume profil	Descriere profil
Codul de acces	Profilurile cu cod de acces necesită ca utilizatorii finali să-şi protejeze dispozitivele cu coduri de acces de fiecare dată când se întorc din starea de inactivitate (idle). Acest lucru asigură protecția tuturor informațiilor corporative pe dispozitivele gestionate. În cazul în care mai multe profiluri necesită politici separate a codurilor de acces, poate intra în vigoare politica cea mai restrictivă.
Restricții	Restricțiile sunt disponibile pentru telefoanele Samsung ce rulează Cream Sandwich. Aceste restricții includ funcționalitatea dispozitivului, restricții de sincronizare şi stocare, Bluetooth, Roaming şi restricții de conectare a modemului.
Wi-Fi	Profilurile Wi-Fi trimit setările corporative Wi-Fi direct la dispozitivele gestionate pentru acces instantaneu.
VPN	Profilurile VPN trimit setările private virtuale corporative la dispozitivele corporative, astfel încât utilizatorii să poată accesa în siguranță infrastructura companiei din locații de la distanță.
Setări de Email	Profilurile de e-mail trimit configurații de e-mail direct la dispozitive, astfel că utilizatorii finali primesc în mod automat un e-mail.
Exchange ActiveSync	Profilurile de tip Exchange ActiveSync permit utilizatorilor finali să acceseze infrastructura email corporativă. Schimbul se poate seta acum cu clientul de mail nativ pe dispozitive Samsung folosind sistemul de operare Cream Sandwich.
Marcaje	Profilurile cu marcaje funcționează în acelaşi mod ca şi profilurile Webclip. Marcajele sunt scurtături personalizate Web care sunt trimise până la Ecranul de întâmpinare al dispozitivului utilizatorului. Marcaje multiple pot fi adăugate la profil, dând click pe semnul plus (+), în colțul din dreapta sus al ferestrei.
Informații de acces	Profilurile pe bază de informații de acces (acreditări) implementează certificate corporative la dispozitivele gestionate. Dacă rețeaua acceptă, şi cererile ad-hoc de certificat pot fi configurate. Marcaje multiple pot fi adăugate la profil, dând click pe semnul plus (+), în colțul din dreapta sus al ferestrei.

4.1.5 Profiluri BlackBerry

Nume profil	Descriere profil
Dispozitivul	Profilurile dispozitivelor determină diverse opțiuni specifice dispozitivului precum cum luminozitatea, iluminarea de fundal, eşantionarea GPS şi intervale de eşantionare GPS.
Telecom	Profilurile Telecom specifică diverse opțiuni de telecomunicații precum redirecționări 411 şi opțiuni de eşantionare SMS-uri.
Setări avansate	Setări avansate permite configurarea particularizată a Jurnalelor BlackBerry.
Setări personalizate	Setările personalizate permit ca XML particularizat să fie inclus în sarcina utilă a profilului.

4.1.6 Profiluri Symbian

Nume profil	Descriere profil
Codul de acces	Profilurile cu cod de acces necesită ca utilizatorii finali să-şi protejeze dispozitivele cu coduri de acces de fiecare dată când se întorc din starea de inactivitate (idle). Acest lucru asigură protecția tuturor informațiilor corporative pe dispozitivele gestionate. Acest profil permite o resetare a codului de acces setat de un administrator.
Wi-Fi	Profilurile Wi-Fi trimit setările corporative Wi-Fi direct la dispozitivele gestionate pentru acces instantaneu.
Exchange ActiveSync	Administratorul are posibilitatea de a stabili frecvența de sincronizare a calendarului şi e-mailurilor pe un dispozitiv mobil folosind profilurile de schimb Microsoft Exchange EAS.
Setări personalizate	Setările personalizate permit ca profilul XML particularizat să fie inclus în sarcina utilă a profilului.

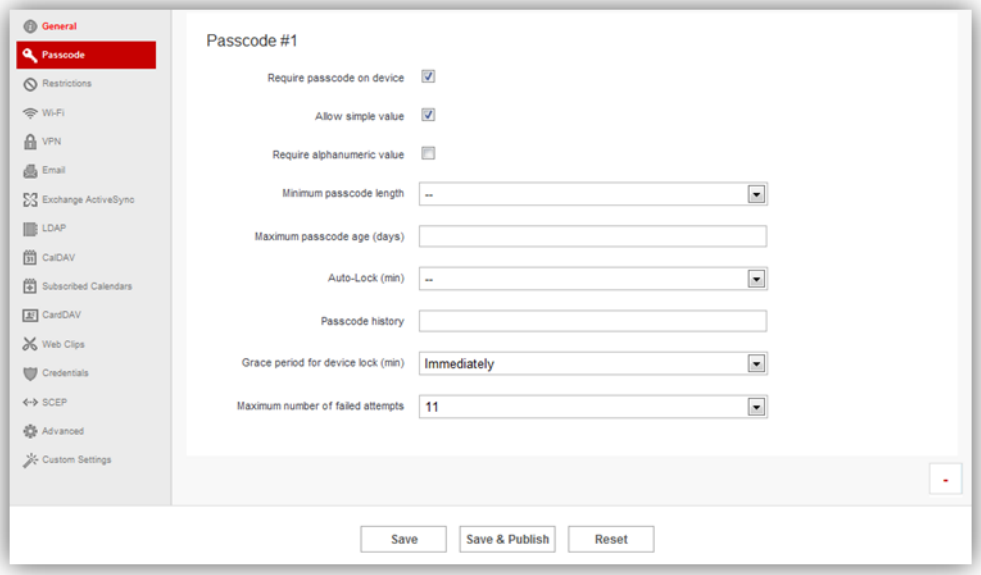
4.1.7 Telefonul Windows

Nume profil	Descriere profil
Codul de acces	Profilurile cu cod de acces necesită ca utilizatorii finali să-şi protejeze dispozitivele cu coduri de acces de fiecare dată când se întorc din starea de inactivitate (idle). Acest lucru asigură protecția tuturor informațiilor corporative pe dispozitivele gestionate.

Descriere profil

4.1.8 Codul de acces

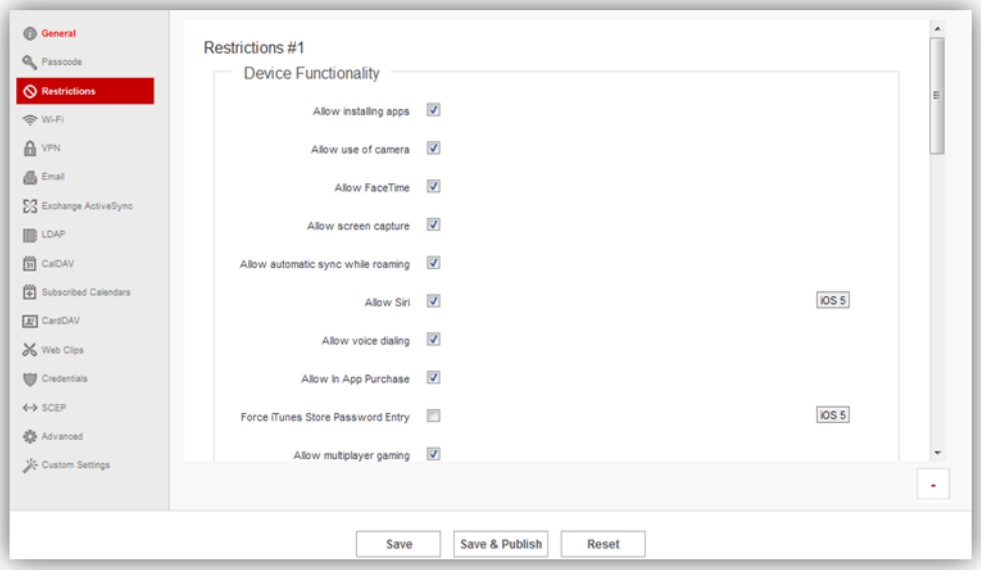
Profilurile cu cod de acces permit utilizatorilor finali să-şi protejeze dispozitivele cu un cod de acces. În cazul în care mai multe profiluri necesită politici separate a codurilor de acces, poate intra în vigoare politica cea mai restrictivă.



- **Solicitare cod de acces pe dispozitiv** – Obligă utilizatorul să seteze un cod de acces pe dispozitiv.
- **Permite valoare simplă** – Permite valori “simple” privind parola (de exemplu, “1111” sau “1234”)
- **Necesită valoare alfanumerică** – Necesită un cod de acces, cu litere şi cifre
- **Lungime minimă a codului de acces** – Setează o lungime minimă necesară parolei
- **Durata maximă (în zile) a codului de acces** – Setează numărul de zile până la expirarea parolei.
- **Auto-Blocare (min)** – Setează limita pentru blocarea automată a dispozitivului şi solicită introducerea unui cod de acces
- **Istoria codului de acces**– Setează numărul parolelor anterioare care nu pot fi folosite
- **Perioada de grație pentru blocarea dispozitivului (min)** – Perioada de timp după blocarea dispozitivului în care nu este solicitată re-introducerea codului de acces
- **Numărul maxim de încercări eşuate** –Numărul de tentative eşuate de introducere a codului de acces înainte ca dispozitivul să fie şters

4.1.9 Restricții

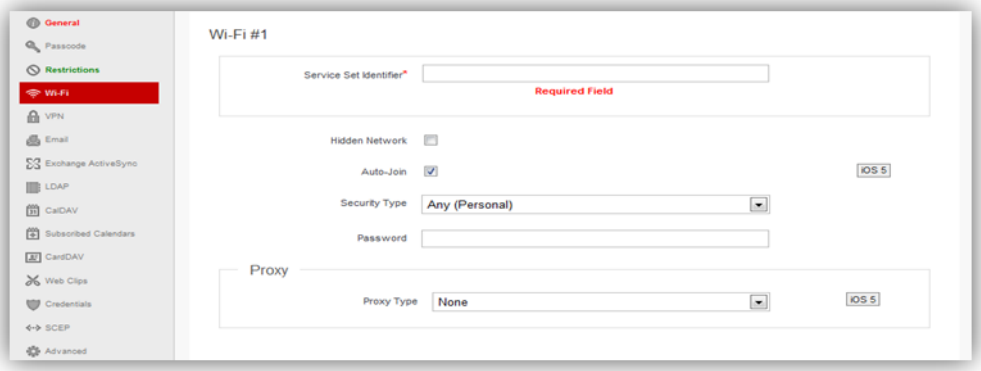
Profilurile cu restricții (disponibile numai pentru iOS şi Android) limitează caracteristicile disponibile utilizatorilor de dispozitive gestionate prin restricționarea anumitor caracteristici, cum ar fi YouTube, iTunes Store sau aparatul foto de pe dispozitiv.



- **Funcționalitate dispozitiv** –Stabileşte ce funcții poate efectua utilizatorul unui dispozitiv.
- **Aplicații** –Determină ce aplicații poate accesa utilizatorul unui dispozitiv.
- **Evaluări** –Restricționează accesul la filme, emisiuni TV şi aplicații bazate pe evaluări specifice.

4.1.10 Wi-Fi

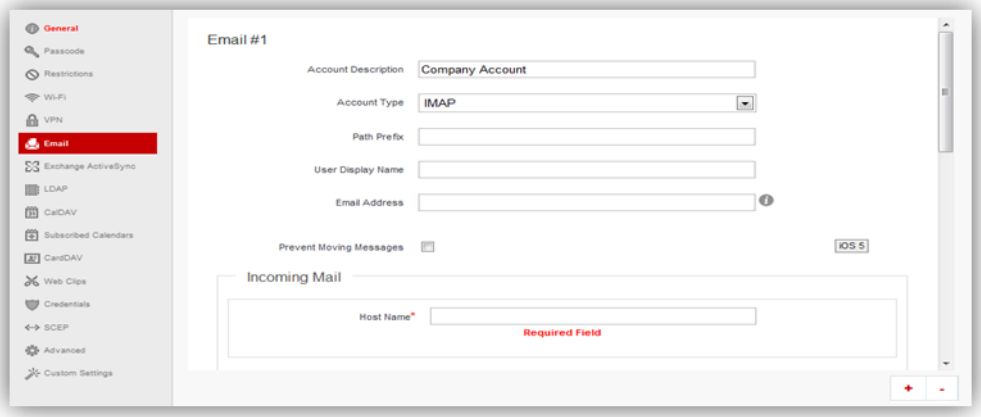
Profilurile Wi-Fi trimit setările corporative Wi-Fi direct la dispozitivele gestionate pentru acces instantaneu.



- **Identificator set service** –Pentru a configura profilurile Wi-Fi, selectați protocoalele wireless adecvate şi setări de securitate pentru rețeaua Wi-Fi.
- **Proxy** – Permite administratorului să configureze un server proxy.
- Adăugați conturi multiple dând click pe semnul (+), sau creați profiluri Wi-Fi în grup prin navigarea la **Profiluri şi Politici→Profiluri→ Import în grup**.

4.1.11 Email

Profilurile de **Email** permit administratorului să configureze conturile de e-mail IMAP/POP3 pentru mail-urile care intră şi ies.

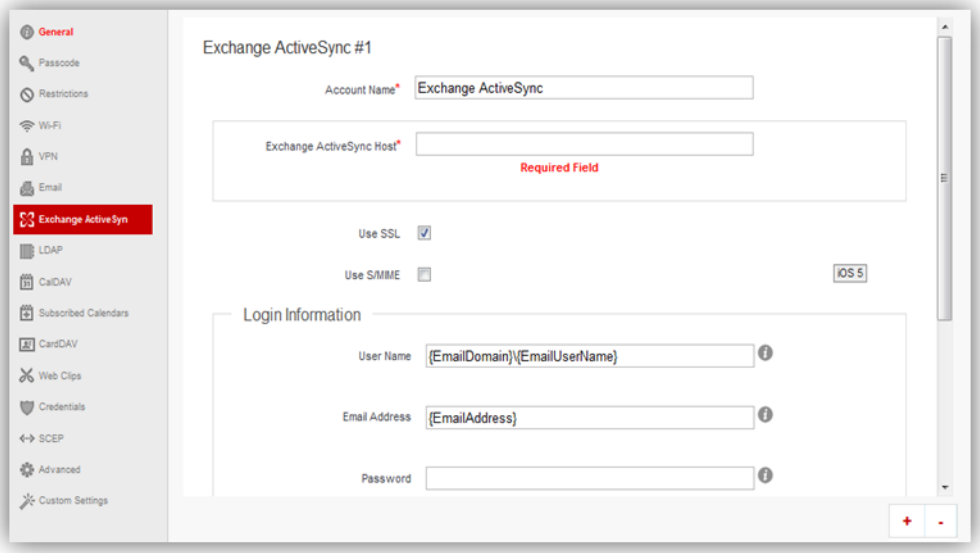


- Adaugă conturi multiple dând click pe semnul plus (+).

Notă: Anumite caracteristici ale profilelor privind emailul sunt disponibile numai pentru dispozitivele iOS.

4.1.12 Exchange ActiveSync

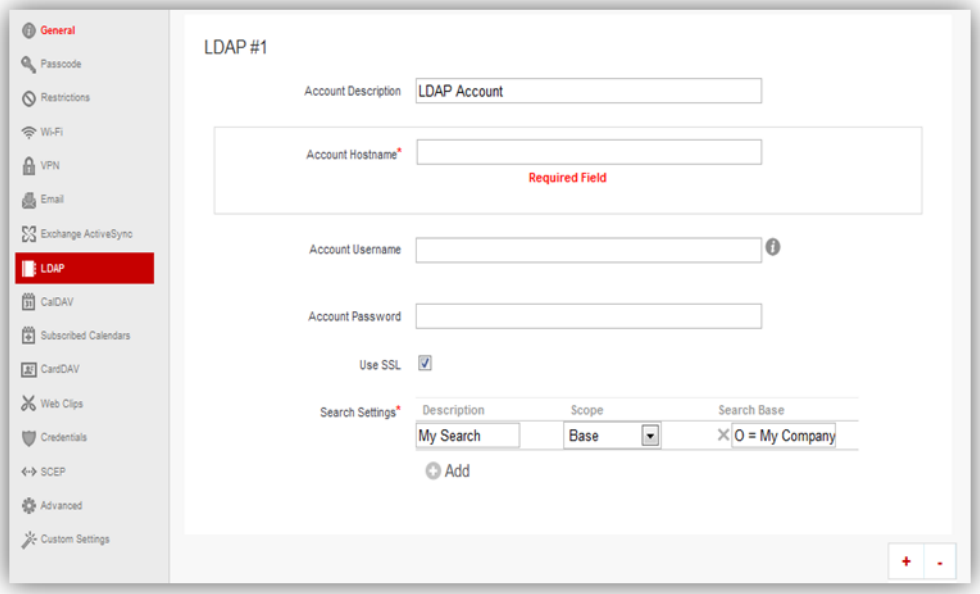
Profilurile de tip Exchange ActiveSync permit utilizatorilor finali să acceseze infrastructura automată corporativă privind emailul.



- Crearea unui profil pentru un anumit utilizator specificând numele domeniului, numele de utilizator, adresa de e-mail şi parola. Sau, lasă necompletat câmpul pentru parolă şi utilizatorilor li se va cere parola (pentru această configurație, câmpul pentru numele de utilizator necesită o **valoare de căutare**).
- Dacă certificatele sunt utilizate pentru a valida conexiunea ActiveSync şi doreş ti să le incluzi în profil, selectează una din cele două opțiuni enumerate în conformitate cu **Tipul certificatului.**
- **Certificat încărcat** –Încarcă un certificat şi include o frază de acces pe care utilizatorul trebuie să o introducă înainte de a primi certificatul.
- **Autoritate certificată** –Specifică autoritatea certificată în existență pe rețeaua locală ca sursă a certificatului.
- Configurează mai multe conturi de schimb, dând click pe **Adăugare** (+) .

4.1.13 LDAP

LDAP permite configurarea uşoară cu informaţii despre directorul LDAPv3.

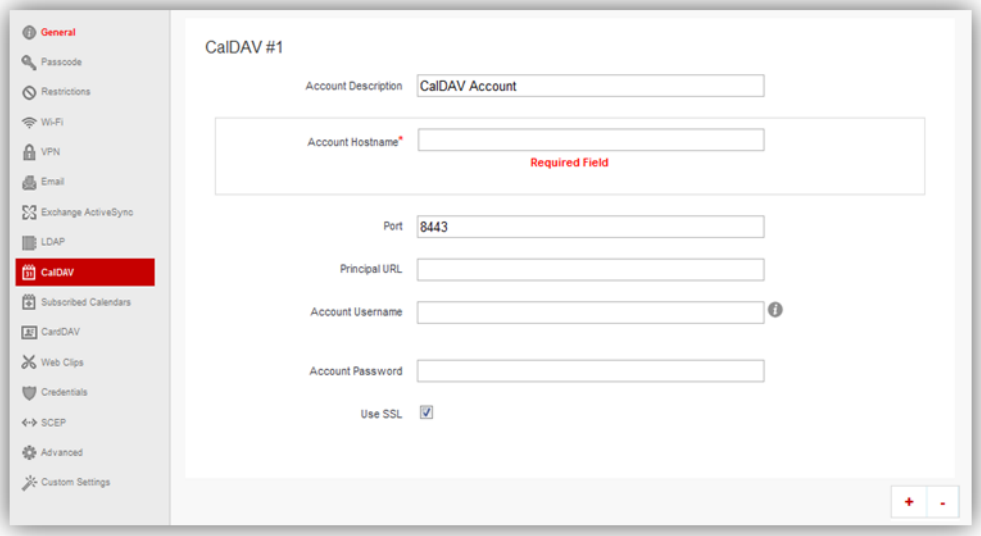


Câmpurile din această secţiune acceptă valori de căutare. Dă click pe pictogramă pentru valori şi definiţii.

Adaugi conturi multiple dând click pe semnul plus (+). Consultă secţiunea integrarea LDAP pentru mai multe informaţii privind LDAP.

4.1.14 CalDAV

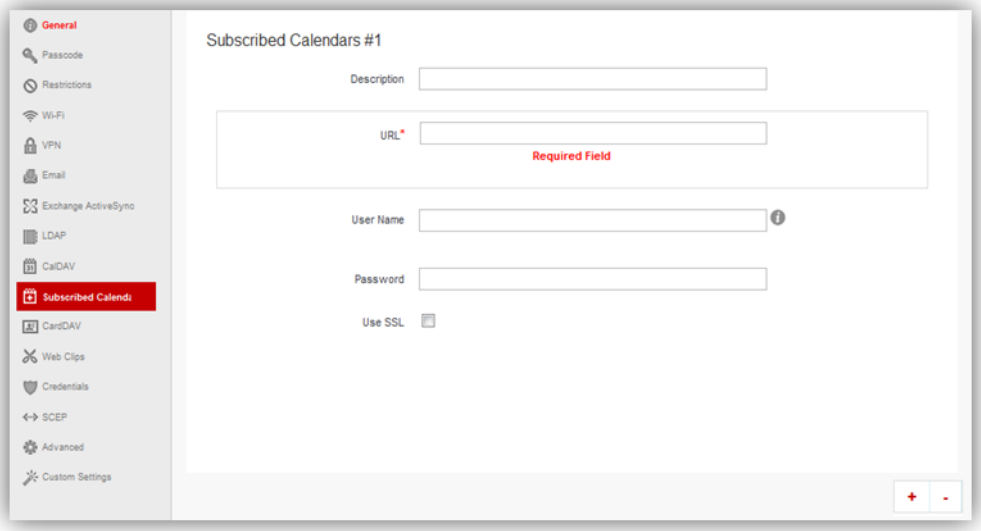
Profilurile CalDAV pot fi configurate cu informaţii pentru a permite utilizatorilor să sincronizeze wireless cu serverul de companie CalDAV.



▶ Câmpurile din această secţiune acceptă valori de căutare. Dă click pe pictogramă pentru definiţii.

4.1.15 Calendare abonate

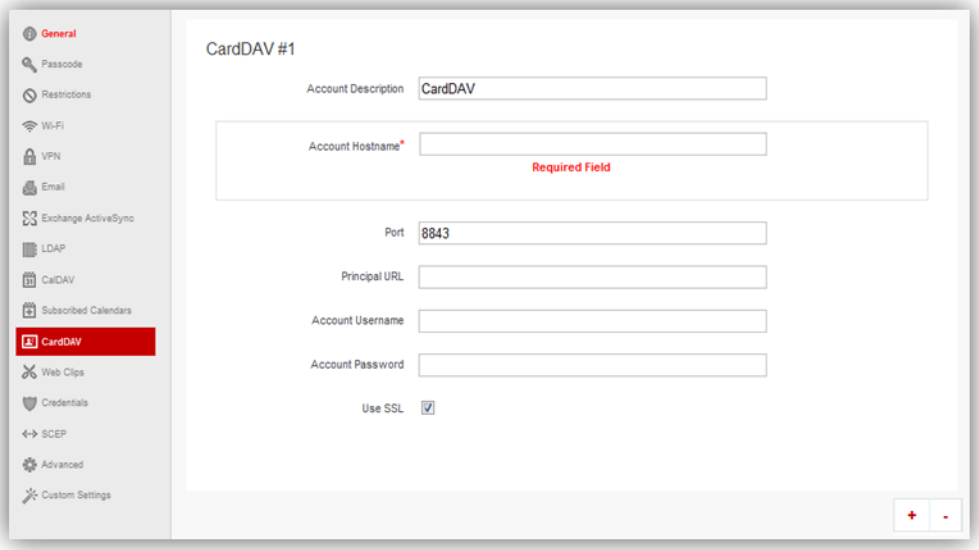
Calendare abonate gestionează integrarea şi abonamentele calendarului corporativ.



- Câmpurile din această secțiune acceptă valori de căutare. Dă click pe pictogramă pentru definiții.

4.1.16 CardDAV

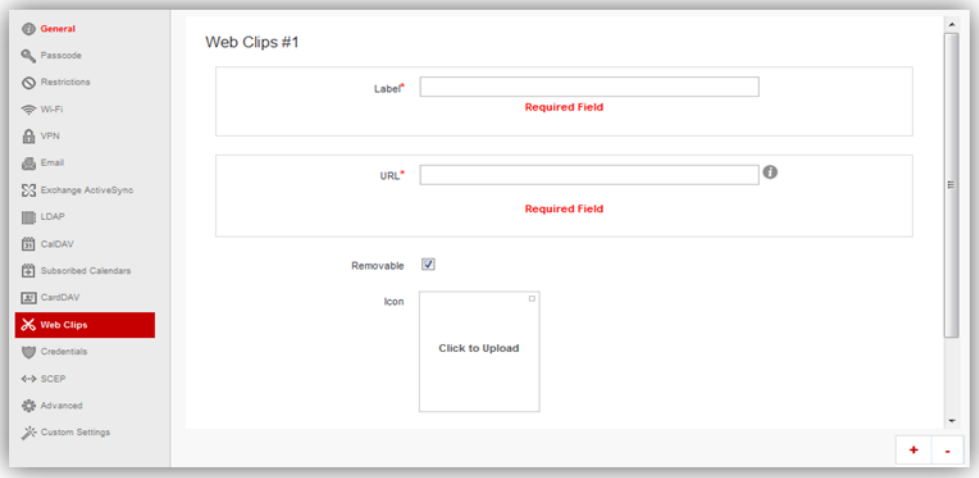
CardDAV permite administratorului să configureze servicii specifice CardDav.



- Câmpurile din această secțiune acceptă valori de căutare. Dă click pe pictogramă pentru definiții.

4.1.17 Clipuri web

Profilurile cu Clipuri Web trimit către dispozitive hyperlink-uri care se pot accesa sub forma unei pictograme pentru a oferi acces rapid la resurse web comune (de exemplu, pentru a adăuga versiunea online a ghidului de utilizare iPhone la ecranul de întâmpinare) http://help.apple.com/iphone/). Clipurile web sunt folosite şi pentru a implementa catalogul de aplicații Vodafone şi a activa portalul de Self-Service.

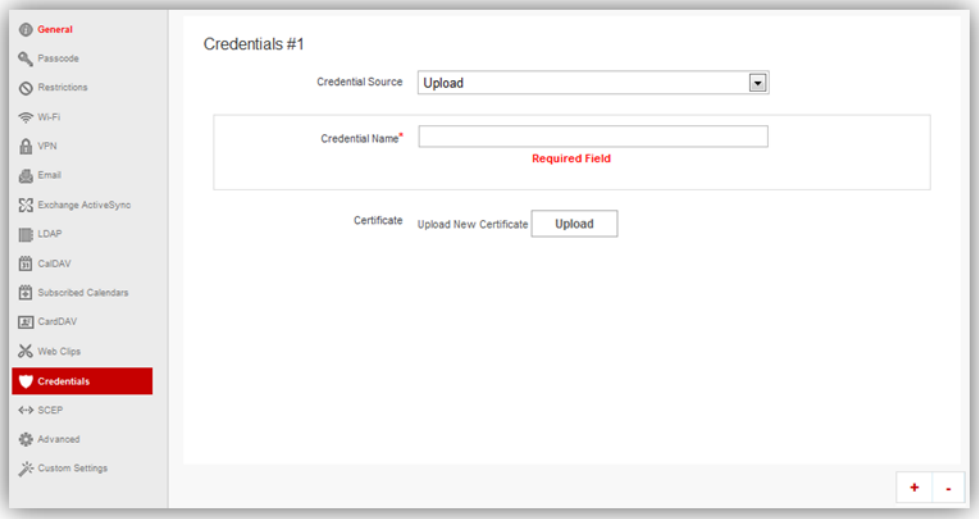


- **Eticheta** este numele care apare pe ecran.
- **URL-ul** este adresa la care utilizatorul este redirecționat către pe dispozitiv (poate fi intern sau extern).
- **Eliminabil** specifică dacă utilizatorul are sau nu capacitatea de a elimina web clipul din dispozitiv.
- **Pictogramă** – Pentru a adăuga o pictogramă personalizată, selectează un fişier grafic în format .gif, .jpg, sau .png.

- Pentru cele mai bune rezultate, furnizează o imagine pătrată nu mai mare de 400 de pixeli pe fiecare parte şi mai puțin de 1 MB ca dimensiune atunci când este necomprimată. Grafica se scalează automat şi se ajustează pentru a se potrivi, dacă este necesar, convertindu-se la formatul .png. Pictogramele Web Clip au 104 x 104 pixeli pentru dispozitivele cu un afişaj Retina sau 57 x 57 pixeli pentru alte dispozitive.
  - **Pictogramă pre-compusă** –Bifarea acestei casete împiedică dispozitivul să adauge o imagine strălucitoare la pictogramă.
  - **Ecran total** specifică faptul că adresa este încărcată pe tot ecranul pe dispozitiv, fără bara de adrese şi marginile Safari.
  - Adaugă multiple Clipuri web dând click pe semnul plus (+).

4.1.18 Informații de acces

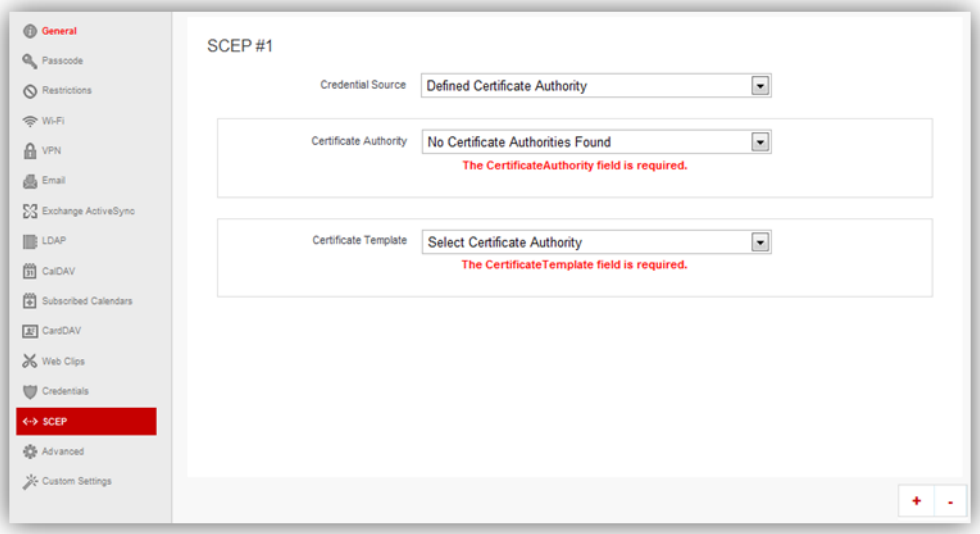
Profilurile pe bază de informații de acces (acreditări) implementează certificate corporative în dispozitivele gestionate.



- Profilul pe bază de informații de acces oferă, de asemenea, un domeniu pentru configurarea ad-hoc a cererilor de certificat (dacă sunt acceptate de rețea).
- Adaugă multiple configurări privind acreditările dând click pe semnul plus (+).

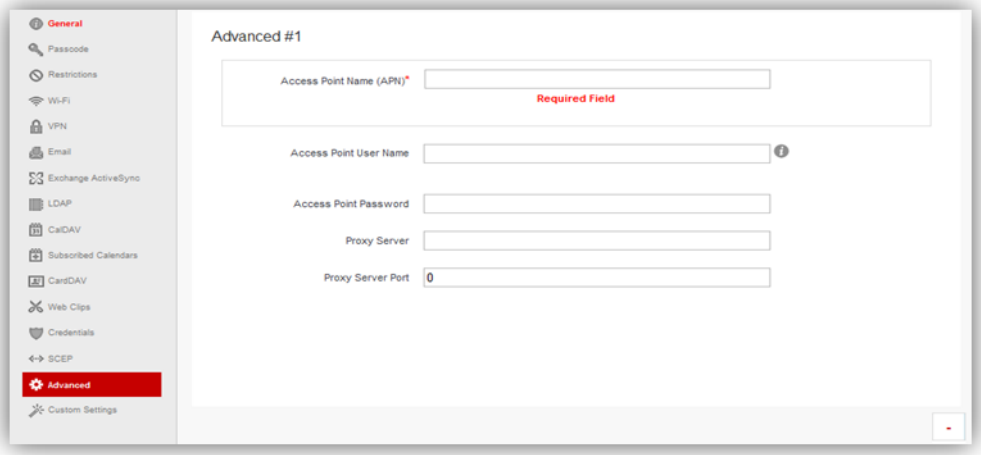
4.1.19 SCEP

Sarcina utilă SCEP specifică setări care permit dispozitivului să obțină certificate de la o autoritate certificată folosind un protocol de tip **Simple Certificate Enrolment Protocol** (SCEP).



- Pentru mai multe informații cu privire la utilizarea şi integrarea certificatului, consultă secțiunea Integrarea infrastructurii certificatului.

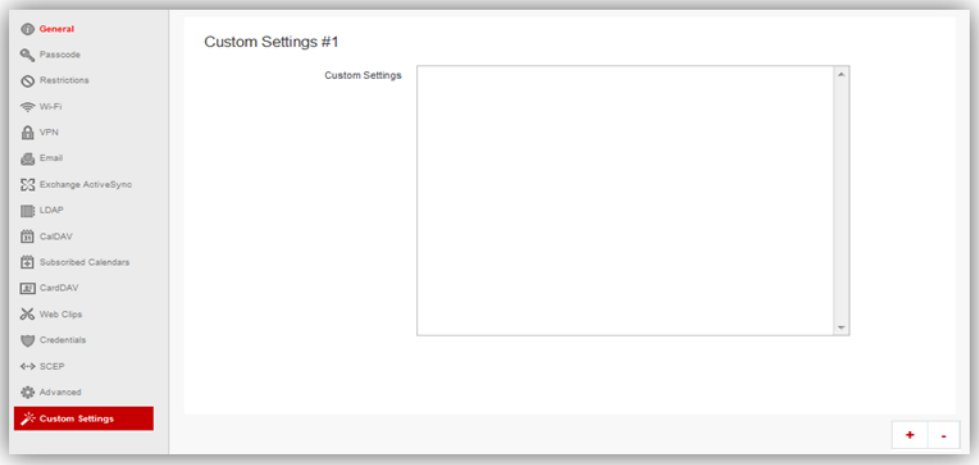
4.1.20 Setări avansate



- Profilurile avansate permit o configurare avansată a **Punctului de acces**.

4.1.21 Setări personalizate

Setările personalizate permit ca profilurile XML particularizate să fie incluse în sarcina utilă a profilului.



- Profilurile cu setări personalizate permit administratorilor să introducă direct codul XML utilizat la dispozitivele iOS, pe aer, cod care defineşte setările unui profil cu configurări în cazul în capabilitățile platformei dispozitivului sunt eliberate înainte de actualizarea capabilităților profilului VSDM.

- Profilurile personalizate se deschid şi se închid întotdeauna cu tag-urile <dict> şi conțin cel puțin, următoarele taste ale profilului:

- **PayloadDisplayName** – Opțional. Numele profilului ce va fi utilizat în dispozitiv.
- **PayloadDescription** – Opțional. Descrierea profilului ce va fi implementată în dispozitiv.
- **PayloadVersion** – Versiunea sarcinii utile pentru a vă conecta la actualizări şi modificări.
- **PayloadIdentifier** – Un identificator revers în format DNS care este unic pentru această sarcină utilă specifică.
- **PayloadUUID** – Un identificator unic global pentru sarcina utilă.
- **PayloadOrganization** – Opțional. Organizația care a implementat sarcina utilă a profilului.

- **PayloadType** – Tipul de sarcină utilă care va fi configurată. De exemplu, aceasta defineşte dacă sarcina utilă trebuie să fie o sarcină utilă cu cod de trecere, o sarcină Wi-Fi sau una cu restricţii.
  - Un exemplu al modului în care aceste taste sunt implementate în profilul personalizat este prezentat mai jos.

```
<dict>
<key>PayloadDescription</key>
<string>Configures 15-min autolock for iPads</string>
<key>PayloadDisplayName</key>
<string>15min AutoLock</string>
<key>PayloadIdentifier</key>
<string>com.autolock.fifteenmin.passcode1</string>
<key>PayloadOrganization</key>
<string></string>
<key>PayloadType</key>
<string>com.apple.mobiledevice.passwordpolicy</string>
<key>PayloadUUID</key>
<string>AA3C17A5-5C62-4295-BE30-920405D53F9D</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
```

  - Apoi, imediat ce un **Tip de sarcină utilă** este definită, administratorii trebuie să definească tastele specifice pentru a defini setările pentru tipul specific al profilului. Acestea sunt toate dependente de tipul de sarcină utilă pe care administratorul încearcă să o implementeze. Pentru dispozitivele iOS, o listă a tuturor tastelor de proprietate specifice disponibile poate fi găsită aici: http://developer.apple.com/library/ios/#featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html
  - Odată ce aceste domenii ale sarcinii utile specifice sunt definite, profilul este gata de implementare. Un profil personalizat finalizat este afişat de mai jos pentru a activa caracteristici de auto-blocare pentru 15 minute pentru profilul iPad pe bază de cod de acces.

```
<dict>
<key>PayloadDescription</key>
<string>Configures 15-min autolock for iPads</string>
<key>PayloadDisplayName</key>
<string>15min AutoLock</string>
<key>PayloadIdentifier</key>
<string>com.autolock.fifteenmin.passcode1</string>
<key>PayloadOrganization</key>
<string></string>
<key>PayloadType</key>
<string>com.apple.mobiledevice.passwordpolicy</string>
<key>PayloadUUID</key>
<string>AA3C17A5-5C62-4295-BE30-920405D53F9D</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>forcePIN</key>
<true/>
<key>maxInactivity</key>
<integer>15</integer>
</dict>
```

Crearea profilurilor Wi-Fi în grup

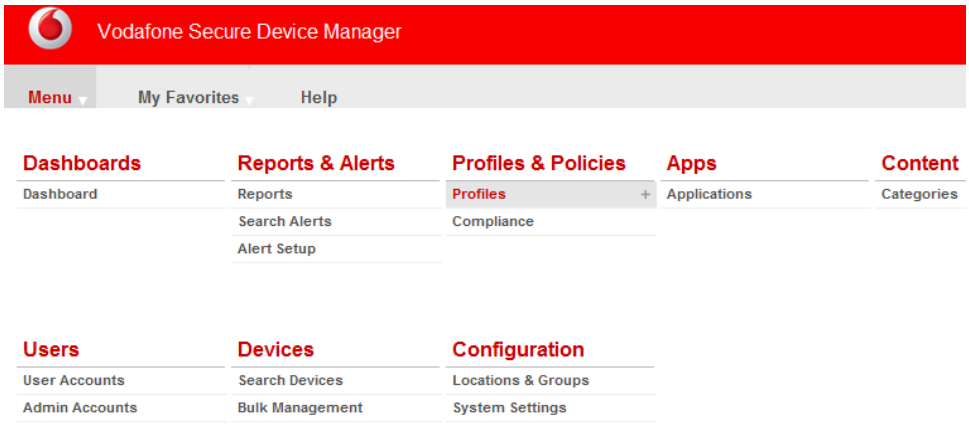
Crearea profilurilor Wi-Fi în grup permite administratorului să publice profilele Wi-Fi ale utilizatorilor în funcție de categoria lor de amplasare. Caracteristica de creare în grup oferă aceleaşi setări de configurare Wi-Fi ca şi un singur profil Wi-Fi, cu excepția faptului că configurează simultan mai multe profiluri pe Grupurile de locație. Pe lângă crearea de noi profiluri în grup, caracteristica de încărcare în grup permite administratorului să efectueze următoarele sarcini:

- Modificarea Grupului de locație pentru profil Wi-Fi existent.
- Editarea profilurilor Wi-Fi existente
- Gestionarea setărilor parolei în grup

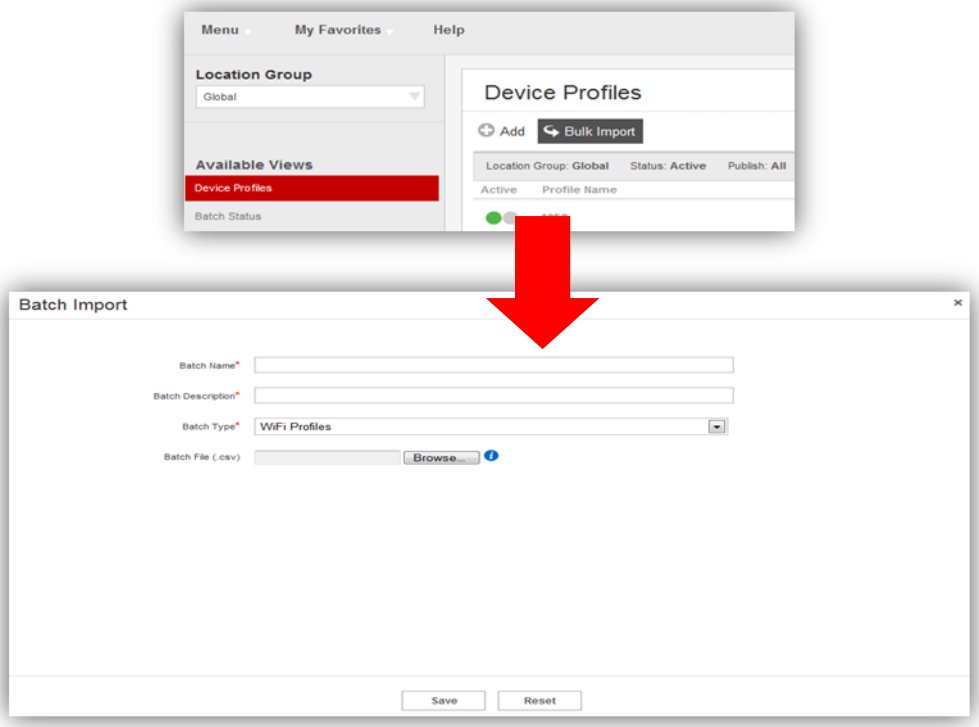
4.1.22 Crearea profilurilor Wi-Fi în grup

Pentru crearea profilurilor Wi-Fi în grup:

- Navighează la **Profiluri & Politici→ Profiluri**.



- Dă click pe **Import în grup** pentru a deschide Formularul de Import în Grup.



▶ Completează informațiile de bază:

- **Nume grup** - Numele utilizatorului sau grupului dispozitivului (pentru referință în Consola VSDM Admin).
- **Descriere grup**- O descriere a utilizatorului /sau grupului dispozitivului (pentru referință).
- **Tip grup**–Selectează **Profiluri Wi-Fi** din meniu.

▶ Dă click pe pentru a deschide **Formularul de import în grup**:

▶ De aici, selectează Descărcare şablon pentru a descărca Şablonul de import al grupului.

▶ Dă click pe **Deschide** pentru a deschide şablonul.

▶ Introdu toate informațiile relevante pentru profilul Wi-Fi pentru fiecare grup (definit pe Grup de locație) Trei utilizatori pentru eşantionare au fost adăugați în partea de sus a şablonului ca referință pentru tipul de informații ce trebuie introduse în fiecare coloană. Câmpurile obligatorii sunt desemnate cu un asterisc (*).

Notă:

- Coloana A, **Folosește caz**, se referă la tipul profilului (Adăugare, Editare sau Modificare)
  - ▶ **Modificare** permite administratorului să modifice Modelul (dispozitivul) şi domeniile atribuite Grupului de locație pentru un profil existent.
  - ▶ **Adăugare** creează un nou profil.
  - ▶ **Editare** permite administratorului să editeze un profil existent (creează o nouă configurare Wi-Fi).
- Coloana E, **Grupul de locație,** specifică permisiunile grupului de locație pentru editarea profilului Wi-Fi. Fiecare administrator plasat cu un nivel mai sus decât acest grup de locație (şi mai sus) poate edita profilul Wi-Fi desemnat.
- Coloana F, **Grup de locație atribuit,** desemnează Grupul de locație în care profilul este implementat.

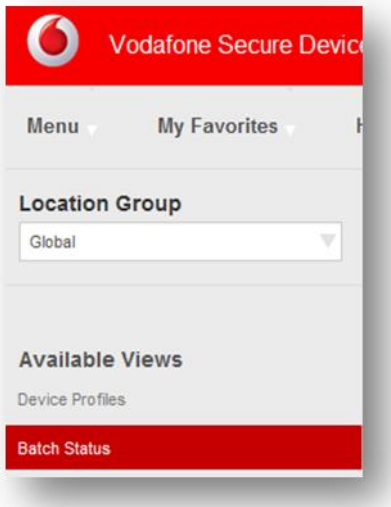
▶ Odată ce ai terminat, salvează şablonul ca un fişier **.csv**.

▶ Selectează **Caută** din **Import grup Formular,** şi selectează fişierul **.csv** care tocmai a fost creat din şablon.

▶ Când ai terminat, dă click pe **Salvare**.

Gestionarea profilurilor Wi-Fi în grup

Vizualizați statutul importurilor de profile în grup selectând **Statut grup** din **Ecrane disponibile** de pe pagina **Profiluri**.



Acest ecran afişează datele grupurilor de profiluri, inclusiv:

▶ Statut grup

- **Finalizat** indică faptul că importul grupului a fost finalizat cu succes.
- **Eroare** indică o problemă cu importul grupului.

▶ Dă click pe eroare ⚠ din coloana "Acțiune" pentru a vizualiza detaliile erorii.

▶ Acțiune

- Gol indică faptul că nicio acțiune nu este în curs.
- O eroare ⚠ indică faptul că importul grupului nu s-a finalizat.

▶ Dă click pe pictogramă pentru a vedea erorile în funcție de numărul rândului şi descrierea erorii.

Cele mai bune practici

Următoarele sfaturi vor ajuta administratorii să gestioneze mai eficient grupul de dispozitive smart prin intermediul instrumentelor de gestionare a profilului din VSDM:

- Fii atent la tipul de proprietate al dispozitivului (Corporativ-dedicat, Corporativ-divizat sau Deținut de angajat), atunci când specifici Setările generale ale profilului.
  - De exemplu, administratorul poate dori să implementeze profiluri cu restricții mai severe pentru dispozitivele corporative decât cele deținute de angajați.
- Atribuirile profilurilor se modifică odată cu cele ale grupului de locație.
  - De exemplu, dacă muți un utilizator într-un grup de locație nou, profilurile asociate cu grupul de locație original sunt eliminate iar utilizatorul moşteneşte profilurile asociate cu noul grup de locație.
- Pentru securitatea maximă a Emailului, foloseș te profilurile de Email în conjuncție cu Vodafone Secure Email Gateway.
- Pentru a crea rapid mai multe profiluri cu setări similare, utilizează acțiunea Copiere pentru a copia profilul original şi a face modificările necesare.

5.0 Gestionarea aplicațiilor

Soluția de gestionare Vodafone Mobile Application Management permite administratorului să distribuie wireless şi să gestioneze aplicații interne, publice şi achiziționate din grupul dispozitivelor mobile. În plus, **Catalogul de aplicații Vodafone Enterprise** permite corporației să construiască aplicații sigure de afaceri care pot fi implementate, gestionate şi securizate împreună cu aplicații publice, printr-un catalog de aplicații particularizat. Prin instrumentele de gestionare a aplicațiilor în VSDM, administratorii pot permite utilizatorilor să vizualizeze fără efort, să instaleze şi să actualizeze atât aplicații interne cât şi publice.

Activarea catalogului de aplicații Vodafone

Primul pas pentru implementarea aplicațiilor prin intermediul serviciului Vodafone este introducerea catalogului de aplicații App Enterprise, în forma unui clip Web (iOS) sau a unui profil Marcaj (Android):

- Navighează la **Profiluri & Politici→Profiluri**.
- Selectează **Adăugare**.
- Va apărea **Selectare formular platformă**. Alege **Android** sau **Apple**, în funcție de dispozitivul pe care doreș ti să îl configurezi.
- Configurează profilul Setări generale.
- Selectează Web Clips pentru iOS sau Bookmarks pentru Android, în lista profilului din partea stângă.
- Alege Configurare şi completează profilul clipului Web sau parametrii profilului Marcaj.

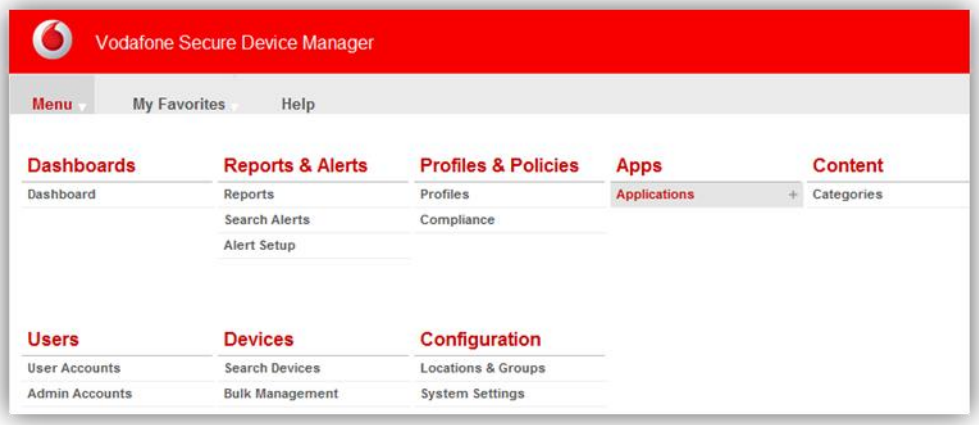
- **Etichetă**– Numele afişat pe dispozitivele gestionate pentru clipul Web. De exemplu, ar putea fi folosit **Catalogul de aplicații Vodafone**.
- **URL –** URL-ul în pentru catalogul de aplicații este în acest format: **https://<YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}** where <YourEnvironment> este URL-ul de înscriere atribuit companiei dumneavoastră.
  - ***Notă:*** Dacă foloseș ti mediul divizat SaaS, foloseș te convenția: https://dsxx.airwatchportals.com/devicemanagement/AppCatalog?uid=%7bDeviceUid%7dDe exemplu, dacă eș ti în mediul CN22, foloseș te **https://<YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}**
  - ***Notă:*** Puteți de asemenea modifica pagina de întâmpinare pentru Catalogul de aplicații. Folosiți convențiile listate mai jos:
  - Interne: https://YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}&defaultTab=Internal
  - Publice: https://YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}&defaultTab=public
  - Categorii: https://YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}&defaultTab=categories
  - Achiziționate: https://YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}&defaultTab=purchased
  - Actualizări: https://YourEnvironment>/devicemanagement/AppCatalog?uid={DeviceUid}&defaultTab=updates
- **Pictogramă** – Pentru a adăuga o pictogramă personalizată, selectează un fişier grafic în format .gif, .jpg, sau .png.
  - Pentru cele mai bune rezultate, furnizează o imagine pătrată nu mai mare de 400 de pixeli pe fiecare parte şi mai puțin de 1 MB ca dimensiune atunci când este necomprimată. Grafica se scalează automat şi se ajustează pentru a se potrivi, dacă este necesar, convertindu-se la formatul .png. Pictogramele Web Clip au 104 x 104 pixeli pentru dispozitivele cu un afişaj Retina sau 57 x 57 pixeli pentru alte dispozitive.

- Când ați finalizat, selectează **Salvare şi Publicare** pentru a implementa imediat catalogul de aplicații pe bază de Web în toate dispozitivele necesare.

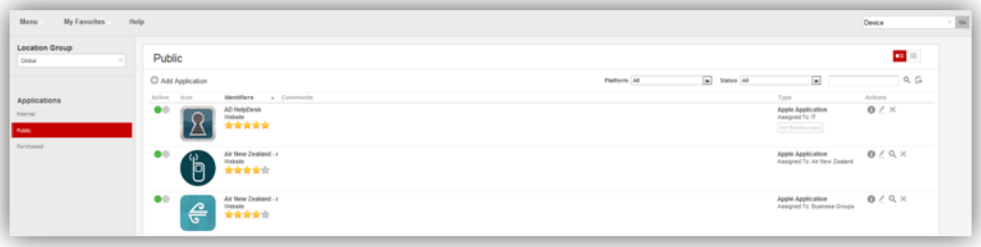
Recomandarea aplicațiilor publice

Odată ce catalogul de aplicații Vodafone a fost instalat cu succes în grupul de dispozitive smart, administratorii pot începe să recomande aplicațiile publice şi distribuirea aplicațiilor corporative prin Consola de administrare VSDM. **Pentru a recomanda aplicații publice catalogului de aplicații Vodafone de la Consola de administrare VSDM:**

- Navighează la **Aplicații & Profiluri** → **Aplicații**.

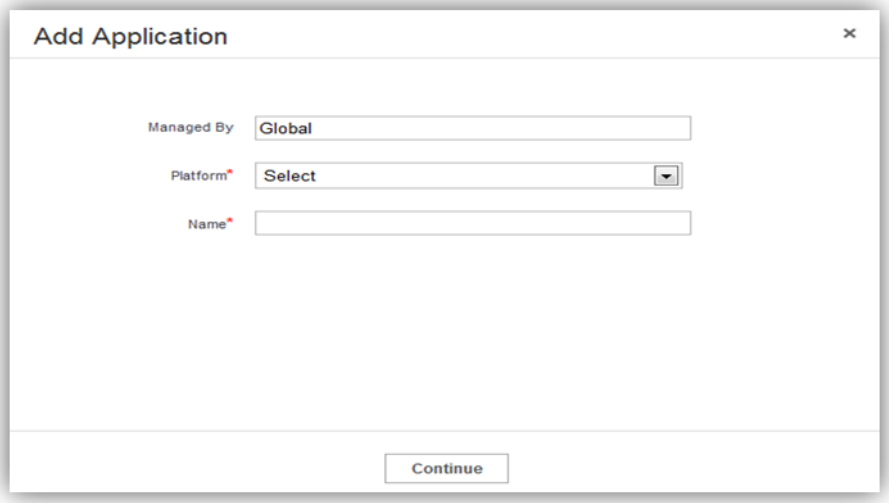


- Selectează **Public** din meniul de **Aplicații** din stânga.

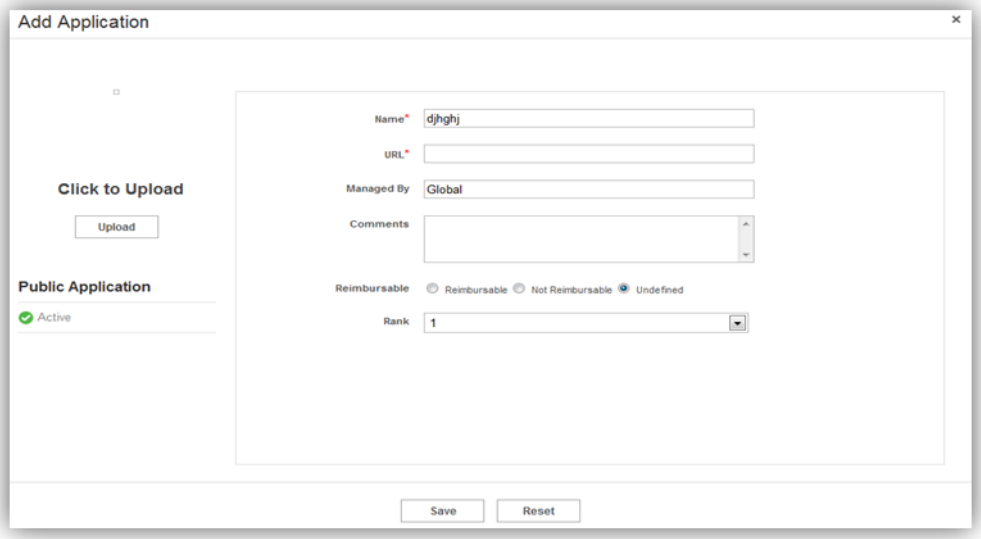


- Selectează Add Application

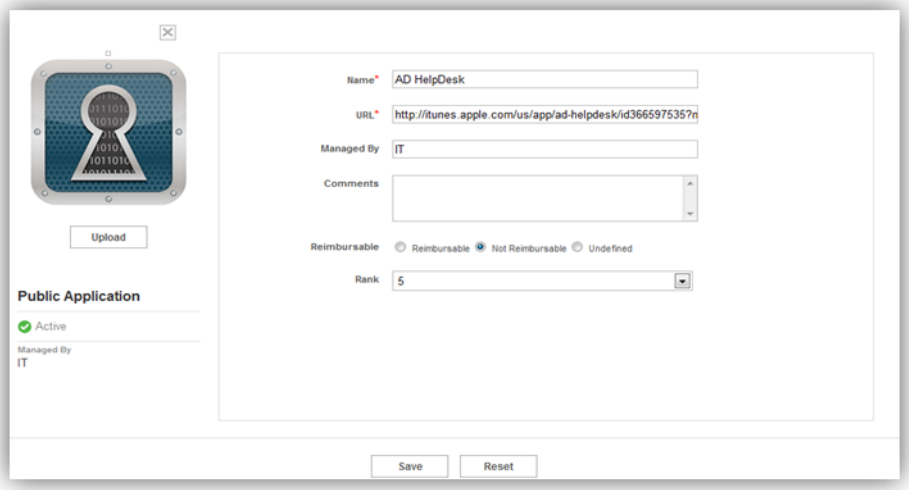
- Completează **Adăugare formular aplicații** cu toate câmpurile necesare.



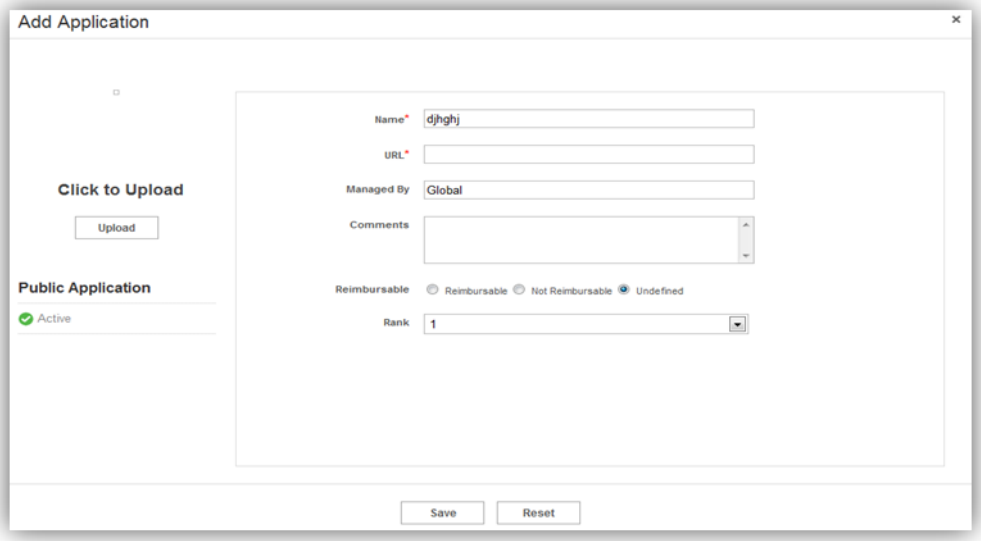
- **Gestionat de**– Grupul de locație, cu permisiunea de a edita aplicația.
- **Platforma** – Apple sau Android
- **Nume** – Numele pe care dorești să îl dai aplicației



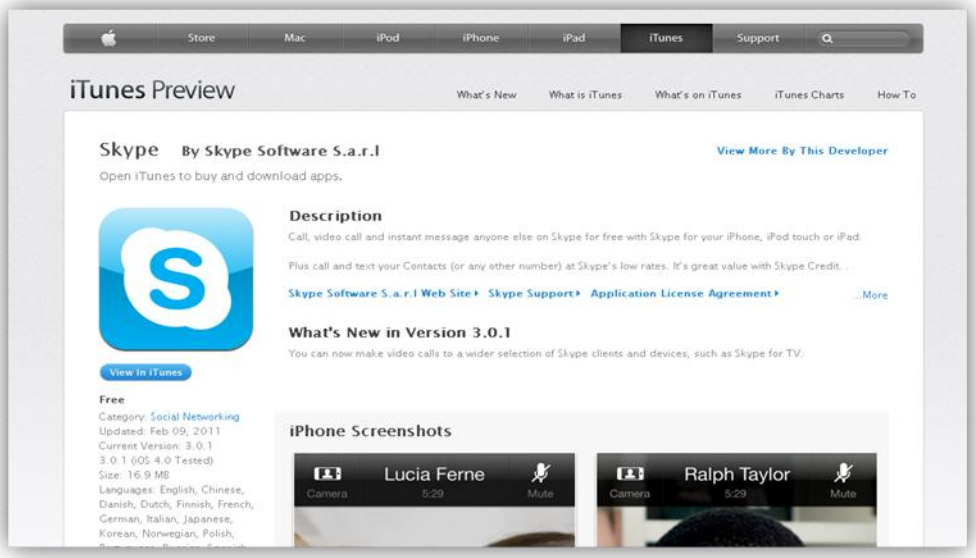
- **Caută în magazinul Apple (numai pentru iOS)** – Caută în magazinul Apple în mod automat aplicația şi populează toate detaliile aplicațiilor în următorul formular. Dispozitivele Android trebuie să completeze aceste informații manual.
- Selectează **Continuare**.
- Dacă selectezi pentru a căuta **Magazinul Apple** atunci profilul tău se populează aşa cum se poate vedea mai jos, şi trebuie doar să completezi parametrii de bază.



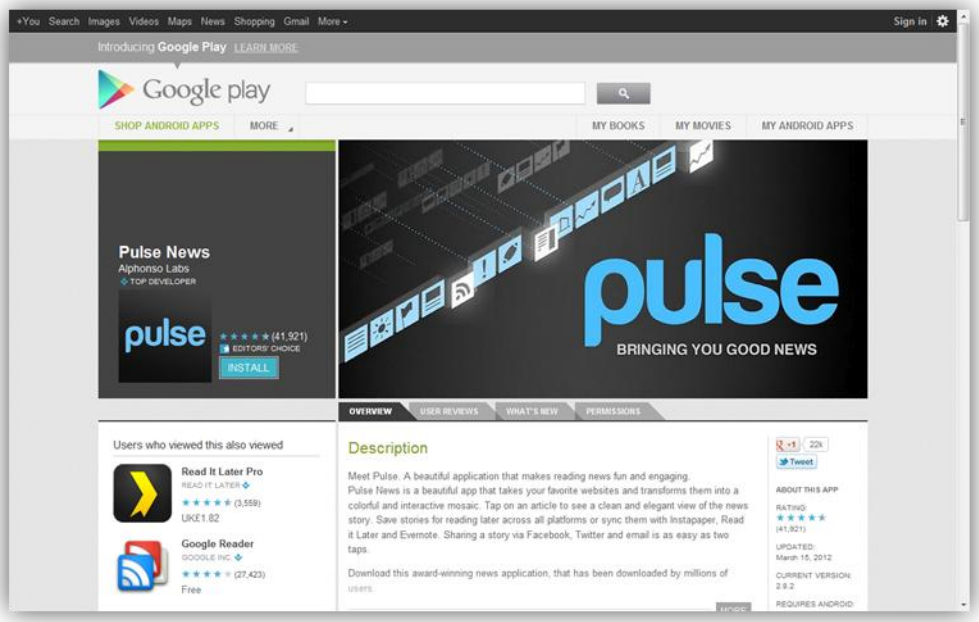
- În caz contrar, aplicația ta va arăta astfel şi trebuie să completezi următoarele informații.



- Dă click pe **Încărcare** pentru a selecta pictograma pentru aplicație.
- Introdu informații suplimentare referitoare la aplicații:
  - Pentru dispozitive iOS, utilizați URL-ul pentru aplicația specifică în iTunes Store, adică în formatul: http://itunes.apple.com/ * unde * este specifică aplicației.
- Dacă este vizualizată într-un browser, pagina arată similar cu aceasta. În acest exemplu, URL-ul pentru aplicația Skype iOS este http://itunes.apple.com/us/app/skype/id304878510?mt=8



- Pentru aplicațiile Android apps, folosești URL-ul pentru aplicația specifică din **Google play** (fosta Android Market) care este în formatul http://play.google.com/store/apps/details?id=* unde * este identificatorul pachetului pentru aplicațiile Android.
  - Găsești pagina de aplicații pentru aplicația specifică Android pe care o cauți. De exemplu, https://play.google.com/store/apps/details?id=com.alphonso.pulse pentru aplicația Pulse News Reader.

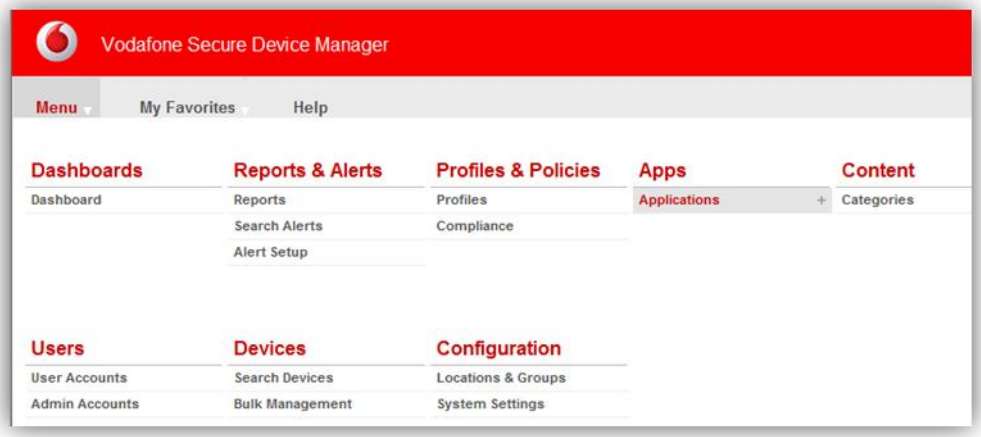


- Copiază şi apoi redă URL-ul acestei pagini în câmpul pentru **URL**.
- Completează parametrii rămaşi:
  - **Comentarii** - Comentariile suplimentare afişate atunci când utilizatorii finali dau click pe aplicația recomandată în **Catalogul de aplicații**.
  - **Rambursare**– Specifică dacă o companie rambursează sau nu utilizatorii finali pentru prețul acestei aplicații. O mică pictogramă este afişată în catalogul de aplicații Vodafone, indicând dacă pentru această aplicație se oferă rambursare.
  - **Clasificare** – Un sistem de evaluare între 1 şi 5 stele, afişat în catalogul de aplicații.
  - Caracteristic numai iOS5. Dacă aplicația va fi implementată în dispozitivele iOS5, completează în următoarele domenii:
    - **Elimină la renunțare** – Determină dacă aplicația este înlăturată atunci când un dispozitivul nu mai este înscris.
    - **Mod automat** – Determină dacă aplicația este instalată automat sau manual.
- Când ai finalizat, dă click pe **Salvare** şi aplicația recomandată este adăugată în catalogul de aplicații.

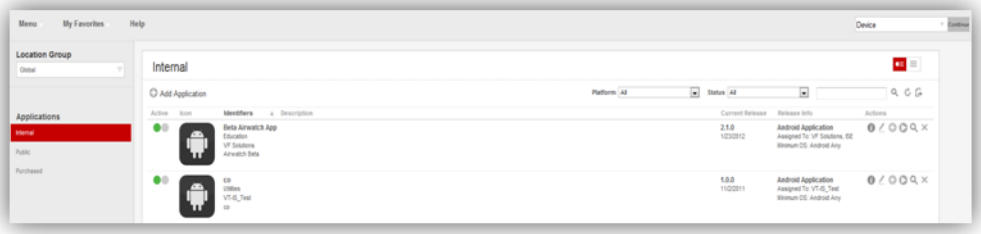
Implementarea aplicațiilor interne

Odată ce catalogul de aplicații Vodafone a fost instalat cu succes în grupul de dispozitive smart, administratorii pot începe să recomande aplicațiile publice şi distribuirea aplicațiilor corporative prin Consola de administrare VSDM. **Pentru a distribui aplicații corporative în catalogul de aplicații Vodafone din Consola de administrare VSDM:**

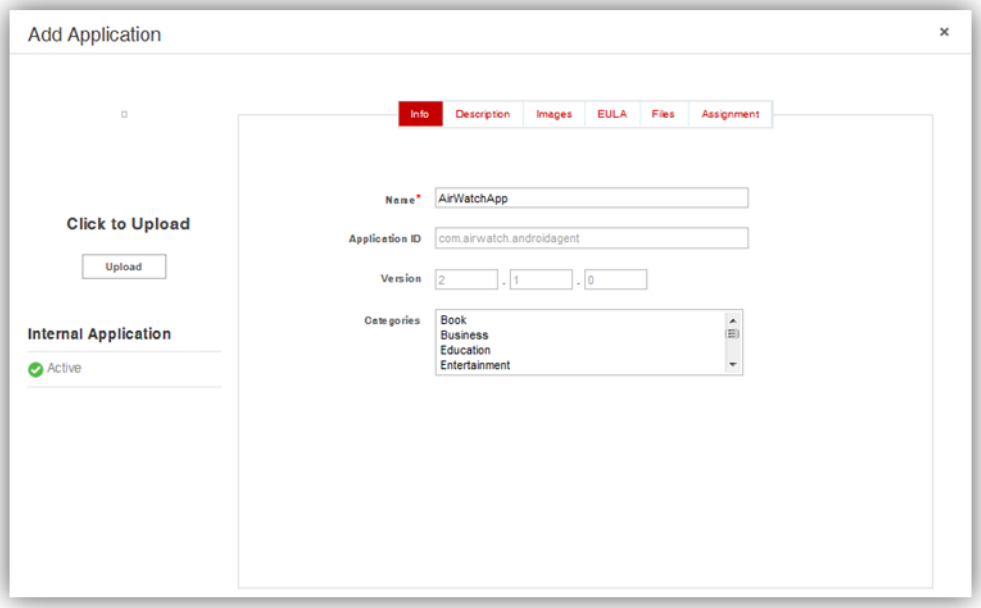
- Navighează la **Apps →Aplicații**.



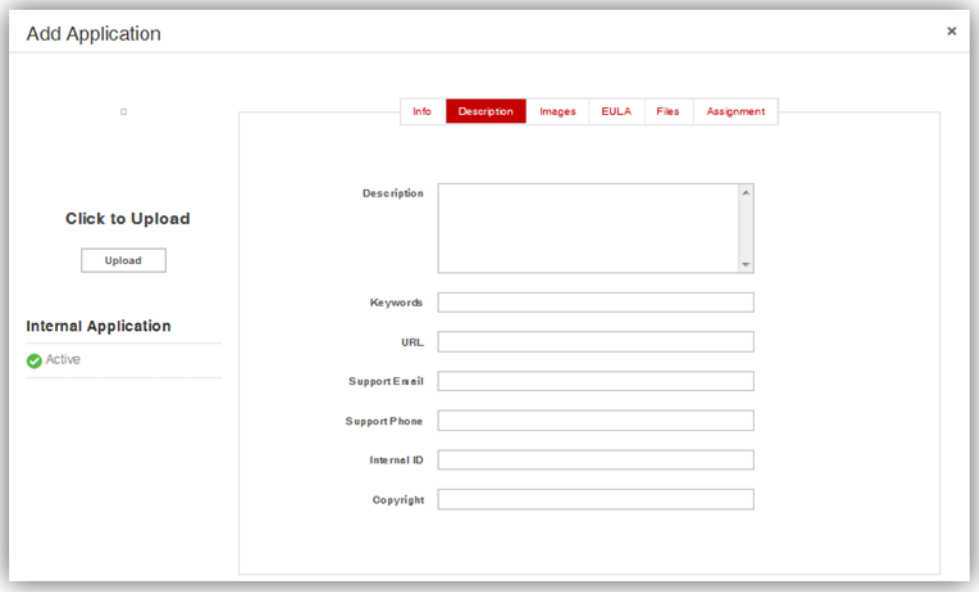
- Selectează **Interne** din meniul de **Aplicații** din stânga.



- Selectează Add Application
- Va apărea **Adăugare formular aplicație**. Completează toți parametrii generali așa cum este nevoie. Unele din câmpuri sunt subliniate mai jos.
  - **Gestionat de**– Grupul de locație, cu permisiunea de a edita Aplicația.
  - **Platforma** – Apple sau Android
  - **Fișierul aplicației** – Fișierul locației și al aplicației. Aplicațiile Apple sunt încărcate sub forma unui fișier **.ipa** iar aplicațiile Android sunt încărcate sub forma unui fișier **.apk**.
- Selectează **Continuă** și completează toate domeniile descrise mai jos, după cum este nevoie.
- Pe tab-ul **Info** tab, completează următoarele:

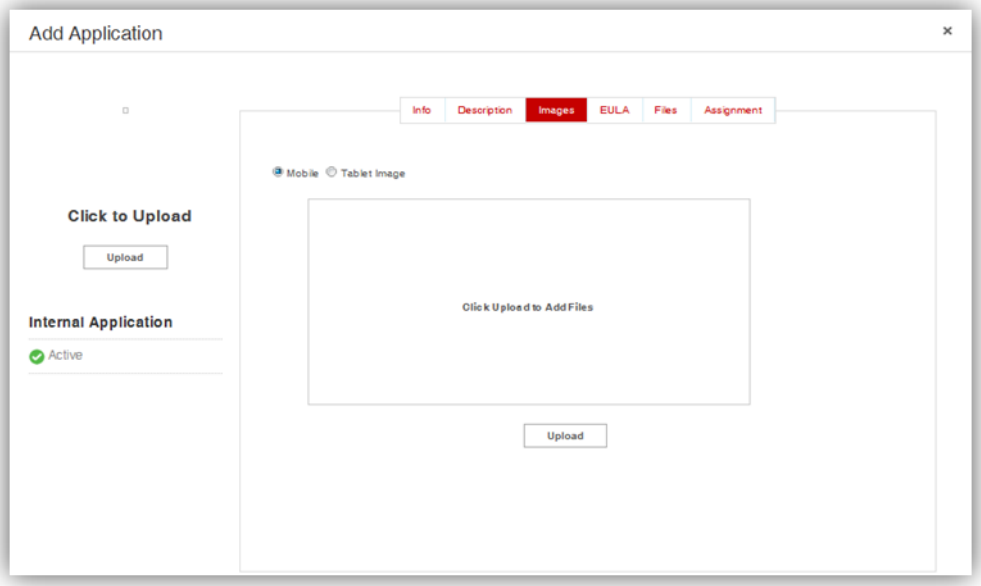


- **Nume** - Acesta este numele aplicației care este efișat pe dispozitiv.
- **ID aplicație** – Dacă încărcarci o aplicație Android, acest domeniu trebuie sa fie **Identificatorul pachetului**. Dacă este o aplicație iOS app, aceasta **TREBUIE** să fie **identificatorul grupului**
- **Versiune**– Versiunea aplicației
- Pe tab-ul **Descrieri**, completează următoarele informații opționale:

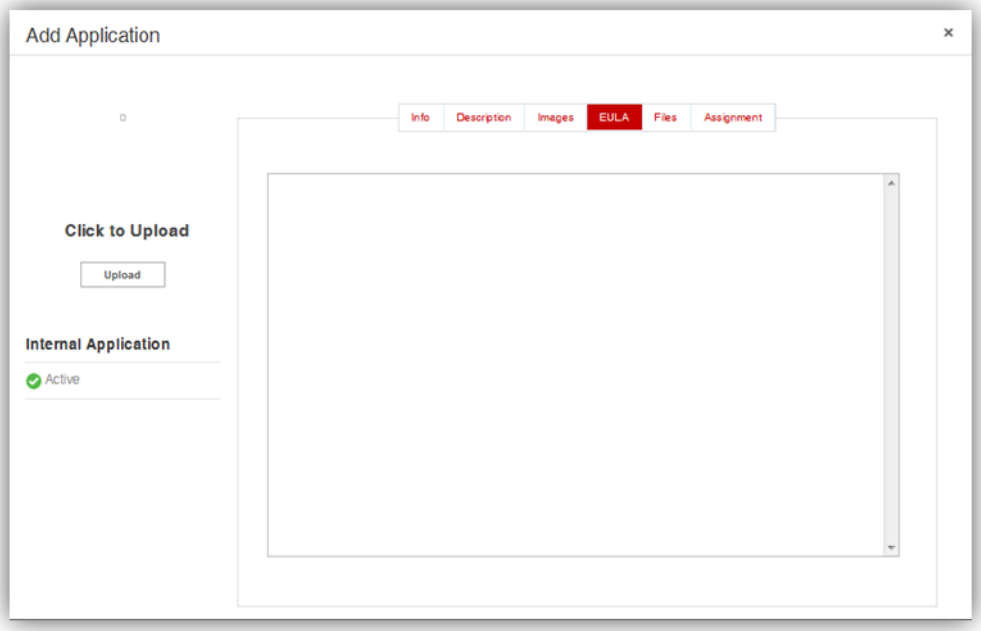


- **Descriere/Cuvinte cheie** – Introdu o descriere cu privire la aplicarea ce va fi afișată Catalogul aplicațiilor.
- **URL** - Introdu o adresă de website care are mai multe informații despre aplicație.
- **Email asistență/Telefon asistență** – Introdu informațiile de contact asistență legată de aplicații.
- **ID intern/Copyright** – Folosit pentru scopuri interne.

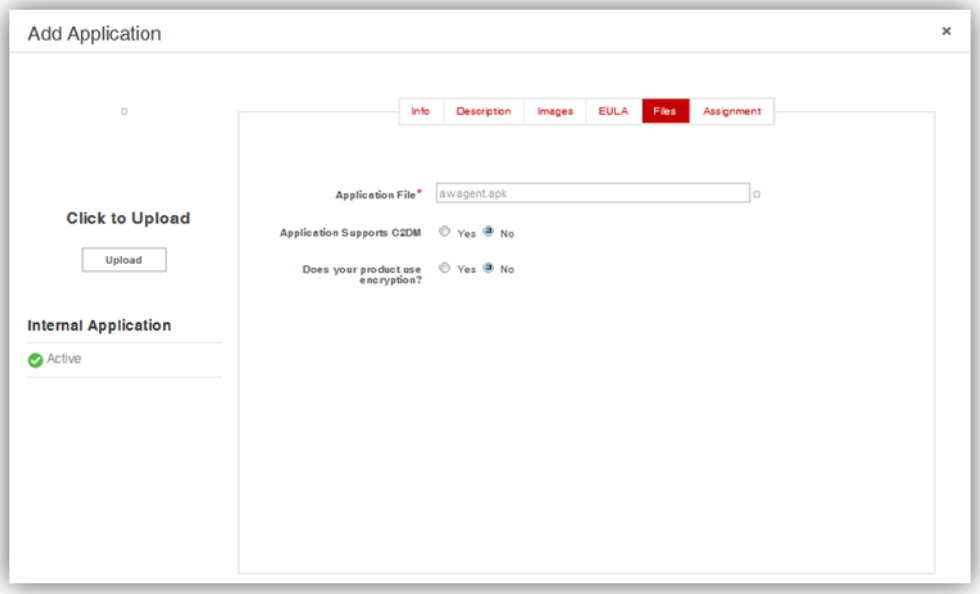
- **Imagini:** Încarcă opțional capturi de ecran ale aplicației în uz ce va fi afișată pe pagina de aplicații, împreună cu descriere, înainte de a descărca aplicația din catalogul de aplicații.



- **EULA:** Opțional , introdu o licență pentru utilizatorul final pe care doreș ti să o soliciț i înainte de a instala aplicația.

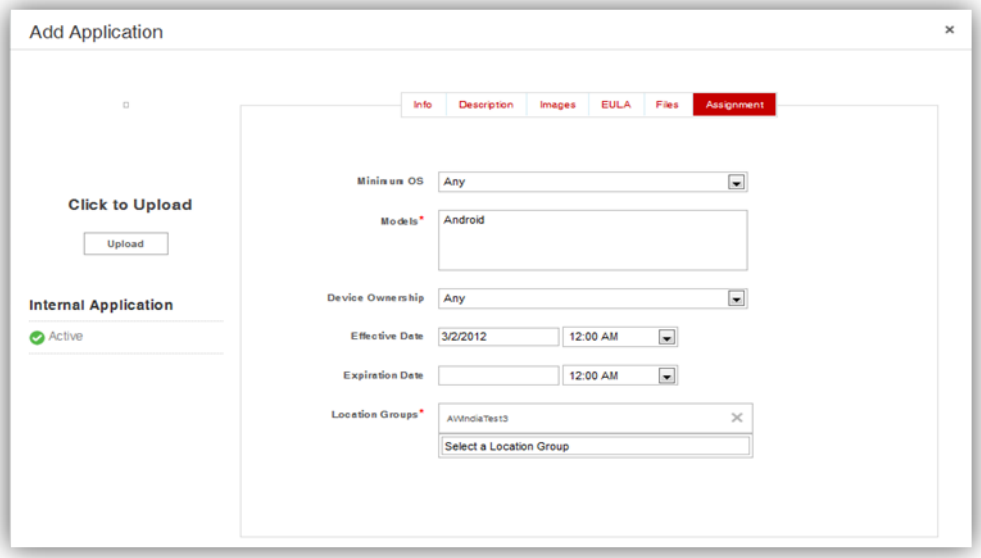


- În tab-ul **Fişiere**, completează următoarele:



- **Fişier aplicație/Furnizare profil** –Populat automat atunci când aplicație este încărcată.
- **Aplicația accepta APN** – Declară dacă aplicația acceptă Serviciile de Notificare Automate de la Apple.
  - Dacă da, încărcarea Certificatului APN este necesară.
- **Aplicația folosește AirWatch SDK (numai pentru iOS)** – Declară dacă aplicația este construită folosind AirWatch Software Kit pentru a creşte funcționalitatea acesteia în interiorul a portalului VSDM.

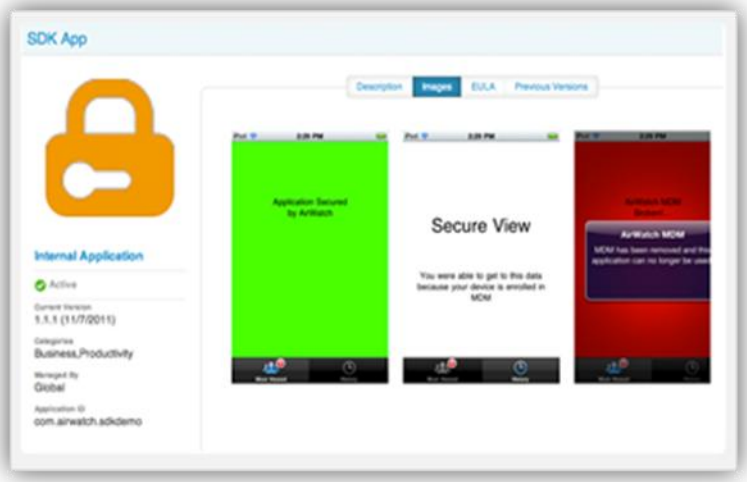
- În cele din urmă, în tab-ul **Atribuiri**, completează următoarele:



  - **Sistem de operare minim** – Permite stabilirea cerințelor minime ale sistemului de operare sistemului pentru funcționarea aplicației.
  - **Modele** – Permite desemnarea aplicației pentru anumite modele.
  - **Proprietatea dispozitivului** – Atribuie aplicația dispozitivelor cu proprietate specifică.
  - **Data efectivă /Data de expirare** – Acestea îț i permit să stabileș ti date pentru momentul în care aplicația devine activă sau expiră.
  - **Grupuri de locație -** Această casetă conține toate Grupurile de locație la care se implementează aplicația. Acest lucru este complet diferit de setarea de mai sus, care schimbă pur și simplu privilegiile administrative ale aplicației.
- **Numai pentru iOS5.** Dacă aplicația va fi implementată la dispozitive iOS5, completează următoarele câmpuri pentru a permite implementarea și gestionarea îmbunătățită a aplicațiilor:
  - **Eliminare și renunțare –** Determină dacă aplicația este înlăturată atunci când dispozitivul nu mai este înscris.
  - **Mod automat** – Determină dacă aplicația se instalează automat sau manual.
- Când ai terminat, dă click pe **Salvare** pentru a implementa aplicația internă în catalogul de aplicații Vodafone.

Cele mai bune practici

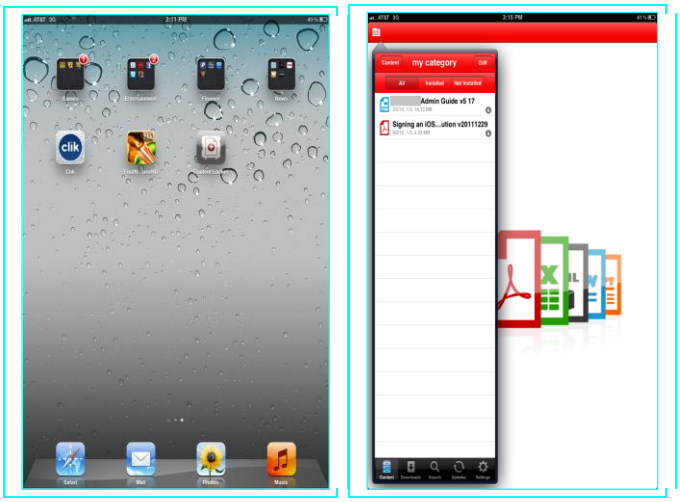
- Pentru a urmări aplicații publice pe dispozitivele angajaților prin Detalii dispozitive şi Panoul de control al dispozitivelor, asigură-te că Setările de confidențialitate ale Consolei VSDM Admin (specificate în **Configurare→Setări sistem →Dispozitiv→General→Confidențialitate**) permit strângerea şi afişarea datelor privind aplicațiile.
- Unele aplicații pot avea condiții prealabile privind dispozitivele (de exemplu, setările iCloud), pentru a fi pe deplin funcționale. Verifcă cerințele aplicației înainte de a trimite aplicațiile utilizatorilor finali. Fie activează setările corespunzătoare pentru utilizatorii finali, fie informează utilizatorii finali cu privire la orice cerințe privind setările.
- Utilizarea AirWatch SDK pentru maxima securitate şi funcționalitate în construirea de aplicații interne corporative securizate.



6.0 Gestionarea conținutului

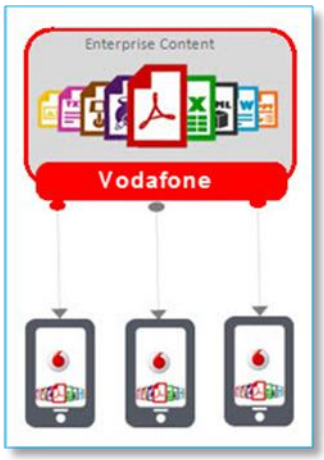
Vodafone Secure Content Locker (VSCL) este o caracteristică opțională ca parte a soluției **Vodafone Secure Device Manager (VSDM)**, **Vodafone Secure Content Locker**, permite administratorilor IT să gestioneze distribuția de documente şi accesul mobil la documente corporative, printr-o consola pe bază de web. Aplicația **Vodafone Secure Content Locker** permite angajaților să acceseze în siguranță resursele companiei, din mers, de pe dispozitivele mobile. Fie că firma ta urmăreşte să distribuie rapoarte anuale către acționari sau ultima prezentare a vânzărilor, VSCL asigură că toate informațiile corporative sunt protejate.

Notă: Vodafone Secure Content Locker este o funcție suplimentară iar disponibilitatea poate varia în funcție de piețeşe locale.



Conținutul poate fi configurat pentru a fi accesat în modurile online sau offline iar datele conținutului sunt criptate pe dispozitiv. Următorul conținut la nivel de document este acceptat de Secure Content Locker:

- **iWork:** Notă cheie (inclusiv Notă cheie09), Numere (inclusiv Numere09), Pagini (inclusiv Pagini09)
- **MS Office:** Excel, PowerPoint şi Word
- **Imagini**: Formate JPG şi PNG
- **Altele:** PDF, XML, Text, Rich Text Format (RTF) şi HTML

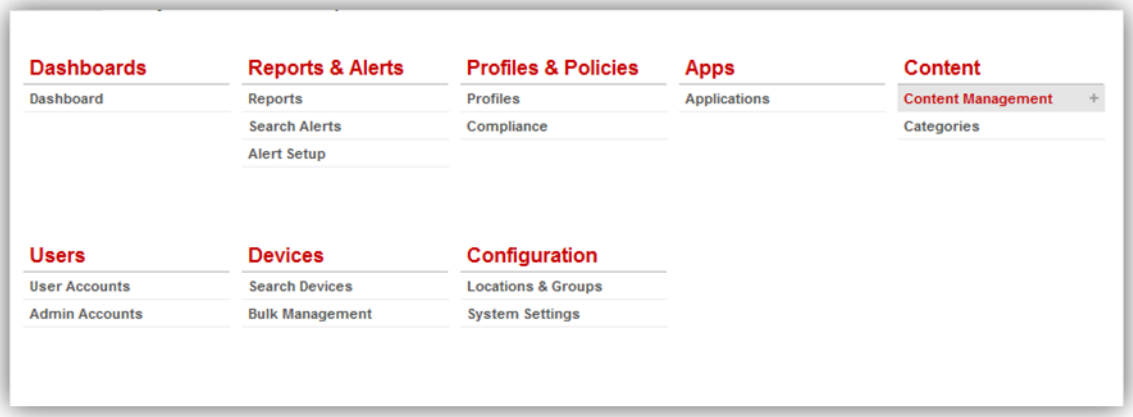


- Conținutul este gestionat la nivel de grup de locație folosind un nou meniu Conținut / interfață cu utilizatorul.
- Similar cu profilurile şi aplicațiile, conținutul este creat la un Grup de locație dar poate fi atribuit unuia sau mai multor Grupuri de locație.
- În plus, conținutul poate fi pus la dispoziția utilizatorilor finali / dispozitivelor pe baza proprietății asupra dispozitivului.

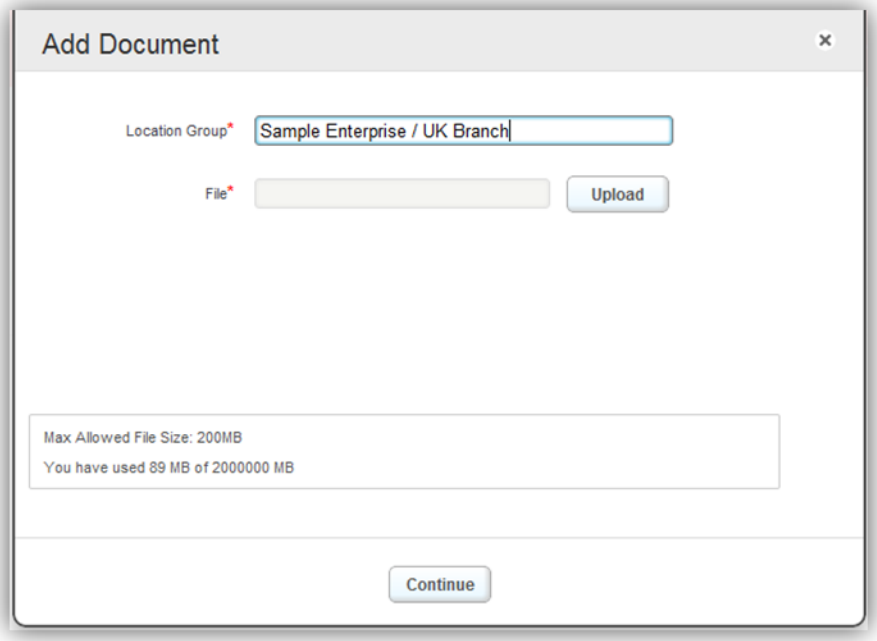
Publicarea unui document individual

Pentru a distribui un document over-the-air prin intermediul Vodafone Secure Content Locker:

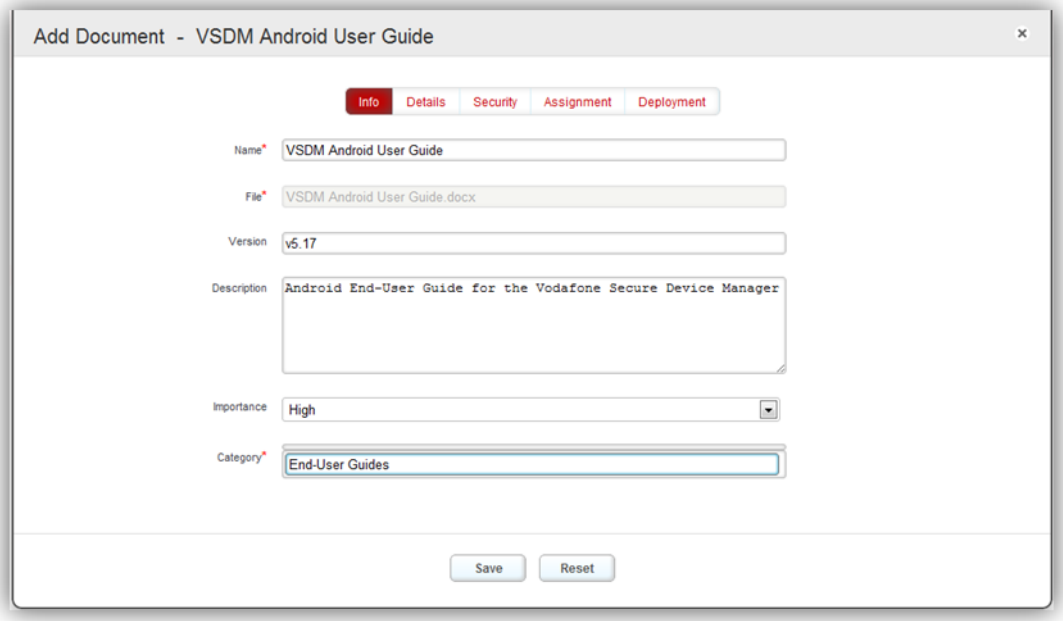
- Navighează la **Conținut→Gestionare conținut**



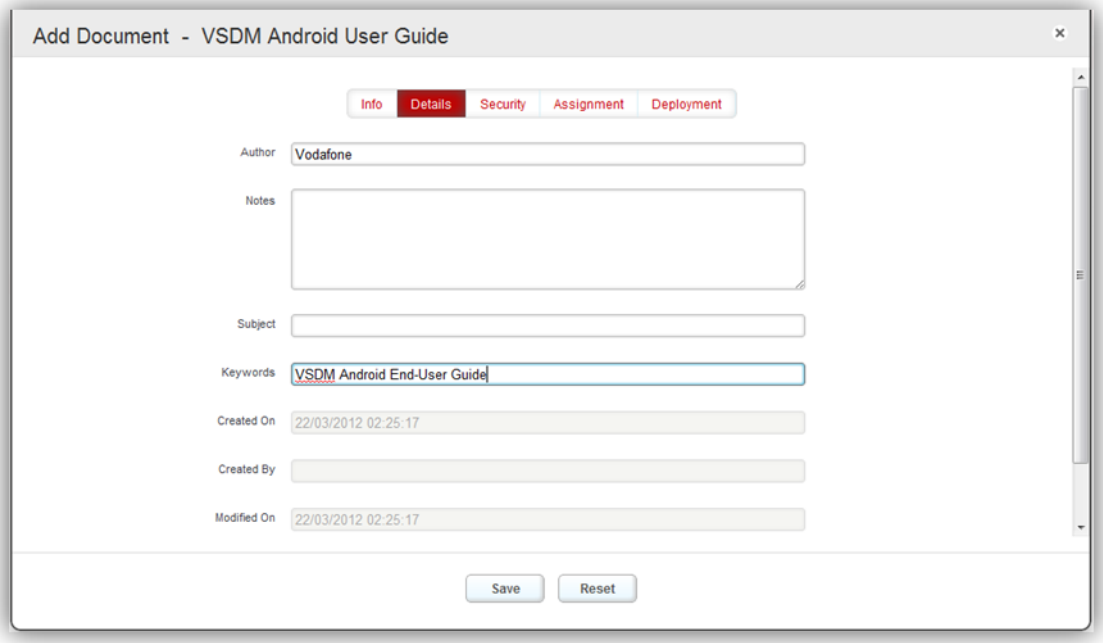
- Selectează Add Document pentru a deschide **Adăugare formular document**.
- Selectează un **Grup de locație**



- Dă click pe Upload și selectează documentul pe care doreș ti să-l distribui.
  - Numai următoarele formate sunt compatibile: **PDF**, **Numere**, **Pagini**, **Note cheie**, **Word**, **PowerPoint**, **Excel**, **HTML**, **XML**, **Text**, **RTF**, **JPG**, **PNG.**
- Dă click pe Continue

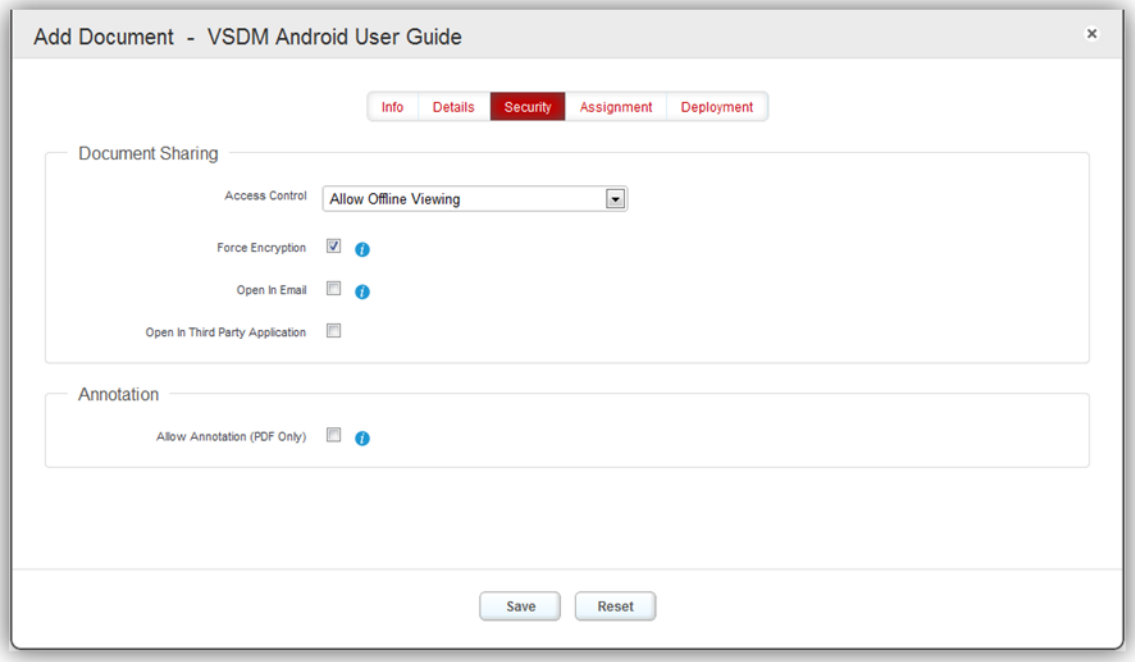


- Introdu toate informațiile de bază:
  - Asteriscurile roşii denotă câmpuri obligatorii.
  - Categoriile documentelor sunt utilizate în aplicația Secure Content Locker pentru a organiza şi grupa documentele. Fiecare document poate aparține mai multor categorii, după cum se arată mai sus.
- Selectează tab-ul **Detalii** pentru a adăuga mai multe detalii dacă este necesar.



  - Nu sunt necesare detalii, dar acestea adaugă informații suplimentare despre document care pot fi afişate în aplicația Secure Content Locker.

- Selectează tab-ul **Securitate** pentru a configura setările de control al accesului.

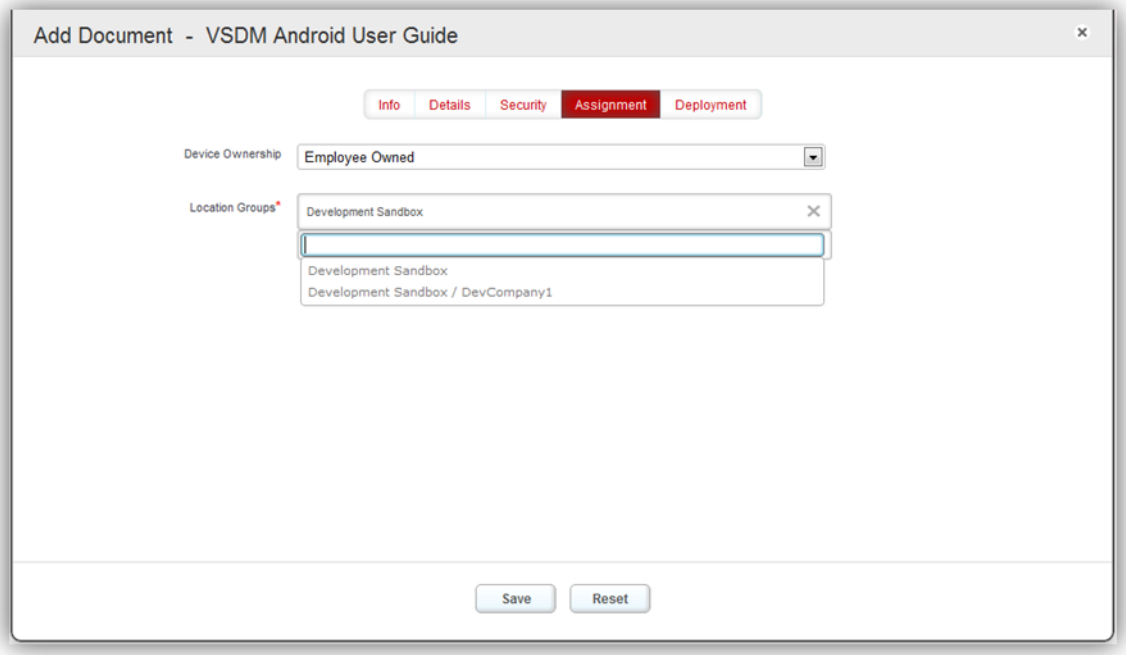


- Verifică primele două casete pentru a permite documentelor SCL să fie deschise în aplicații ale terților sau în e-mail.
- Alege dacă dispozitivul este disponibil offline când dispozitivul nu comunică cu Vodafone Locker Secure Content,
- Selectează dacă doreș ti să criptezi acest document atunci când a fost descărcat pe dispozitiv.

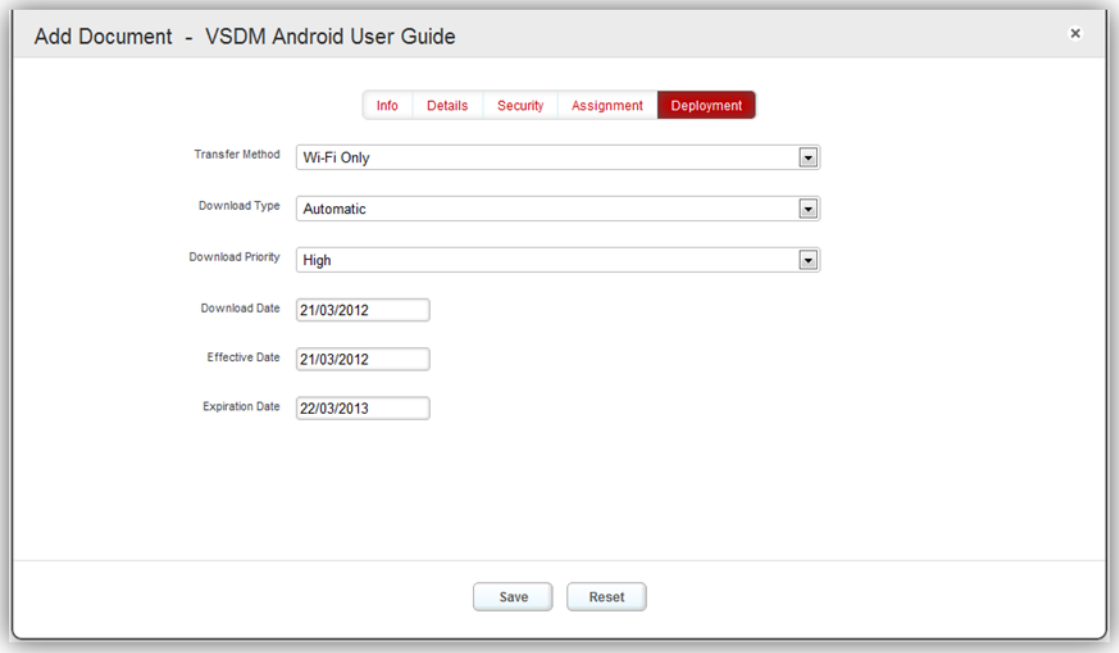
Notă: Aceasta se recomandă pentru întregul material corporativ de importanță majoră. Numai documentele care sunt considerate cu destinație publică nu trebuie criptate dacă administratorul doreşte să economisească timpul de procesare pe toate dispozitivele în timpul deschiderii documentului.

- În cele din urmă, alegi dacă permiți adnotarea (comentarea şi marcajele) documentelor PDF.

- Selectează tab-ul **Atribuire** pentru a filtra receptorii documentului.



  - Selectează un tip de proprietate asupra dispozitivului pentru a trimite documentul la dispozitive înscrise în acea categorie de proprietate.
  - Atribuie documentului ce va fi implementată în una sau mai multe grupuri de locație. Aceasta este o cerință obligatorie.
- Selectează tab-ul **Implementare** pentru a specifica opțiuni avansate de implementare pentru document.



  - **Metoda de transfer** – Selectează dacă este trimis la utilizatorul final în orice moment sau numai atunci când dispozitivul este conectat la **Wi-Fi**.

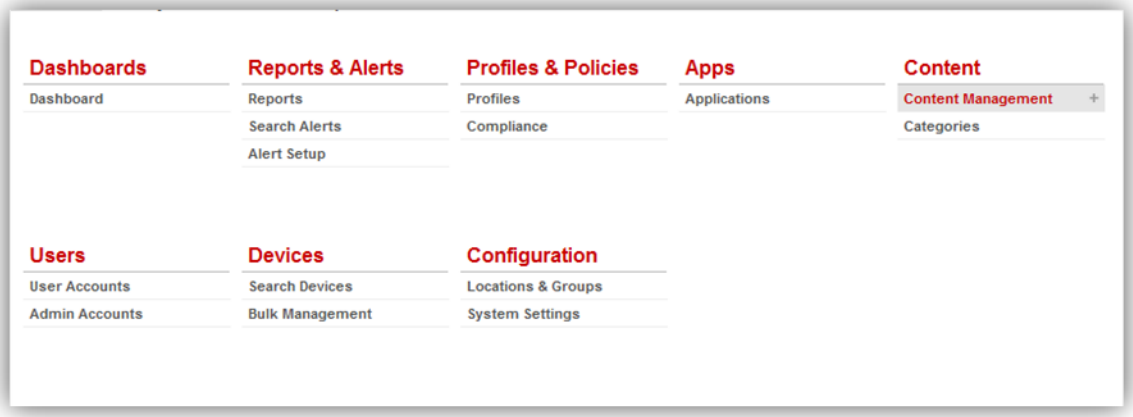
- **Tip descărcare** – Selectează **La cerere** pentru a permite utilizatorului final să descarce documentul atunci când doresc, sau **Automat**, pentru a trimite documentul la dispozitiv de îndată ce se înscrie şi descarcă Secure Content Locker.
- **Prioritate de descărcare** – Prioritatea în care se face descărcarea fişierelor dacă s-a format o coadă de documente suplimentare. De exemplu, dacă două documente aşteaptă să fie descărcate şi au o prioritate de descărcare diferită, documentul cu cea mai mare prioritate se va descărca primul.
- **Data efectivă şi data de expirare** – Data în care documentul devine disponibil şi data când dispare în aplicația Secure Content Locker.

- Odată ce ai terminat, dă click pe **Salvare** pentru a finaliza procesul.

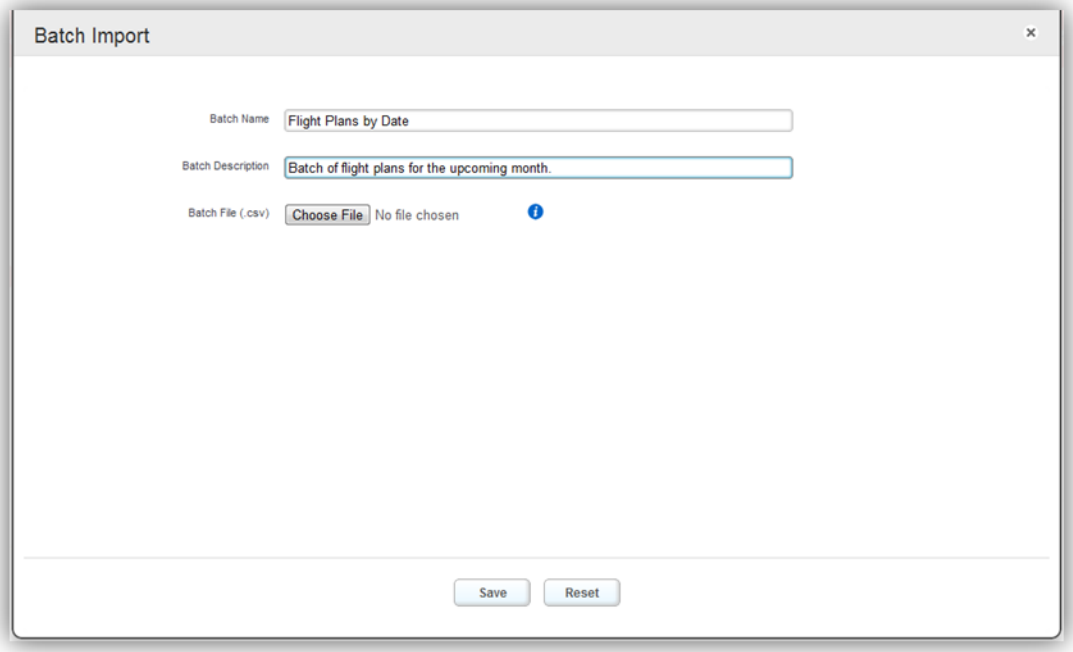
Publicarea documentelor în grup

Pentru a încărca şi distribui documente multiple:

- Navighează la **Conținut→Gestionare conținut**



- Dă click pe Bulk Import pentru a deschide **Formularul de import în grup.**



- Introdu **Numele grupului** şi **Descrierea grupului**.
- Dă click pe pentru a deschide **Content Locker Import Help Topic**: De aici descarcă **Şablonul de import pentru Content Locker**.
- Introdu toate informațiile necesare în şablon şi salvează. Asigură-te că ai salvat sub forma unui fişier **.csv**.
  - Toate câmpurile obligatorii sunt desemnate cu un asterisc *.
  - Pentru a selecta o copie locală a unui document din computerul tău, introdu FilePathType (Coloana B) ca **filepath**. Pentru a descărca documentul de la o adresă Web address, introdu **http**.

- Separă categoriile multiple prin ;
- Toate coloanele rămase conțin câmpuri care au fost explicate în procesul de încărcare a documentului unic.

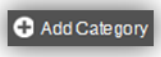
- Când ai terminat, salvează fişierul ca **.csv** şi încarcă-l în **Formularul de import în grup**.
- Selectează **Salvare** pentru a finaliza procesul.

Crearea categoriilor de documente

Categoriile de documente ajută la organizarea conținutului şi a documentelor legate de grup, atât pentru a simplifica dar şi a îmbunătăți experiența utilizatorului final. Pentru a acrea o categorie de documente:

- Navighează la **Vizualizare categorii** 

în **Pagina de conținut.**

- Selectează 

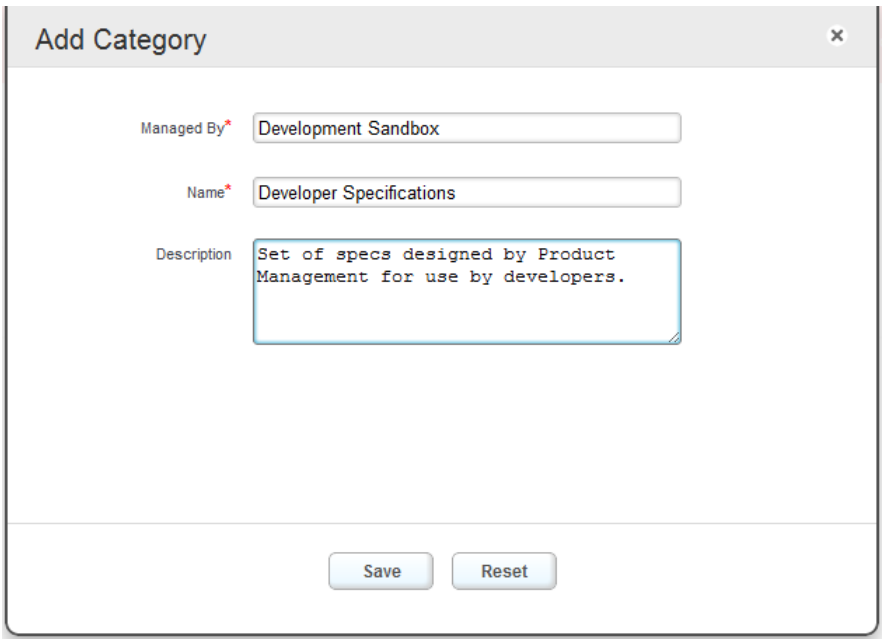
pentru a deschide formularul **Adăugare formular categorii**.
- Completează informațiile necesare.

- **Gestionat de** –Grupul de locație care poate edita, adăuga subcategorii şi şterge categoria.
- **Nume** –Numele categoriei.
- **Descriere** –O descriere a categoriei.

- Selectează **Salvare** pentru a finaliza procesul.

Administratorii unui grup de locație pot crea, de asemenea, subcategorii astfel:

- Selectând **Adăugare** de lângă denumirea categoriilor originale din **Vizualizare categorii**.



- Introdu **Denumirea** şi **Descrierea**.
- Selectează **Salvare** pentru a finaliza procesul.

Gestionarea documentelor

Există mai multe acțiuni disponibile pe pagina de **Gestionare conținut** pe care un administrator le poate efectua pentru a gestiona conținutul corporativ din Secure Content Locker.

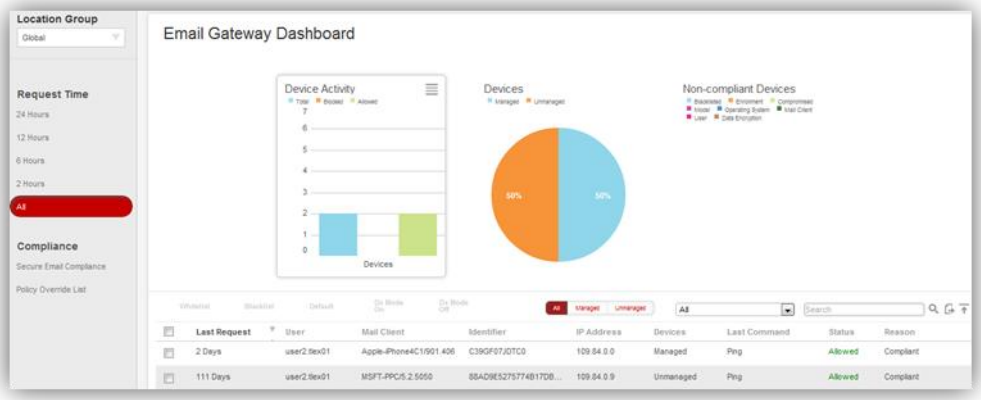
-  Editează oricare din detaliile create în timpul procesului de adăugare a unui nou document.
-  Dacă documentul este actualizat, administratorii pot adăuga o versiune mai nouă a documentului. Utilizatorii finali sunt notificați în mod automat dacă există o versiune nouă a unui document.
-  Vizualizează o listă a dispozitivelor de care au descărcat în prezent acest document.
-  Descarcă o copie locală a documentului pentru a o vizualiza.
-  Şterge documentul din Secure Content Locker.

Cele mai bune practici

- Crează categorii de documente **înainte** de a începe să încarci documente. Categoriile sunt selectate în timpul procesului de încărcare dar trebuie să create separat.
  - Pentru a crea o categorie, selectați setarea **Categorii** din pagina de **Gestionare a conținutului** sau navigați la **Gestionare conținut→Categorii**.
- Administratorii ar putea dori să permită utilizatorilor finali să stocheze şi să acceseze conținutul local, utilizând aplicații de la terți.
  - În cazul în care li se permite, utilizatorii finali pot descărca şi vizualiza o copie locală a documentelor selectând  .
- **Încurajarea utilizatorilor finali să activeze urmărirea prin GPS**–Utilizatorii pot activa servicii de localizare în setările Secure Content Locker pentru a permite administratorilor să urmărească şi să acceseze coordonatele GPS.

7.0 Gestionarea emailului

Vodafone oferă administratorilor mai multe opțiuni pentru a configura integrarea în siguranță a serviciilor de email corporative. Soluția cea mai robustă şi extensibilă este prin **Vodafone Secure Email Gateway**, care permite administratorului să asigure, monitorizeze şi gestioneze atât grupul de dispozitive smart cât şi accesul corporativ la e-mail, toate din VSDM.



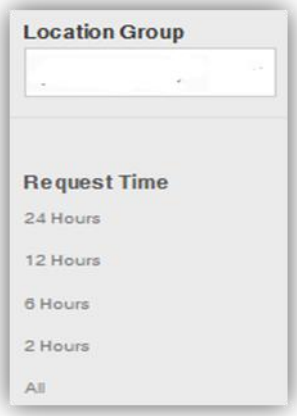
Vodafone simplifică şi asigură gestionarea e-mailului, permițând administratorului să efectueze următoarele sarcini:

- Monitorizarea şi depanarea rapidă a cererilor către serverele de e-mail prin Bordul Secure Email Gateway.
- Câştigarea vizibilității şi controlului asupra structurii corporative existente privitoare la e-mail, pentru a asigura că acțiunile corporative legate de e-mail sunt sigure şi corespunzătoare..
- Crearea şi editarea de reguli de conformitate privitoare la email, inclusiv a politicilor Lista neagră şi Lista albă.
- Controlarea accesului la Email atât pentru **dispozitivele gestionate** cât şi **dispozitivele negestionate**
  - Pentru dispozitivele din Vodafone Secure Device Manager, datele colectate de la Secure Email Gateway pot fi corelate cu înregistrările existente ale dispozitivului pentru a vedea modul în care dispozitivele gestionate interacționează cu serverul de email.
  - Pentru dispozitivele care nu se află sub VSDM, datele pot fi vizualizate pe bord pentru a ajuta administratorul să urmărească dispozitivele frauduloase şi a obține o imagine completă asupra implementării e-mailului pe mobil.
- Configurarea integrării cu o serie de servicii de e-mail corporative, inclusiv: Gmail, Exchange, BPOS 365, Lotus, Group wise versions 8.5+ şi altele.

Politici de conformitate privind emailul

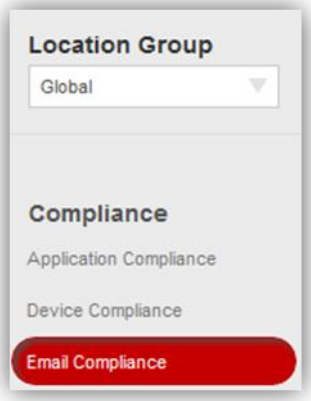
Politicile de conformare privind e-mailul permit administratorului să blocheze accesul la serverele de e-mail corporative pentru o securitate îmbunătățită a e-mailului, pe baza politicilor de conformare de pre-definite. Pentru a configura Politicile de conformitate privind emailul:

1. Navighează la **Bord**→Secure Email Gateway şi selectează **Conformitate Email pe Mobil** din ecranul **Conformitate**.



SAU

2. Navighează la **Profiluri & Politici**→**Conformitate** şi selectează **Conformitate Email** din Ecrane disponibile.



Există două categorii de politici de conformitate: **Politici generale privind emailul** şi **Politici ale dispozitivului gestionat**. Ecranul afişează o listă a Politicilor actuale de conformitate.

- Cercurile din coloana **Activ** indică dacă politica este activă (cerc verde) sau inactivă (cerc roşu):
- Dă click pe pentru a edita politica.
- Dă click pe **Salvare** pentru a finaliza editarea politicii sau pe **Resetare** pentru întoarcere la valorile dinainte.

7.1.1 Politici generale privind emailul

Politicile de conformitate privind emailul sunt aplicate pe **toate dispozitivele** care solicită accesul la Emailul corporativ prin Secure Email Gateway.

▶ Dispozitiv gestionat

- Deschide politica şi specifică dacă doreş ti să **Permiț i** sau să **Blochezi** dispozitivele negestionate care încearcă să contacteze serverul de Email corporativ.

▶ Client mail

- Deschide politica şi dă click pe **Adăugare regulă**.
- Selectează o opțiune din meniul derulant **Tip client**:
  - ▶ **Pre-definit** – Cienții cunoscuți de mail stocați în baza de date.
  - ▶ **Descoperit** – Clienții mailurilor care se conecteaza prin gateway dar nu sunt în prezent stocați în baza de date.
  - ▶ **Personalizat** – Clienți de mail specificați (i.e. Apple sau Android).
- Selectează **Clientul de mail** din meniul derulant sau alegeți **Personalizat** pentru a introduce un client de mail.
- Alege fie să **Permiți** sau să **Blochezi** clientul de mail specificat şi tipul.
- Specifică politica implicită (**Permisiune** sau **Blocare**) pentru toți clienții de mail care nu sunt listați (se aplică tuturor clienților cunoscuți de mail care nu sunt incluş i în prezent în politică).
- Specifică politica implicită (**Permisiune** sau **Blocare**) pentru toți clienții de mail noi sau descoperiți (se aplică tuturor clienților de mail care nu sunt incluşi în prezent în baza de date).
- Dă click pe **Salvare**.

▶ **Utilizator** – Blochează utilizatorii specifici de la accesarea e-mailului corporativ de pe dispozitivul lor mobil:

- Selectează un **Tip de client** din meniul derulant:
  - ▶ **Cont utilizator Vodafone** – Selectează un utilizator de dispozitiv înregistrat din baza de date VSDM.
  - ▶ **Descoperit** – Utilizatorii care se conecteaza prin gateway dar nu sunt în prezent stocați în baza de date.
  - ▶ **Personalizat** – Utilizatori specificați.
- Selectează un **Nume de utilizator** din meniul derulant.
- Fă o selecție pentru a **Permite/Bloca/Înscrie pe lista albă** pe utilizatorul specificat.
- Fă o selecție între **Permite/Blochează** ca acțiune implictă pentru toate numele de utilizatori care nu sunt listate la acel moment.
- Specifică politica implicită (**Permite** sau **Blochează)** pentru toate celelalte nume de utilizator noi sau descoperite care nu sunt listate în acest moment.

7.1.2 Politici gestionate ale dispozitivului

Politicile dispozitivului gestionat sunt **puse în aplicare numai pe dispozitivele în prezent înscrise în Vodafone Secure Device Manager**.

▶ Inactivitate

- Deschide politica şi specifică dacă doreş ti să **Permiți** sau să **Blochezi** dispozitivele negestionate care încearcă să contacteze serverul de email.
- Introdu numărul de zile de inactive pentru a defini inactivitatea.

▶ Conformitatea compromisă a dispozitivului

- Deschide politica şi selectează dacă doreș ti să **Permiți** sau să **Blochezi** dispozitivele compromise care încearcă să contacteze serverul de email.

  ▶ Conformitate criptare

- Deschide politica şi selectează dacă doreș ti să **Permiți** sau să **Blochezi** dispozitivele care încearcă să contacteze serverul de email şi care nu au activat protecția datelor.

  ▶ Conformitatea platformei şi a modelului

- Deschide politica şi dă click pe **Adăugare regulă**.
- Selectează o opțiune din meniurile derulante **Platformă** şi **Model**.
- Fă o selecție de a **Permite** sau **Bloca** platfoma sau modelul specificat.
- Specifică politica implicită (**Permite** sau **Blochează)** pentru toate modele nelistate în acest moment.

  ▶ Conformitatea sistemului de operare: Administratorii pot dori să blocheze o anumită versiune de sistem de operare pe un dispozitiv mobil care îngreunează serverul de e-mail din cauza unui bug sau a altor probleme tehnice.

- Deschide politica şi dă click pe **Adăugare regulă**.
- Selectează o opțiune din meniurile derulante **Platformă** :
- Selectează **Min OS** (sistem de operare minim) **şi Max OS** (sistem de operare maxim).
- Specifică politica implicită (**Permite** sau **Blochează)** pentru toate versiunile de sistem de operare care nu sunt listate în acest moment.

7.1.3 Aplicarea politicilor de conformitate privind emailul

1. După ce creezi sau editezi politicile de conformitate ale emailului, politicile sunt în mod automat aplicate când Mobile Email Gateway este actualizat (Configurați intervalul de actualizare în **Setări sistem→Email→Setări avansate**).

2. Pentru a aplica instantaneu politica, dă click pe **Operare modificări politică** în partea de jos a paginii **Politici de conformitate a emailului**.

Bord Gateway Email-uri

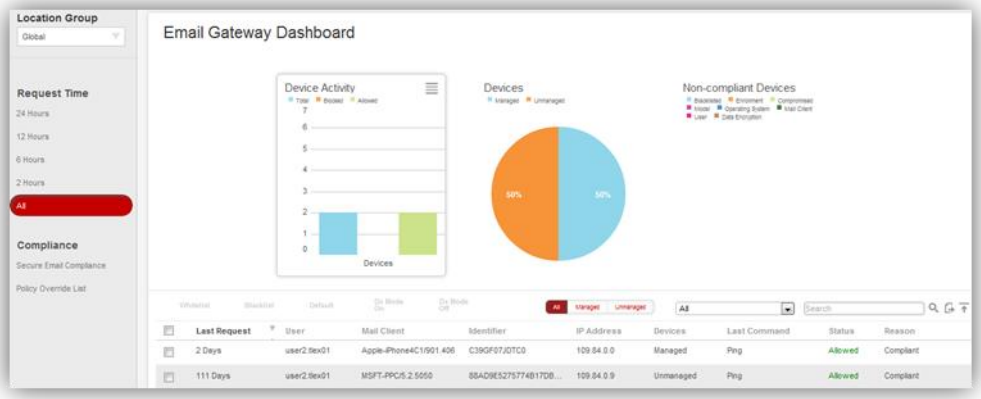
De fiecare dată când un dispozitiv încearcă să se conecteze la serverul tău mobil de email Vodafone Secure Email Gateway, gateway-ul adună statistici privind cererea. Aceste informații sunt prezentate pe bord în consola de administrare VSDM şi pot fi utilizate pentru a evalua statusul implementării e-mailului pe mobil.

- Pentru a accesa bordul Secure Email Gateway, navighează la **Borduri→Secure Email Gateway**.

- Bordul de bază al Secure Gateway este disponibil ca ecran din bordul principal dar aceasta nu conține opțiunile de interval de timp sau capabilități de editare.

Grafice şi grila

Bordul Secure Email Gateway este controlat de trei **grafice** în partea de sus a ecranului şi o **grilă** în partea de jos a ecranului care afişează datele din graficul selectat sau grupul de date.



- **Activitate dispozitiv** –Numărul total de dispozitive care comunică prin gateway, pe lângă numărul de dispozitive blocate şi acceptate.

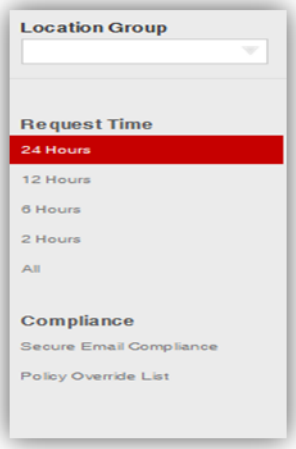
- **Dispozitive** –Numărul total de dispozitive care comunică prin gateway şi numărul de dispozitive gestionate şi negestionate.

- **Dispozitive non-conforme**–Numărul de dispozitive non-conforme ce comunică prin gateway în conformitate cu criteriile de conformitate, aşa cum sunt specificate în Politicile de conformitate privind emailul. .

7.1.4 Ecrane solicitare timp

Ecranele pentru **Solicitare timp** permit administratorului să ajusteze ecranul bordului pentru toate perioadele de timp sau pentru intervalele de timp din ultimele 24 de ore.

- Dă click pe **Toate** sau selecteaza un interval de timp pentru a actualiza tabelele şi grilele cu selecția timpului.



7.1.5 Conformitate emailuri în bord

Pentru a edita politicile de conformitate privind emailul, selectează **Conformitate email pe mobil** din ecranul **Conformitate**. Pentru informații suplimentare cu privire la crearea de politici de conformitate asupra emailului, a se vedea Politici de conformitate privind emailul.

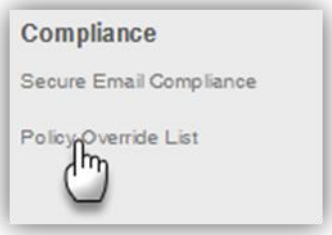
7.1.6 Suprareglarea politicii de conformitate privind emailul

Odată ce politicile privind conformitatea e-mailului au intrat în vigoare pentru Secure Email Gateway, administratorul poate găsi necesar să facă excepții la lista neagră sau la lista albă, sau să elimine un dispozitiv din lista de excepții.

Pentru a corecta o politică de conformitate:

- Selectează **Ecranul cu lista de suprareglare a politicii** pentru a vizualiza starea curentă de suprareglare pentru toate dispozitivele care comunică prin gateway.

- Această pagină oferă, de asemenea, posibilitatea de a adăuga, elimina sau opera o corecție a dispozitivelor listate.



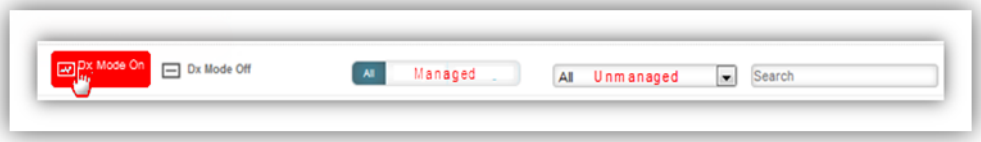
- Selectează un dispozitiv din grilă pentru a efectua o suprareglare a politicii pe acel dispozitiv.

Selectează o pictogramă a politicii:

- **Lista albă**–Permite dispozitivului să corecteze politicile de conformitate.
- **Lista neagră**–Blochează dispozitivul, indiferent de orice politici care ar putea accepta dispozitivul.
- **Implicit**–Eliminarea dispozitivului din lista de înlocuire şi aplicarea politicilor configurate de conformare la dispozitiv.

7.1.7 Diagnostice de bord şi modul de testare

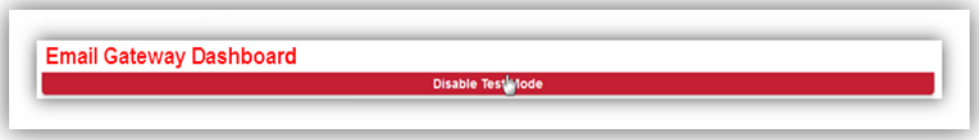
1. Modul de diagnostic poate fi pornit sau oprit pentru testare şi depanare prin selectarea unui dispozitiv şi alegerea sau activarea modului Dx.



▶ Modul testare permite dispozitivelor mobile să comunice prin gateway chiar când politicile restrictive de conformitate sunt în prezent activate. Bordul afişează codul / codurile motivelor de non-conformitate pentru un dispozitiv, care să indice toate restricțiile aplicabile dacă modul de testare nu a fost activat.

- Pentru a activa modul de testare, selectează link-ul **Activare Test Mode** de pe bord.

- Când **modul de testare este dezactivat**, politicile de conformitate se aplică din nou fiecărui dispozitiv care comunică prin gateway. Bordul afişează codul / codurile motivelor de non-conformitate pentru un dispozitiv, pentru a indica toate restricțiile care sunt aplicabile. Pentru a dezactiva modul de testare, selectează link-ul **Dezactivare Test Mode** de pe bord.



Cele mai bune practici

▶ Foloseș te ecrane de filtrare şi căutare pentru a vizualiza dispozitivele din bordul Secure E-mail Gateway, în conformitate cu criteriile de conformitate.

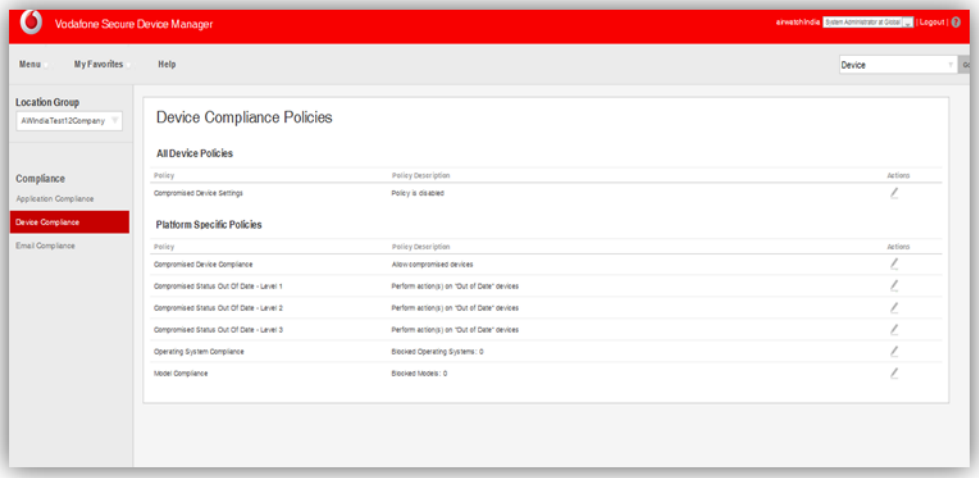
▶ Administratorul poate filtra dispozitivele afişate pe grilă de baza statutului de corecție. Selecteaza un filtru pentru a vizualiza numai dispozitivele de pe Lista neagră, Lista albă sau Toate dispozitivele.

▶ Funcționalitatea de filtrare oferă posibilitatea de a căuta în grilă în rezultatele afişate.

▶ Introdu termenul de căutare integral sau parțial în caseta **Căutare**.

8.0 Securitate şi conformitate

Vodafone Secure Device Manager foloseşte un motor de conformitate personalizabil ca să permită crearea de politici robuste de conformitate şi punerea lor în aplicare. Capacităţile VSDM de conformitate permit administratorilor să protejeze datele corporative privind proprietatea de expunerea nedorită şi să stabilească reguli pentru tratarea activităţii neconforme pe dispozitivele gestionate. Aceste politici de conformitate sunt gestionate central în pagina **Conformitate** din Consola VSDM Admin.



Pentru a naviga la pagina Conformitate, selectează **Profiluri & Politici** → **Conformitate**. De aici, administratorul poate crea mai multe tipuri de politici de conformitate:

- Politici de conformitate ale aplicaţiilor
- Politici de conformitate ale dispozitivului
- Politici de conformitate privind emailul

Notă: Politiceile de conformitate privind emailul se aplică numai când Secure Email Gateway este instalat pe soluţia Vodafone Secure Device Manager.

Privire generală asupra profilurilor cu cod de acces şi restricţii

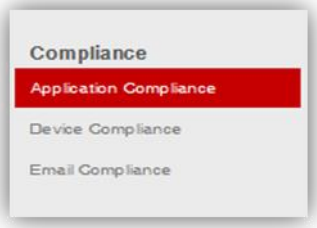
Restricţiile privind codul de acces şi dispozitivul oferă protecţie mărită dispozitivelor gestionate. Politicile de conformitate privind codul de acces includ capacitatea de a pune în aplicare coduri de acces, se a stabili complexitatea parolei şi de a gestiona auto-blocarea şi setările privind istoria codului de acces. Profilele cu restricţii permit administratorului să interzică şi să controleze utilizarea funcţionalităţilor specifice anumitor dispozitive, cum ar fi instalarea aplicaţiei aparatul foto al dispozitivului precum şi alte funcţii similare. Pentru a seta profile cu cod de acces şi restricţii pe dispozitive individuale, consultă Crearea profilelor.

Motorul de conformitate

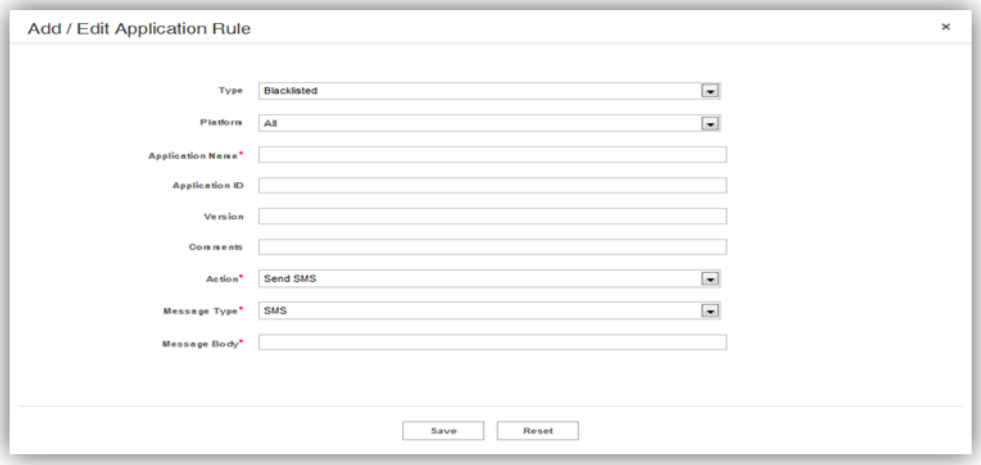
8.1.1 Conformitatea aplicațiilor

Politicile de conformitate a aplicației restricționează accesul la aplicațiile neautorizate pe dispozitive corporative. Politicile de conformitate a aplicațiilor permit administratorului să desemneze aplicații pe o listă neagră şi să trimită un mesaj sau să şteargă dispozitivul dacă Vodafone detectează o aplicație de pe lista neagră. Pentru a crea sau a edita o politică de conformitate privind aplicațiile:

▶ Pe pagina **Conformitate**, selectează ecranul **Conformitate aplicație** din bara din stânga a paginii.



▶ Selectează Add pentru a vizualiza pagina **Adăugare /Editare regulă privind aplicațiile**.



▶ Completează câmpurile de informații:

- **Tip** –Tipul de politică de conformitate a aplicațiilor. În prezent, singura opțiune este **Lista neagră.**
- **Platforma** –Platforma dispozitivului la care se aplică politica de conformitate a aplicației. În prezent, singurele opțiuni sunt platforme **iOS** şi **Android** (sau selectați **Toate** pentru a aplica politica la ambele platforme).
- **Numele aplicației** –Numele aplicației pentru care doreș ti să creezi o regulă de conformitate.
- Opțional introdu **ID-ul aplicației** şi **Versiunea.**

  ▶ Specificând ID-ul aplicației permite companiei Vodafone să detecteze dispozitivele care au aplicația de pe lista neagră instalată identificând aplicațiile în funcție de ID-ul grupului, mai degrabă decât prin căutarea numelui aplicației aşa cum este introdus în câmpul Numelui aplicației.
- **Comentarii** –Opțional, introdu un comentariu cu privire la respectarea politicii de a împărtăşi cu ceilalți administratori al Consolei VSDM admin (comentariul apare numai în Consola de administrare VSDM).
- **Acțiune** –Acțiunea administrativă care are loc automat pe orice dispozitive ce conțin aplicația numită:

  ▶ **Trimitere SMS** - Alege **Tipul mesajului** şi introdu mesajul text în câmpul **Corpul mesajului**.

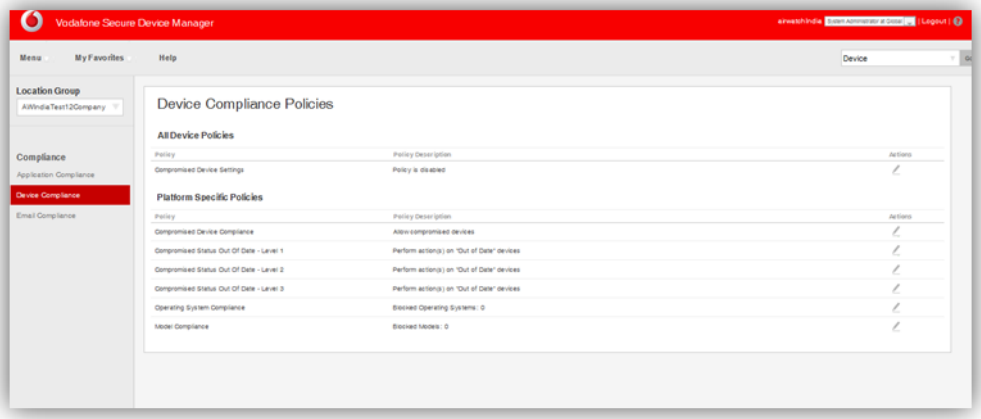
- **Ştergere completă** –Efectuează o Ştergere completă la detectarea unei violări a conformității aplicației.
- **Ştergere dispozitiv**–Efectuează o Ştergere a dispozitivului la detectarea unei încălcări a conformității aplicației.

- Când ai terminat, dă click pe **Salvare** pentru a aplica politica de conformitate.

8.1.2 Conformitatea dispozitivului

Politicile de conformitate ale dispozitivului pot fi create pentru a efectua acțiuni administrative pe dispozitive gestionate atunci când criteriile specifice ale dispozitivului sunt îndeplinite. Pentru a crea o politică de conformitate a dispozitivului:

- Pe pagina **Conformitate**, selectează ecranul **Conformitate dispozitiv** din bara din stânga a paginii.
- Alege unul din tipurile de politici de conformitate a dispozitivului din "Toate politicile dispozitivului" sau "Politici de platforme specifice".



Toate politicile dispozitivelor

Toate Politicile privitoare la dispozitiv permit administratorilor să creeze şi să editeze politicile care se aplică pentru toate dispozitivele, indiferent de platformă. Unele politici specifice se bazează pe Toate politicile dispozitivului, aşa că este o practică bună de a crea toate politicile dispozitivului înainte de a crea setările de conformitate ale dispozitivului, în funcție de platformă.

- **Setări compromise ale dispozitivului** – Politica privind conformitatea se aplică pentru toate dispozitivele şi permite administratorului să:

- Efectuează acțiuni (cum ar fi blocarea accesului la profiluri şi aplicații), pe toate tipurile de dispozitive care nu au raportat un statut compromis sau sunt detectate ca fiind compromise (bifați caseta pentru a aplica politica).
- Marchează dispozitivul ca "Out of date", dacă dispozitivul nu s-a conectat pentru un anumit număr de zile şi stabiliți niveluri de gravitate pe baza duratei fără a se conecta.

  - Nivelurile de severitate sunt definite în această casetă. Pentru a edita regulile pentru fiecare nivel de Severitate, întreprinde aceasta în Politici în funcție de platformă.
  - Pentru a defini nivelurile de gravitate, introdu durata pentru fiecare nivel de severitate şi alege valoarea (zile, ore sau minute), din meniul drop-down.

Politici specifice platformelor

Politicile specifice în funcție de platformă includ următoarele:

- **Conformitate compromisă a dispozitivului** –Efectuarea de acțiuni specifice pe dispozitive care au fost marcate ca fiind compromise. În prezent, această caracteristică acceptă doar platformele iOS şi Android. Pentru a crea sau a edita politici de conformitate privind un dispozitiv compromis:

- Selectează acțiunile administrative care urmează să fie efectuate atunci când dispozitivele îndeplinesc criteriile specificate.

- **Statut compromis Out Of Date - Nivel 1, Nivel 2 şi Nivel 3** –Efectuarea de acțiuni pe dispozitive iOS care sunt "Out of date" şi intră sub Nivelul de gravitate 1, Nivelul de gravitate 2 sau Nivelul de gravitate 3, aşa cum este definit în Setări dispozitiv compromis (a se consulta Toate politicile dispozitivelor de mai sus). Pentru a edita regulile pentru dispozitivele cu statut compromis:

- Selectează şi deschide politica dorită "**Statut compromis Out of Date–Nivel**".
- Dă click pe **Adaugă regulă**.
- Alege acțiunea (Trimite o notificare automată, Trimite e-mail, Eliminare profile EAS) şi, dacă este cazul, introdu Notificarea automată sau textul e-mailului.

  - Conformitatea sistemului de operare - Efectuarea de acțiuni pe dispozitivele iOS care folosesc o anumită versiune a sistemului de operare.
  - Respectarea Modelului - Efectuarea de acțiuni pe anumite modele de dispozitive iOS.

Pentru a edita conformitatea sistemului de operare şi politicile de Conformitate a Modelului:

- Selectează şi deschide politica de conformitate pe care doreş ti să o editezi şi dă click pe **Adăugare regulă listă neagră**.

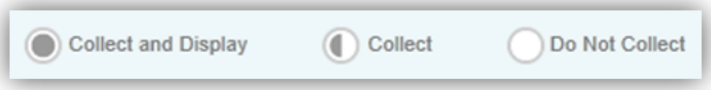
- ▶ Specifică sistemul de operare sau criteriile dispozitivului model pentru regula privind Lista neagră.
- ▶ Specifică acțiunile administrative ce trebuie întreprinse când criteriile sunt îndeplinite:

- **Trimitere SMS** - Alege **Tipul mesajului** şi introdu mesajul text în câmpul **Corpul mesajului**.
- **Ştergere completă** –Efectuează o Ştergere completă la detectarea unei violări a conformității modelului sau sistemului de operare.
- **Ştergere dispozitiv**–Efectuează o Ştergere a dispozitivului la detectarea unei violări a sistemului de operare sau a modelului.
- Repetă prin adăugarea oricăror reguli suplimentare privind politica pentru lista neagră.
  - ▶ Pentru a termina de editat politica de conformitate selectată, dă click pe **Salvare**.

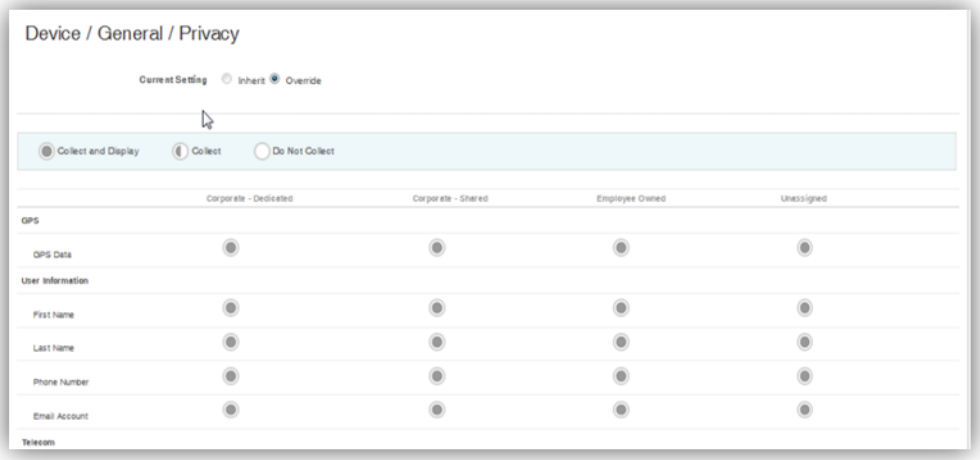
Politica de confidențialitate

Administratorii pot stabili politici complexe de confidențialitate în cadrul VSDM. Aceste politici se aplică pentru anumite tipuri de proprietate a dispozitivului în cadrul Grupurilor de Locație (tipurile de proprietate sunt: Corporativ – Dedicat, Corporativ– Divizat, Deținut de angajat şi Neatribuit).

- Pentru a accesa politicile de confidențialitate, navighează la **Configurare** → **Setări sistem**→ **Dispozitiv**→ **General**→ **Confidențialitate**.
- Pentru fiecare politică de confidențialitate, administratorii au trei opțiuni pentru gestionarea informațiilor dispozitivului. Politicile sunt definite printr-un cerc plin, jumătate de cerc, sau un cerc gol în partea de sus a ecranului.



  - Colectarea şi Afişarea - Informațiile sunt colectate de către Vodafone şi administratorii sunt capabili să vizualizeze datele.
  - Colectarea - informațiile sunt colectate de Vodafone iar administratorii nu pot vizualiza datele.
  - Nu colectați - Informațiile nu sunt colectate de către Vodafone.
- Pentru a ajusta setările de informare a politicii de confidențialitate:
  - Mută mouse-ul peste cercul care se potriveşte cu politica de confidențialitate şi tipul de proprietate asupra dispozitivului. Un mic meniu pop-up apare (aşa cum se vede mai jos), care afişează opțiunile setării de confidențialitate.
  - Dă click pe cercul adecvat.



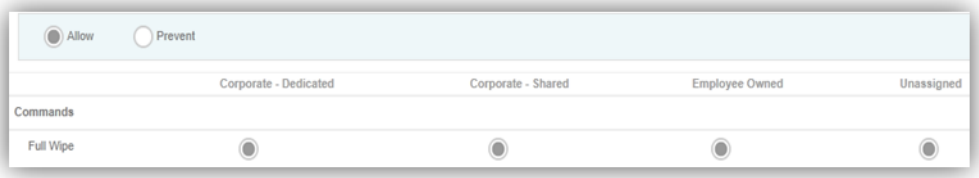
- Dă click pe **Salvare** pentru a termina procesul şi a aplica imediat setările.

8.1.3 Comenzi de confidențialitate

În plus, secțiunea **Comenzi** din partea de jos a paginii permite Administratorului să restricționeze anumite comenzi în funcție de tipul de proprietate asupra dispozitivului.

- Un cerc complet indică faptul că o comandă este acceptată, în timp ce un cerc gol indică faptul că o comandă este dezactivată.

- În prezent, singura comandă care poate fi acceptată sau dezactivată este **Ştergere completă**.
- Dă click pe cercul corespunzător pentru a alege permisiunile dorite.



- Dă click pe **Salvare** pentru a termina procesul şi a aplica imediat setările.

Notă privind setările de confidențialitate: Setările de confidențialitate explicate afectează dacă dispozitivul şi informațiile utilizatorului sunt afişate atât în VSDM cât şi în Portalul Self-Service. Te rugăm să fii conştient de setările de confidențialitate atunci când navighezi prin informațiile utilizatorilor şi dispozitivelor (în special paginile explicate în următoarele secțiuni: Informații dispozitiv, Detalii dispozitiv, Acțiuni de la distanță şi Gestionarea detaliilor dispozitivului)

Multe din setările portalului Self-Service şi setările de Ştergere a dispozitivului sunt determinate atât de setările de a confidențialitate şi setările de rol (**Utilizatori → Conturi administrative**). Dacă mai multe setări sunt în vigoare, politica cea mai strictă se va aplica.

Cele mai bune practici

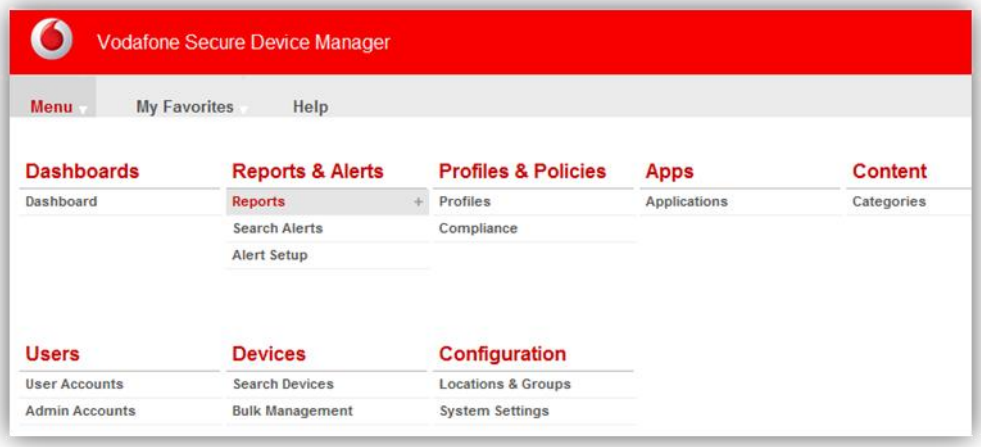
- Pentru a oferi securitate maximă şi protecție a datelor atât pentru utilizatorii finali cât şi companie, setările de confidențialitate lucrează în colaborare cu Configurarea rolului. Pentru a ne asigura că setările de confidențialitate sunt configurate corect implementate, este recomandat să faci o notă cu privire la următoarele setări de rol:
  - **Setări rol utilizator** (**Utilizatori→Conturi utilizator→Roluri**) controlează afişarea datelor despre utilizator şi ale dispozitivului în portalul Self-Service.
  - **Setări de rol administrator** (**Utilizatori→Conturi administrative→Roluri**) controlează afişajul datelor despre utilizator şi dispozitiv, în Consola VSDM Admin, şi controlează abilitatea de a efectua o ştergere completă a dispozitivului.
- Fii consecvent atunci când implementezi mai multe politici de conformitate sau codul de trecere; dacă mai multe politici sunt implementate, cea mai restrictivă politică este pusă în aplicare.
- Pentru o vizualizare a statutului dispozitivului compromis, codul de acces şi politica de criptare, navighează la **Borduri→Bord**) şi selectați **Conformitatea dispozitivului** din **Ecrane disponibile**.
- Pentru a gestiona mai eficient conturile de e-mail în grup, utilizează ori de câte ori este posibil valorile de căutare.
- Pentru securitatea maximă a Emailului, foloseş te profilurile de Email în conjuncție cu **Vodafone Secure Email Gateway**.

9.0 Rapoarte şi alerte

Rapoarte

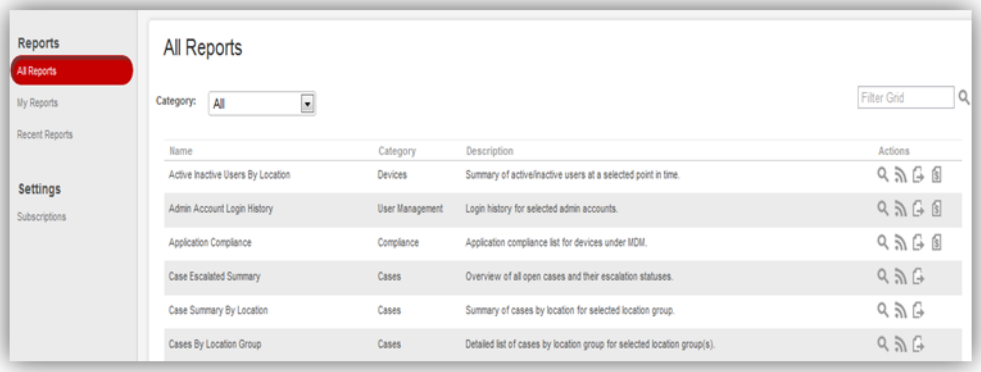
Vodafone Secure Device Manager are capabilități extinse de raportare care oferă administratorilor statistici cu rezultate eficiente cu privire la flotele lor de dispozitive. Administratorii IT pot să utilizeze aceste rapoarte pre-definite sau să creeze rapoarte personalizate bazate pe dispozitive specifice, grupuri de utilizatori, intervale de timp sau preferințe de fișiere. În plus, administratorul poate programa oricare din aceste rapoarte pentru a fi distribuite automat unui grup de utilizatori şi beneficiari, fie pe baza unui program stabilit sau în mod recurent. Aceste caracteristici sunt centralizate în cadrul VSDM. Pentru a accesa pagina de Rapoarte:

- Navighează la **Rapoarte & Alerte→Rapoarte**.



De aici, există mai multe piese cheie privind funcționalitatea pe care administratorii le pot utiliza pentru capabilitățile de raportare VSDM:

- Generarea de rapoarte personalizate
- Crearea de abonamente la rapoarte
- Adăugarea unui raport la Rapoartele mele
- Instrumente suplimentare de raportare



9.1.1 Generarea rapoartelor

Administratorii pot crea rapoarte personalizate în timp ce lucrează în VSDM. Pentru a genera un raport personalizat:

- Navighează la pagina Rapoarte la **Rapoarte & Alerte** → **Rapoarte**.
- Selectează un şablon de raportare predefinit din listă şi apoi dă click pe **Vizualizare** .
- Specifică toți parametrii de raportare. Câmpurile obligatorii sunt marcate cu un semn roşu .
- Selectează View Report.

9.1.2 Adăugarea unui raport la Rapoartele mele

Adăugarea unui raport la Rapoartele mele permite administratorilor să "marcheze", rapoarte populare pe care le consideră deosebit de utile. Pentru a adăuga un raport la Rapoartele mele:

- Navighează la pagina Rapoarte din Rapoarte & Alerte → Rapoarte.
- Selectează un şablon de raportare predefinit din listă şi apoi dă click pe **Adăugare la Rapoartele mele** .
- De acum, raportul este accesibil de la **Ecranul Rapoartele mele** din partea stânga a paginii cu **Rapoarte** pentru acces rapid.

9.1.3 Crearea de abonamente la rapoarte

1. Abonamentele raport pot fi folosite pentru a trimite rapoarte personalizate către destinatari specifici, la un eveniment programat. Pentru a subscrie la un raport:
2. Navighează la pagina Rapoarte din **Rapoarte & Alerte** →**Rapoarte**.
3. Selectează un şablon de raportare predefinit din listă şi apoi dă click pe **Abonare** .
4. Completează formularul de Abonament la rapoarte cu toate informațiile necesare.

- **Informații generale** – Denumirea abonamentului, subiectul e-mailului etc.
- **Parametrii de raportare** – Parametrii care definesc domeniul de aplicare şi opțiunile raportului
- **Lista de distribuție** – Receptorii care primesc raportul personalizat ori de câte ori abonamentul este executat.
- **Program de execuție** – Timpul şi programul la care raportul personalizat este generat.

- Dă click pe **Salvare**.

9.1.4 Instrumente suplimentare de raportare

1. Există, de asemenea, multe alte instrumente suplimentare care ajută administratorii să utilizeze capabilitățile de raportare ale Vodafone:
2. **Instrumente de asistență căutare** – Caseta derulantă **Categorie raport** şi caseta **Căutare** din partea de sus a paginii fac ca găsirea anumitor rapoarte să fie foarte simplă.
3. **Instrument raport eşantion**– Pentru a vizualiza rezultatul unui anumit raport, dă click pe **Eşantion** .
4. **Instrument de exportare raport** – Pentru a exporta un raport într-unul din multele formate, utilizează Bara de export pentru un raport generat în mod personalizat. Excel Export

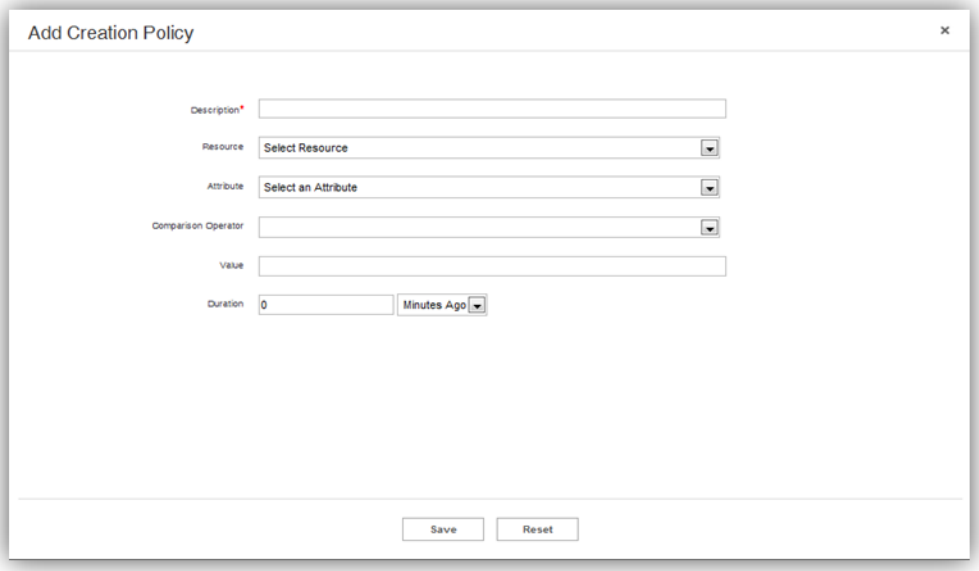
Alerte

Alertele oferă administratorilor posibilitatea de a primi notificări imediate atunci când apar evenimente specifice pentru întregul grup de dispozitive smart. Acestea se cuprind în două componente,

- O **Politică de creare** care descrie criteriile care trebuie îndeplinite pentru a declanşa alerta.
- O **Politică de rutare** care descrie ce dispozitive sunt monitorizate, când şi cine primeşte alerta.

9.1.5 Politici de creare

1. Pentru crearea unei noi politici de creare:
2. Navighează la **Rapoarte & Alerte** → **Setare alertă** → **Politică de creare**
3. De aici, pot fi vizualizate o listă a tuturor politicilor de creație disponibile.
4. În cazul în care orice politici sunt similare cu politica care trebuie să fie creată, încercați **editarea** politicii prin selectarea pictogramei  din stânga rândului.
5. Selectează Adăugare Politică de creare a alertei în partea de jos pentru a deschide formularul politicii de creare a alertei.
6. Introdu toate informațiile cerute.

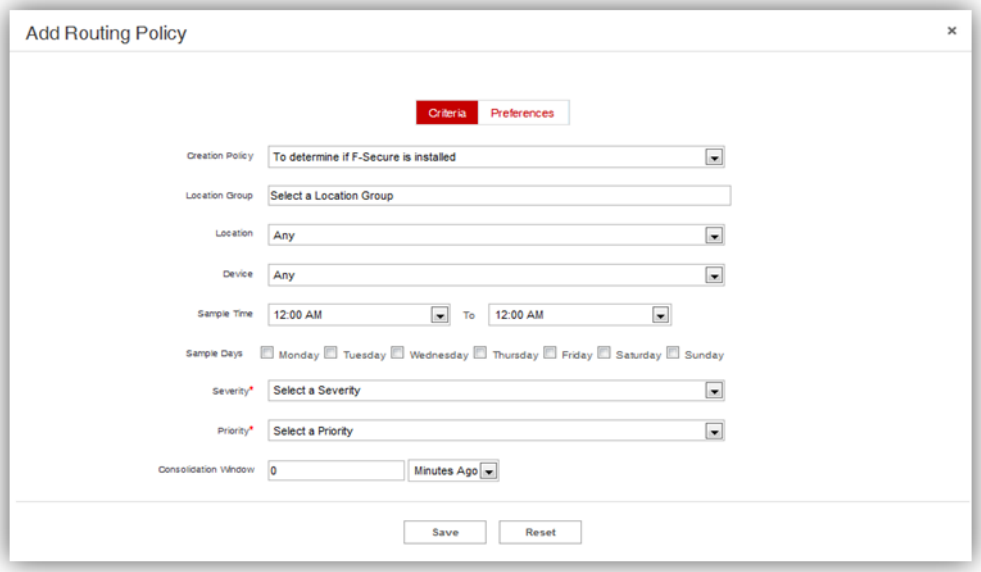


- **Descriere**–Numele politicii de creare care este afişat în Consola de administrare VSDM.
- **Resurse** – Tipul de resurse care vor fi configurate. Selectați **dispozitiv** pentru a monitoriza grupul de dispozitive smart.
- **Atribut** – Parametrul care este utilizat pentru a determina dacă alertă ar trebui să e declanşeze sau nu.
- **Operator comparație** – Operatorul comparației pentru a testa dacă atributul declanşează o alertă.
- **Valoare** – Valoarea care se declanşează când **(Atributul) <Operator comparație> (Valoare) = Adevărat**
- **Durata** – Durata alertei înainte de ultima oprire.

▶ Selectează **Salvare** pentru a finaliza procesul.

9.1.6 Politici de rutare

1. Pentru a acrea o politică de rutare:
2. Navighează la **Rapoarte & Alerte** → **Setare alertă** → **Politică de rutare**
3. Selectează **Adăugare politică de rutare** pentru a deschide formularul **Politică alertă de rutare**.
4. Introdu toate informațiile cerute.



- **Politica de creare** – Politica de crearea care declanşează această alertă.
- **Grupul de locație** – Grupul de locație care conține dispozitivele care sunt monitorizate pentru criteriile politicii de creare.
- **Locație** – Locația care conține dispozitivele care sunt monitorizate pentru criteriile de creare a politicii. Valoarea implicită este **Oricare**.
- **Echipament** – Orice echipament specific care este monitorizat pentru această politică de creare. Valoarea implicită este **Oricare**.
- **Dispozitiv** – Orice dispozitiv specific care este monitorizat pentru această politică de creare. Valoarea implicită este **Oricare**.
- **Exemplu de timp şi zile** – Data şi ora în care această politică este testată pe dispozitivele selectate.
- **Severitate & Prioritate**- Indicatori pentru organizarea alertelor în termeni de prioritate şi pentru mai multe scopuri administrative.
- **Fereastra de consolidare** – Perioada de timp în care doar o alertă are loc de la multipli declanşatori din aceeaşi politică de creare. Toate alertele care apar în fereastra de consolidare a unuia sau şi rezultă din aceeaşi politică de creare şi rutare sunt consolidate într-o singură alertă.
- **Politica de rutare** – Poate fi rutată numai pentru utilizatori. Selectați **Distribuția utilizatorilor**.
- **Alertare rol** – Selectați **Adăugare rol** şi introduceți un rol şi un grup de locație, astfel ca orice administrator cu combinația rol listat / grup de locație să primească această alertă.
- **Alertare utilizator** – Selectați **Adăugare utilizator** şi introduceți un utilizator din admin. Aceasta permite ca administratorul să primească alerta.

▶ Selectează **Salvare** pentru a finaliza procesul.

9.1.7 Vizualizarea alertelor

Odată ce alertele au fost create, ele pot fi vizualizate la:

- **Alertele mele** – Vizualizare alerte în funcție de utilizator sau rol care a primit alerta.
- Pagina **Detalii dispozitiv**– Vizualizare alerte în funcție de dispozitivul care a declanşat alerta.

Cele mai bune practici

- Pentru a permite cel mai înalt nivel de control şi securitate asupra distribuției rapoartelor de informare în întreaga companie, editați accesul pe bază de rol bazat navigând la **Utilizatori→Conturi utilizatori→Adăugare rol**. Accesul la raport este activat sau dezactivat prin bifarea casetelor din **Categorii resurse**.

10.0 Integrare Enterprise

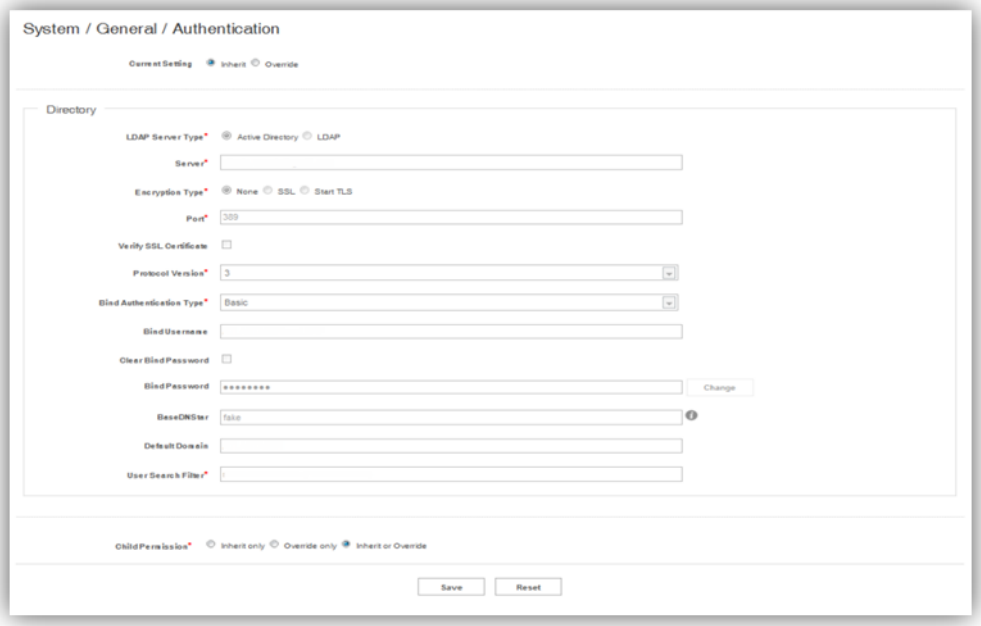
Vodafone Secure Device Manager are capabilități extinse de a ajuta corporațiile să integreze cu uşurință soluția Vodafone în sisteme de tip enterprise existente. Integrarea enterprise Vodafone permite utilizatorilor să se autentifice utilizând acreditările serviciului director enterprise şi oferă o integrare mai profundă în sisteme de tip enterprise, prin utilizarea de API-uri de gestionare a dispozitivului. Aceste API-uri pot fi integrate în aplicații ale terților sau aplicații interne pentru un nivel suplimentar de securitate şi management.

Integrare Lightweight Directory Access Protocol (LDAP) şi Directorului activ (AD)

10.1.1 Autentificarea sistemului

Pagina de **Autentificare** permite integrarea serverului Vodafone într-un server corporativ de servicii de tip director, pentru a oferi acces administratorului la contul pe bază. La crearea conturilor de utilizator, setările pot fi identice sau diferite (explicate în secțiunea următoare). Pentru a configura LDAP sau integrarea AD:

- Navighează la **Configurare→Setări sistem→Sistem→General→Autentificare**.



Câmpurile de autentificare ale sistemului sunt după cum urmează:

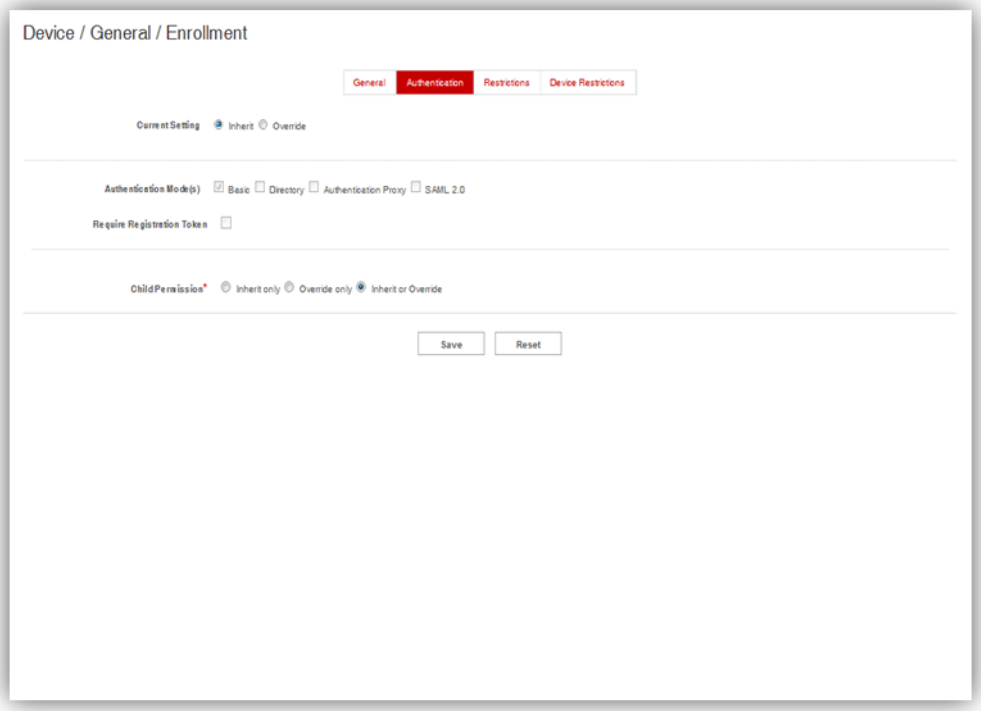
- **Tip Server LDAP** – Selectează LDAP pentru orice tip de server, altul decât Directorul activ.
- **Server** – Introdu adresa serverului serviciilor directoare.
- **Criptare Tip** – Selectează tipul de criptare utilizat pentru comunicarea serviciilor de tip. Valoarea implicită este **Oricare**.
- **Portul** – Introdu portul TCP folosit pentru a comunica cu serverul serviciilor de tip de director. Valoarea implicită pentru comunicarea DS necriptată este 389. Numai mediile SaaS permit traficul SSL criptat folosind portul 636 (gama IP SaaS Vodafone) 205.139.50.0 /23).
- **Verificare SSL Certificat** – Selectează caseta pentru a primi erori SSL atunci când tipul de criptare este Niciunul.
- **Protocol Versiune** – Selectează versiunea protocolului LDAP în uz. Directorul activ foloseşte versiunile LDAP 2 sau 3.

- **Tip autentificare "Bind"** – Selectează tipul de autentificare bind, care este utilizat pentru ca serverul Vodafone să comunice cu serverul serviciilor de director.
- **Nume utilizator & parola Bind** - Introdu acreditările pentru autentificarea cu serverul director. Acest cont permite permisiunea de acces read pe serverul tău director şi leagă conexiunea atunci când autentifică utilizatorii.
- **Baza DN** – Utilizează acest domeniu, ca un test de conectare şi selectează una din căile de bază ale serverului director.
- **Domeniu implicit** – Domeniul implicit pentru toate conturile de utilizator pe bază de director. Dacă numai un singur domeniu este folosit pentru toate conturile de utilizator director, completează câmpul cu domeniul astfel încât utilizatorii să fie autentificați fără a-şi preciza în mod explicit domeniul.
- **Filtru căutare utilizatori** – Introdu parametrul de căutare utilizat pentru a asocia conturile de utilizator cu conturile director. Formatul recomandat este <LDAPUserIdentifier>={EnrollmentUser} unde <LDAPUserIdentifier> este parametrul utilizat pe serverul de servicii director pentru a identifica anumit utilizator.
  - Pentru servere AD , utilizează samAccountName={EnrollmentUser}
  - Pentru servere LDAP, utilizează CN={Enrollment User} or UID={EnrollmentUser}

Conti utilizator & Autentificare dispozitiv

Conturile de utilizator sunt folosite de către utilizatorii finali pentru a asocia dispozitivele la utilizatorii specifici ai companiei. Software-ul Vodafone permite mai multe metode de crearea a conturilor de utilizator, de la un simplu nume de utilizator / combinație de parolă, la integrarea LDAP corporativă prin integrarea cloud şi SAML. .Pentru mai multe informații, consultă tipuri de conturi de utilizator.

Pentru orice cont de utilizator, altul decât autentificarea de bază, VSDM trebuie mai întâi configurat pentru a se integra în mod corespunzător în infrastructura corespunzătoare, înainte ca conturile de utilizator să acceseze tipul de autentificare respectiv. Aceste setări pot fi găsite la pagina **Setări sistem** → **Dispozitiv** →**General** → **Înscriere** din tab-ul **Autentificare** .

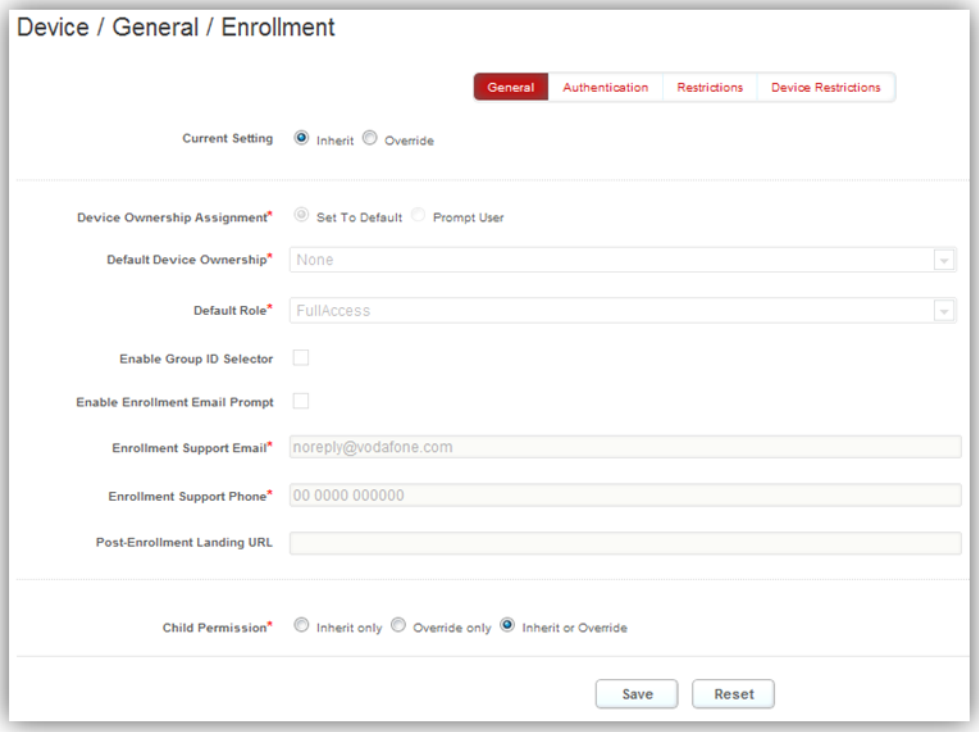


Secțiunea de mai jos descrie modul în care aceste tipuri de autentificare ale conturilor de utilizator pot fi configurate pentru a permite utilizarea fiecărui mecanism de securitate.

10.1.2 Directorul activ / Configurarea înscrierii LDAP

Pentru a activa Directorul activ / conturi de utilizator LDAP pentru utilizarea în timpul înscrierii:

- Asigură-te că sunteți la pagina **Setări sistem** → **Dispozitiv** → **General** → **Înscriere** cu tab-ul **Autentificare** selectat.
- Bifează **Director** pentru a extinde meniul **Autentificare director** şi completează toate domeniile corespunzătoare.



- **Utilizează setările Consolei VSDM Admin** – BIfeaz-o pentru a utiliza setările LDAP care au fost configurate pentru Conturile admin care se loghează în Consola de administrare VSDM. Aceste setări sunt configurate la **Setări sistem -> System -> General -> Autentificare**.
- **Tip Server LDAP** – Selectează LDAP pentru orice tip de server, altul decât Directorul activ.
- **Server** – Introdu adresa serverului serviciilor directoare.
- **Tip criptare** – Tipul de criptare utilizat pentru comunicarea serviciilor de tip director. Valoarea implicită este Niciuna.
- **Port** – Portul TCP folosit pentru a comunica cu serverul serviciilor de tip de director. Valoarea implicită pentru comunicarea DS necriptată este 389.
- **Verificare Certificat SSL** – Debifează această casetă pentru a ignora erorile SSL atunci când tipul de criptare este altul decât niciunul.
- **Versiune protocol** – Versiunea protocolului LDAP care este folosită. Directorul activ foloseşte versiunile LDAP 2 sau 3.
- **Tip autentificare "Bind"** – Selectează tipul de autentificare bind care trebuie să fie utilizat pentru ca serverul Vodafone să comunice cu serverul serviciilor director.
- **Activare DN din Domeniul de utilizator** – Bifează această casetă pentru a activa câmpul DN în serverul serviciilor de tip director din domeniul asociat în contul de utilizator specific AD ce solicită accesul. Dacă tipul de autentificare bind este un nume de utilizator şi o parolă sau anonim, acest domeniu nu are nici un efect.
- **Domeniu implicit** – Domeniul implicit pentru toate conturile de utilizator pe bază de director. Dacă numai un singur domeniu este folosit pentru toate conturile de utilizator director, completează câmpul cu domeniul astfel încât utilizatorii să se poată autentifica fără a-şi preciza în mod explicit domeniul.

- **Setări căutare utilizatori** – Parametrul de căutare utilizat pentru a asocia conturile de utilizator cu conturile director active. Formatul recomandat este **<LDAPUserIdentifier>={EnrollmentUser}** unde <LDAPUserIdentifier> este parametrul care este utilizat în serverul serviciilor director pentru a identifica utilizatorul specific.
- **Căutare Utilizatori LDAP ca utilizatori ai bazei se date** – Selectează pentru a căuta utilizatorii LDAP din lista cu utilizatori ai bazei de date.
- **Utilizare autentificare integrată** – Selectează pentru a utiliza Autentificarea pentru a căuta în baza de date.

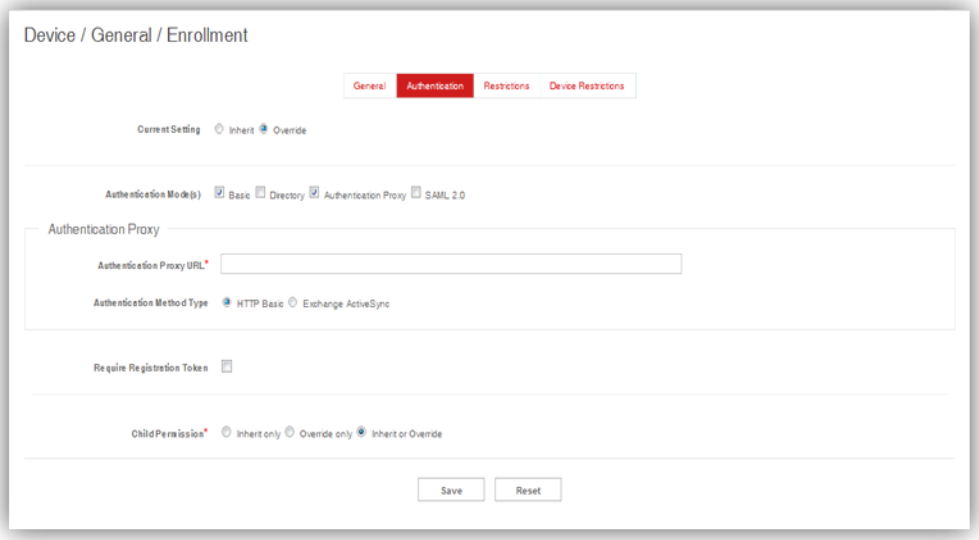
▶ Când ai terminat, dă click pe **Salvare** pentru a salva setările.

10.1.3 Configurare înscriere Proxy de autentificare

Pentru a activa conturile de utilizator pe bază de proxy de autentificare, pentru utilizarea în timpul înscrierii:

▶ Asigură-te că eș ti la pagina **Setări sistem** → **Dispozitiv** → **General** → **Înscriere** cu tab-ul **Autentificare** selectat.

▶ Bifează **Autentificare Proxy** pentru a extinde meniul **Proxy de autentificare**și introdu toate câmpurile corespunzătoare.



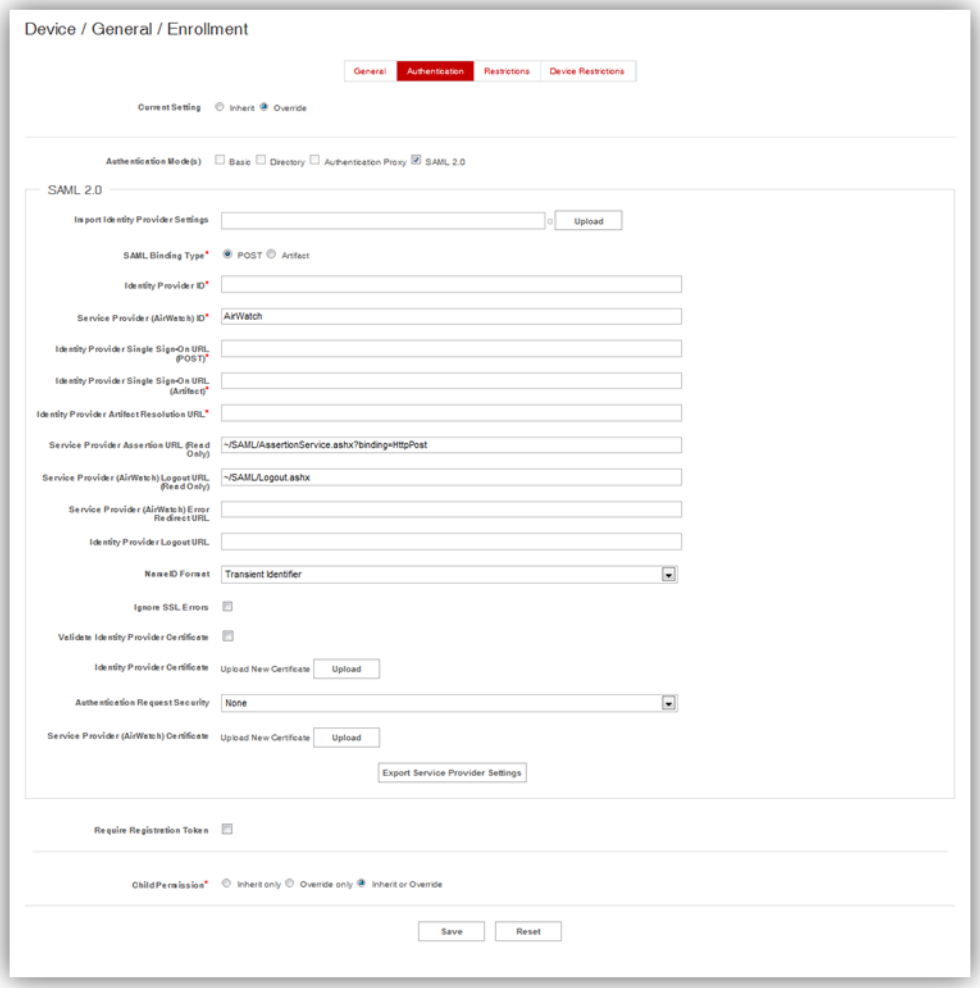
- **URL-ul pentru Proxy de autentificare** – URL-ul serverului proxy de autentificare care solicită utilizatorului autentificarea HTTP EAS.
- **Tip metodă de autentificare** – Tipul de terminal proxy the autentificare. Toate celelalte tipuri de terminale în afară de EAS trebuie să selecteze HTTP de bază.

▶ Când ai terminat, dă click pe **Salvare** pentru a salva setările.

10.1.4 Configurarea de înscriere SAML 2.0

Pentru a activa conturile de utilizator SAML 2.0 pentru utilizarea în timpul înscrierii:

- Asigură-te că eș ti la pagina **Setări sistem** → **Dispozitiv** → **General** → **Înscriere** cu tab-ul **Autentificare** selectat.
- Bifează **SAML 2.0** pentru a extinde meniul **SAML 2.0** şi completează toate câmpurile corespunzătoare.



- **Import Setări Furnizor Identitate** – Această caracteristică permite administratorului să importe metadate SAML obținute de la Furnizorul de identitate.
  - Încărcarea acestui fişier XML stabileşte unele dintre opțiunile de configurare afişate în pagina de setări SAML, şi, ceea ce este mai important, acest fişier include certificatul furnizorului de identitate care este necesar pentru ca Vodafone să aibă încredere în furnizorul de identitate.
- **Tipul obligatoriu SAML** – Această valoare determină modul în care furnizorul de identitate şi Vodafone fac schimb de mesaje.
  - SAML poate fi configurat pentru a permite browser-ului intermediar să POSTEZE întregul mesaj sau să trimită doar un simbol cunoscut ca un artefact care reprezintă datele, după care furnizorul de identitate contactează expeditorul pentru a obține mesajul printr-un proces numit rezoluție artefact.
- **ID-ul Furnizorului de identitate -** Această valoare specifică un URL pe care furnizorul de identitate îl foloseste pentru a se identifica. Vodafone verifică răspunsurile de autentificare pentru a verifica că identitatea corespunde cu ID-ul furnizat aici.
- **ID-ul Furnizorului de servicii -** Această valoare specifică URL cu care Vodafone se identifică la furnizorul de identitate. Această valoare trebuie să se potrivească cu ID-ul care a fost configurat ca real de către furnizorul de identitate.

- **Post/Artefact IDP SSO** - Aceste valori specifică URL-urile furnizorului de identitate pe care Vodafone le foloseste pentru a trimite cereri pentru fiecare tip obligatoriu. Această valoare este stabilită în mod automat din metadatele importate.
- **URL Rezoluție Artefact IDP** - Această valoare specifică URL-ul de la furnizorul de identitate pe care Vodafone îl utilizează pentru a rezolva un răspuns artefact pentru a obține un mesaj de răspuns real. Această valoare este stabilită în mod automat din metadatele importate.
- **URL-ul de aserțiune al Furnizorului de servicii** - Această valoare specifică URL-ul Vodafone care ar trebui configurat de către furnizorul de identitate pentru a direcționa răspunsurile sale de autentificare. "Aserțiunile" privitoare la utilizatorul autentificat sunt incluse în răspunsurile de succes de la furnizorul de identitate.
- **URL-ul de delogare al Furnizorului de servicii** - Această valoare specifică o adresă URL a Vodafone ce trebuie utilizată pentru o singură delogare. Această caracteristică nu este susținută în prezent de Vodafone 5.16.
- **URL eroare al Furnizorului de servicii** - Această valoare specifică o adresă URL a Vodafone pentru afişarea unei erori în procesul de autentificare SAML. Această valoare poate fi lăsată necompletată.
- **URL-ul de delogare al Furnizorului de identitate** - Această valoare specifică o adresă URL a furnizorului de identitate pentru a fi utilizată pentru o singură delogare. Această caracteristică nu este susținută în prezent de Vodafone 5.16. Această valoare este stabilită în mod automat din metadatele importate.
- **Formatul NumeID** - Această valoare specifică formatul în care furnizorul de identitate trebuie să trimită un NumeID pentru un utilizator autentificat. Această valoare nu este necesară dacă Vodafone obține numele de utilizator de atributul necesar "UID" NumePrietenos.
- **Ignorare Erori SSL** - Această valoare specifică dacă Vodafone trebuie să verifice sau nu încrederea SSL pentru furnizorul de identitate. Dacă erorile SSL sunt ignorate, Vodafone comunică cu furnizorul de identitate indiferent de problemele de încredere SSL.
- **Validare Certificat Furnizor de Identitate** - Această valoare specifică dacă Vodafone ar trebui să verifice sau nu dacă răspunsurile de autentificare sunt semnate cu certificatul furnizorului de identitate. Această valoare este necesară doar atunci când se utilizează POST deoarece furnizorul de identitate nu poate semna răspunsurile folosind răspunsuri artefact.
- **Certificatul Furnizorului de Identitate** - Certificatul public al furnizorului de identitate. Această valoare este stabilită în mod automat din metadatele importate.
- **Securitatea cererii de autentificare** - Această valoare specifică dacă Vodafone ar trebui sau nu să semneze mesajele de solicitare a autentificării. Această valoare trebuie setată pentru a încărca un certificat al furnizorului de servicii.
- **Certificat Furnizor de servicii** - Un certificat privat folosit de Vodafone pentru a semna cererile SAML şi pentru a decripta răspunsurile.
- **Setări Export Furnizor de Servicii** - Această caracteristică permite metadatelor SAML ale Vodafone să fie exportate pentru a fi furnizate furnizorului de identitate. Similar cu "Setările de Import ale furnizorului de identitate", această caracteristică permite furnizorului de identitate să importe metadatele Vodafone SAML pentru a consolida încrederea.

▶ Când ai terminat, dă click pe **Salvare** pentru a salva setările.

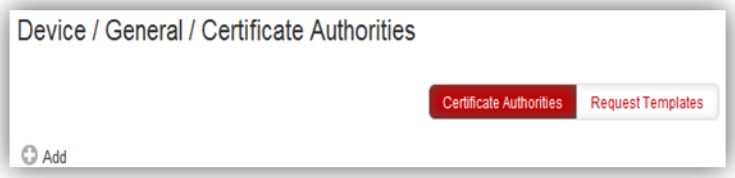
Integrarea infrastructurii certificatelor

Managerul Secure Device Manager se poate integra cu infrastructura de certificare într-un mod care permite Enterprise să distribuie certificate în scopuri de autentificare dispozitivelor care conțin date corporative. Există mai multe opțiuni pentru integrarea infrastructurii de certificare Vodafone, dar fiecare necesită informații tehnice detaliate şi, prin urmare, este foarte important ca administratorul infrastructurii de Certificare să fie implicat în această integrare.

Există două moduri principale în care se integrează Vodafone:

- Integrarea prin Autoritatea de Certificare Directă(**CA**).
  - Vodafone poate acționa ca proxy pentru distribuția certificatului.
- Integrarea prin Protocolul Simplu de Înscriere a Certificatului (**SCEP**).
  - Vodafone poate acționa ca proxy pentru distribuția certificatului.
  - Poate fi autentificat din dispozitiv.

- Navighează la setările de Autorități certificare selectând **Configurare**→ **Setări sistem**→ **Dispozitiv**→ **General** → **Autorități de certificare**.



- Pagina **Autorități de certificare** permite serverului Vodafone să se integreze în Microsoft CA, Vodafone CA sau serverele serviciilor de certificare. Indiferent de tipul de integrare, există două măsurile necesare pentru a configura integrarea certificatului:

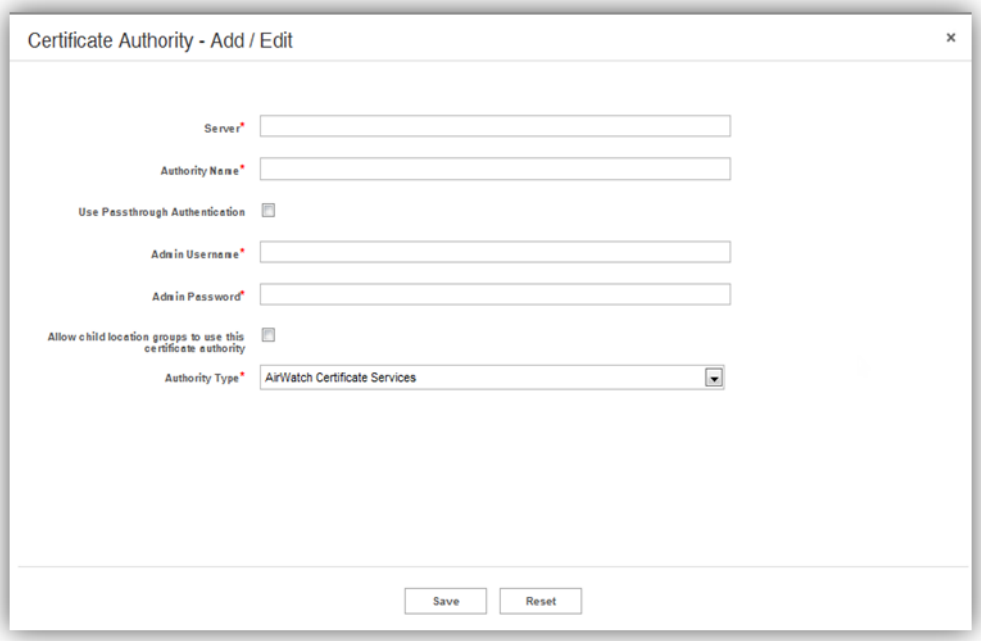
- Configurarea Autorității de certificare.
- Configurarea Şablonului de certificare.

10.1.5 Integrarea autorității certificării directe

Pentru a configura integrarea Vodafone în serverul serviciilor Autorității de certificare directe CA), mai întâi configurează Autoritatea de certificare şi apoi configurează Şablonul de certificare.

CA: Configurarea Autorității de certificare

- În primul rând, configurează Autoritatea de certificare în Vodafone. Pe pagina Autorităților de certificare, selectează Add pentru a deschide Formularul Autorității de certificare.
- Completează câmpurile necesare:



- **Server** – Adresa serverului pentru Serverul CA. Serverul CA trebuie să fie în format IP sau nume de domeniu (mycompany.local.com).
- **Numele autorității** –Se referă la numele real al instanței CA pe serverul CA.
- **Folosire autentificare suplimentară** –Autentificarea suplimentară foloseste contul de serviciu care rulează Vodafone pentru autentificarea în serverul CA.
  - Această setare ar trebui ignorată, în afara excepția cazului în care serverul Vodafone este pe acelaşi domeniu ca şi CA enterprise şi contul de serviciu ce rulează Vodafone este un administrator de domeniu.
- **Nume utilizator Admin & Parolă** –Numele de utilizator şi parola pentru autentificarea în serverul CA. Numele de utilizator şi parola trebuie să aibă permisiunile corecte pe serverul CA pentru modelul certificatului ce este utilizat.
- **Permisiune grupuri de locație copil de a folosi această autoritate de certificare** –Selecteaza caseta de validare pentru a permite moştenirea de către grupuri de locație copil.
- **Tip autoritate** –Tipul de autoritate de certificare. Pentru integrare CA Directă, alege între:
  - **Servicii de certificare Microsoft**–Acceptă o autoritate de certificare Microsoft pe un server Windows 2003/2008

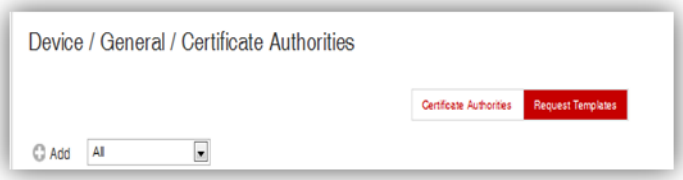
    SAU
  - **Servicii de certificare Vodafone** –Acceptă un serviciu de certifcare instalat de Vodafone sau CA Generic (care acceptă protocolul CA standard)

- Dă click pe **Salvare**. Apoi, configureaza Şablonul de certificare CA.

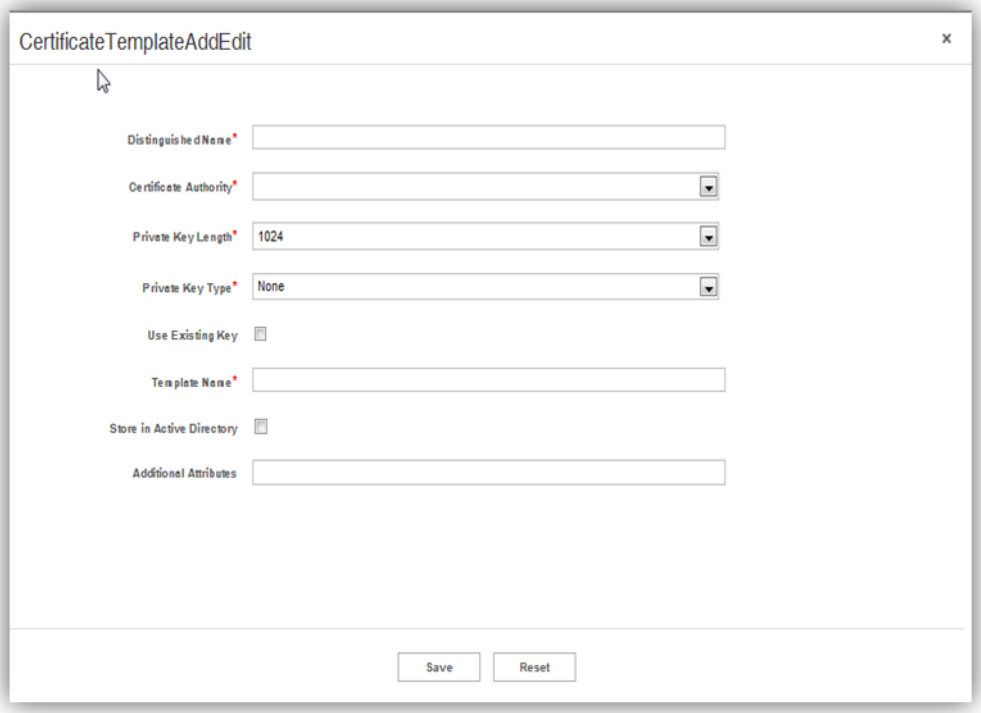
CA: Configurarea Şablonului de certificare

După ce Autoritatea de certificare este configurată, configureaza Şablonul certificatului, astfel încât Vodafone să poată solicita un certificat de la Autoritatea de certificare. Pentru a configura un Şablon de certificare pentru integrarea directă a autorității de certificare:

- Dă click pe **Solicitare şabloane**:



- Selectează Add pentru a deschide Formularul Şablon al certificatului.
- Completează câmpurile necesare.



- **Numele evidențiat** –Numele complet calificat evidențiat al certificatului. Acest domeniu acceptă valorile de căutare utilizate în Vodafone, astfel încât numele certificatului poate fi unic pentru fiecare utilizator / dispozitive Vodafone (de exemplu, CN = {UtilizatorÎnscriere}).
- Numele evidențiat acceptă atât formatul Crypto API cât şi Netscape. Singurul câmp necesar pentru a crea un certificat este Denumirea comună (CN). Numele evidențiat trebuie să reflecte ce anume autentifică certificatul.
- **Autoritatea de certificare** –Specifică CA că acest şablon este atribuit în Vodafone.
- **Lungime cheie privată** – Lungimea cheii private trebuie să se potrivească cu lungimea cheii private pe şablonul utilizat pe CA.
  - Notă de compatibilitate: Lungimile mai scurte sunt compatibile cu tehnologia mai veche şi sistemele de operare.
- **Tip cheie privată** – Stabileşte tipul de cheie privată în integrare directă CA.
  - Setarea standard este “Semnare & Criptare”.

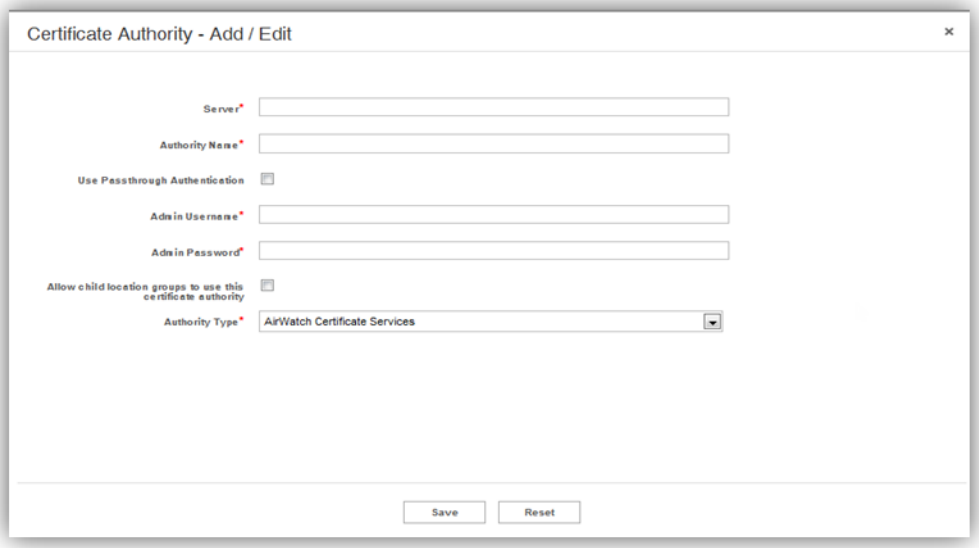
- **Folosire cheie existentă** –Activează această opțiune pentru a utiliza cheia privată existentă, mai degrabă decât a crea una nouă. Şablonul CA şi Certificatul trebuie să accepte această opțiune pentru a funcționa.
- **Nume şablon** –Introdu un nume de şablon astfel încât acest şablon de certificat să poată fi utilizat în viitor. Numai numele şablonului este utilizat în cadrul VSDM.
- **Stocare în directorul activ** –Activează această opțiune pentru a încerca să stochezi certificatul generat în AD pe baza Numelui comun ales în Numele evidențiat.
  - De exemplu, dacă CN=ADUser, Software-ul Vodafone încearcă să stocheze certificatul în ADUser.
  - Pentru a utiliza această opțiune, Vodafone trebuie să fie parte a domeniului tau iar contul de serviciu care rulează Vodafone să fie un administrator de domeniu.
- **Atribute suplimentare** –Acest câmp serveşte pentru două scopuri atunci când configurăm Autoritatea de certificare:
  - În primul rând, câmpul cu Atribute suplimentare specifică Şablonul Certificatului în Autoritatea de certificare. Utilizează ŞablonCertificat pentru a specifica ce şablon să foloseș te (de exemplu, introdu Şablon Certificat:*NumeŞablon* unde *NumeŞablon* este numele şablonului pe care doreşti să îl folosiți).
  - În al doilea rând, Atribute suplimentare îți permite să adaugi atribute suplimentare relevante.
  - Când introduci atributele suplimentare, separă-le de ŞablonulCertificatului cu o bară verticală şi n (*n*). Un exemplu de atribut suplimentar ar fi Numele alternativă al subiectului pentru certificat. Pentru a specifica Numele alternativa al subiectului, vei stabili câmpul de Atribute suplimentare la: CertificateTemplate:*TemplateName*\nSAN:Email Address={EmailAddress}.

10.1.6 Integrarea SCEP

Primul pas în configurarea integrării Vodafone la un server de servicii corporative SCEP este de a configura Autoritatea de certificare. Al doilea pas este configurarea Şablonului certificatului. Pentru configurarea Autorității de certificare:

SCEP: Configurarea Autorității de Certificare

- Selectează Add pentru a deschide un nou **Formular de Autoritate de Certificare** sau selectează (dacă este cazul) pentru a edita un certificat existent.
- Completează câmpurile necesare.



- **URL-ul Serverului** –Adresa Web a URL-ului de înscriere a certificatului. Aceasta este, de obicei, în formatul. EXE sau. DLL, în funcție de furnizorul de SCEP. Mai jos sunt două exemple:
  - Dacă furnizorul SCEP este Microsoft (MSCEP), serverul trebuie să fie https://scepserver.mycompany.com/certsrv/mscep/mscep.dll unde scepserver.mycompany.com este adresa Web a serverului SCEP.
  - Dacă furnizorul SCEP este VeriSign, serverul va trebui setat la https://onsiteipsec.verisign.com/cgi-bin/pkiclient.exe
- **Nume autoritate** –În integrarea SCEP, acest câmp este folosit de Vodafone pentru a evidenția aceste setări.
- **Folosire autentificare suplimentară** –Autentificarea suplimentară foloseste contul de serviciu care rulează Vodafone pentru autentificarea în serverul SCEP. Această setare ar trebui ignorată, în afara excepția cazului în care serverul Vodafone este pe acelaşi domeniu ca şi serverul SCEP şi contul de serviciu ce rulează Vodafone este un administrator de domeniu.
- **Nume utilizator Admin & Parolă** –Numele de utilizator şi parola pentru autentificarea în serverul SCEP. Numele de utilizator şi parola trebuie să aibă permisiunile corecte pe serverul SCEP împreună cu şablonul certificatului ce este folosit pentru autentificare.
- **Permisiune grupuri de locație copii să folosească această autoritate de certificare** –Bifați pentru a permite moştenirea.
- **Tipul de autoritate** –Tipul de autoritate certificat, selectați Protocolul de înscriere certificat simplu (SCEP) din meniul derulant.
- **Încercări maxime în aşteptare** –Numărul maxim de încercări pentru trimiterea cererilor înscriere SCEP. Valoarea standard este 5.
- **Timp expirat pentu încercări** –Determină timpul (în minute) de aşteptare în timpul unei cereri SCEP. Valoarea standard este 30.
- **Tip provocare**–Determină modul în care pagina autentifică URL-ul de înscriere a certificatului.
  - **Provocare statică** este o cheie unică sau parolă care este întotdeauna autentificată cu URL-ul de înscriere al certificatului.
  - **Provocare dinamică** foloseşte Vodafone pentru a extrage o cheie de provocare sau parolă din furnizorul SCEP.

- **Nicio provocare** înseamnă că nicio provocare nu este necesară şi aceasta lucru implică, de obicei, terminale SCEP nesecurizate. Aceasta se aplică în circumstanțe rare.

- **Furnizor SCEP** –Furnizorul SCEP determină restul configurărilor şi ce opțiuni sunt disponibile.

Furnizorul SCEP: MSCEP

Dacă MSCEP este furnizorul SCEP, următoarele opțiuni apar. Reține că unele opțiuni pot varia în funcție de tipul de Provocare selectat.

- Expresia SCEP de provocare (numai provocare statică)- Introdu parola sau cheia furnizate de SCEP.
- Numele de utilizator SCEP este necesar (numai provocare dinamică) - Bifeaza această casetă pentru a solicita adresa Web a Provocării dinamice pentru a solicita autentificarea utilizatorului pentru acces.
- Lungime provocare SCEP (numai provocare dinamică) - Introdu lungimea provocării oferită de furnizorul SCEP.
- URL-ul provocării SCEP (numai provocare dinamică) - Acest câmp trebuie să conțină adresa Web a URL-ului de provocare:

- Pentru MSCEP 2003, URL-ul de provocare este acelaşi ca URL-ul de înscriere Web.
- Pentru MSCEP 2008 URL-ul de provocare este de obicei: https:// *scepserver.mycompany.com*/ certsrv/ mscep_admin/ where *scepserver.mycompany.com* este adresa Web a serverului SCEP (***Notă**: prelungirea / NU este opțională).*

- **Nume utilizator Admin & Parolă SCEP** –Numele de utilizator şi parola pentru autentificarea în URL-ul SCEP. Numele de utilizator şi parola trebuie să aibă permisiuni corecte atât pentru serverul SCEP cât şi şablonul certificatului ce este folosit, pentru autentificare.
- Dă click pe **Salvare**. Acum, configureaza Şablonul certificatului SCEP.

Furnizorul SCEP: VeriSign

Dacă VeriSign este furnizorul SCEP, următoarele opțiuni apar. Reține că unele opțiuni pot varia în funcție de tipul de Provocare selectat.

- Expresia SCEP de provocare (numai provocare statică)- Introduceți parola sau cheia furnizate de SCEP.
- URL- ul codului de acces VeriSign (numai provocare dinamică) –Introduceți URL-ul provocării dinamice. URL-ul ar trebui să arate astfel: https://onsite-admin.verisign.com/OnSiteHome.htm.
- VeriSign DNS Post Fix (numai provocare dinamică) - Introduceți domeniul utilizat pentru înregistrarea contului mPKI relevant.
- De exemplu, dacă domeniul a fost înregistrat cu mycompany.com, introduceți "mycompany.com." în acest domeniu.
- Nume VeriSign Certificat (numai provocare dinamică) - Acest câmp afişează certificatul încărcat folosit pentru a autentificarea cu Cloud VeriSign.
- Fişierul noului certificat şi parola certificatului (numai provocarea dinamică) - Încărcarea unui nou certificat în configurarea SCEP pentru autentificarea cu Cloud VeriSign.

- Dă click pe **Browsw** pentru a încărca un nou fişier.
- Introdu parola certificatului.
- Dă click pe **Salvare**. Acum, configurați Şablonul certificatului SCEP.

Furnizorul SCEP: De bază:

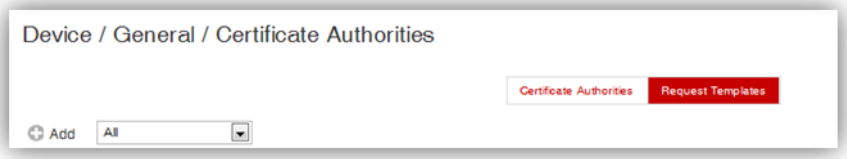
Utilizează opțiunea de bază în cazul în care furnizorul nu este VeriSign sau Microsoft. Pentru ca opțiunea de Bază să fie acceptată, Furnizorul trebuie să permită Provocarea statică (dinamică nu este permisă în starea de bază) şi furnizează protocolul standard. Selectarea opțiunii de Bază necesită următoarele domenii:

- **Fraza provocare SCEP** (numai provocare statică) –Acest câmp trebuie să conțină parola sau cheia furnizate de SCEP.

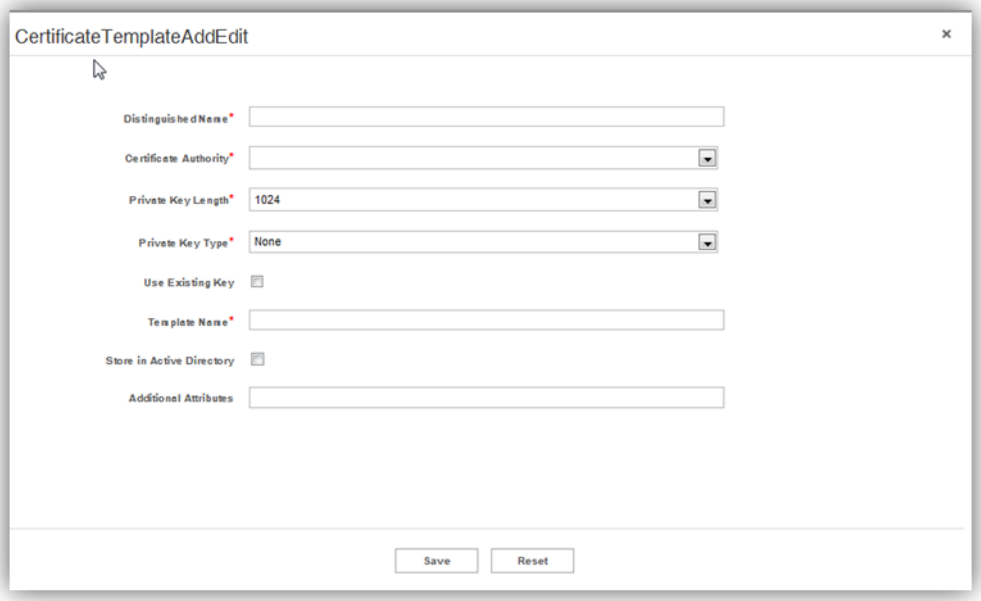
SCEP: Configurarea Şablonului de certificare

După ce Autoritatea de certificare este configurată, configurează Şablonul certificatului, astfel încât Vodafone să poată solicita un certificat de la Autoritatea de certificare.

- Dă click pe **Solicitare şabloane**:



- Selectează Add pentru a deschide formularul **Şablon certificat**.
- Introdu toate informațiile cerute.



- **Numele evidențiat** –Numele complet calificat evidențiat al certificatului. Acest domeniu acceptă valorile de căutare utilizate în Vodafone, astfel încât numele certificatului poate fi unic pentru fiecare utilizator / dispozitive Vodafone (de exemplu, CN = {UtilizatorÎnscriere}).
- Numele evidențiat acceptă atât formatul Crypto API cât şi Netscape. Singurul câmp necesar pentru a crea un certificat este Denumirea comună (CN). Numele evidențiat trebuie să reflecte ce anume autentifică certificatul.
- **Autoritatea de certificare** –Specifică CA că acest şablon este atribuit în Vodafone.
- **Lungime cheie privată** – Lungimea cheii private trebuie să se potrivească cu lungimea cheii private pe şablonul utilizat pe CA.
  - Notă de compatibilitate: Lungimile mai scurte sunt compatibile cu tehnologia mai veche şi sistemele de operare.
- **Tip cheie privată** – Pentru toți furnizorii SCEP, aceasta determină utilizarea cheii private; valoarea implicită este întotdeauna Semnare & Criptare.
  - Pentru o integrare MSCEP, tipul cheii private determină ce şablon este utilizat (specificat în serverul SCEP).
- **Utilizare cheie existentă**–Nu este aplicabil pentru SCEP.
- **Nume şablon** –Introdu un nume de şablon astfel încât acest şablon de certificat să poată fi utilizat în viitor. Numele şablonului este utilizat numai în cadrul VSDM.
- **Stocare în directorul activ** –Activează această opțiune pentru a încerca să stochezi certificatul generat în AD pe baza Numelui comun ales în Numele evidențiat.
  - De exemplu, dacă CN=ADUser, Software-ul Vodafone încearcă să stocheze certificatul în ADUser.
  - Pentru a utiliza această opțiune, Vodafone trebuie să fie parte a domeniului dvs. iar contul de serviciu care rulează Vodafone să fie un administrator de domeniu.

- **Atribute suplimentare** –Câmpul Atribute suplimentare determină atribute suplimentare precum un Nume alternativ Subiect:

  ▶ De exemplu, câmpul Atribute suplimentare poate fi setat la SAN:Alt nume={NumePrincipalUtilizator}.

10.1.7 Utilizarea certificatelor pentru VSDM

După ce autoritatea de certificare şi şabloanele de certificare au fost corect configurate, certificatele pot fi extinse în cadrul Vodafone pentru mai multe scopuri.

Enterprise Wi-Fi, VPN, Autentificarea EAS

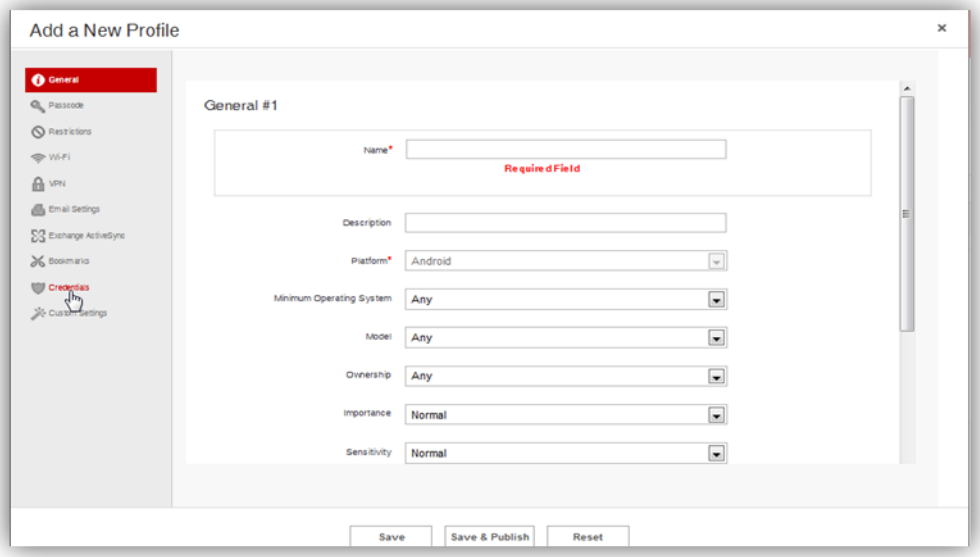
Wi-Fi avansat, VPN şi configurațiile EAS pot acum utiliza certificatele pentru autentificare în locul parolelor simple, pentru a oferi o securitate mai puternică împotriva accesului neautorizat. Vodafone poate distribui automat aceste certificate de autentificare la dispozitive şi poate configura dispozitivul pentru acces Wi-Fi, VPN sau EAS fără nicio interacțiune cu utilizatorul.

O privire de ansamblu asupra procesului este după cum urmează:

▶ Asigură-te că **Autoritatea de certificare** şi **Şabloanele Certificatelor** este configurată corespunzător, apoi crează un profil adecvat pentru platforma ta (iOS sau Android pentru aceste capacități)

- Dacă utilizezi un certificat SSL static care este utilizat pentru toate dispozitivele, poți sări peste acest pas şi încărca certificatul în Vodafone pentru distribuție.

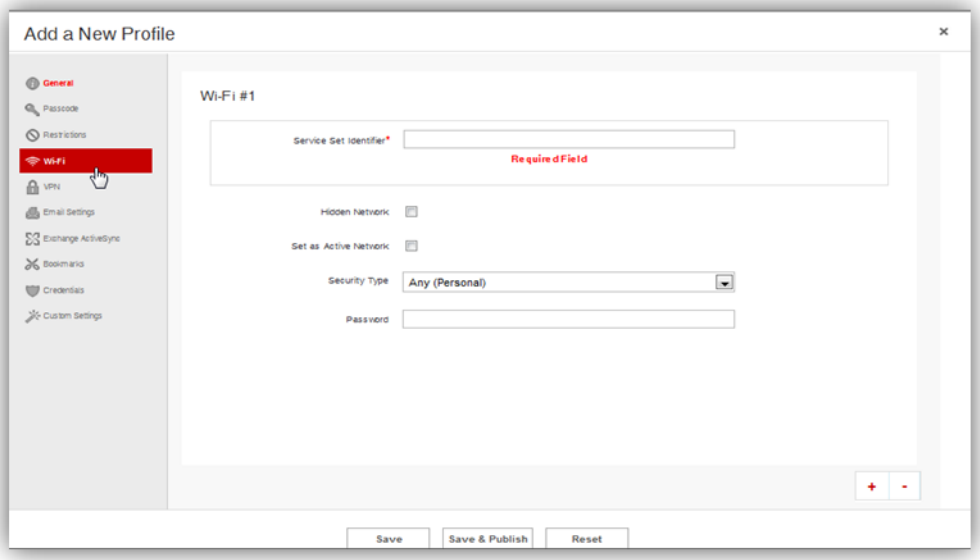
  ▶ Completează toate setările generale de profil şi apoi alege fie **Acreditări**, fie **SCEP** în funcție de tipul de CA ați configurat anterior.



▶ De pe fiecare pagină specifică toți parametrii pentru a selecta certificatul corespunzător pentru a fi utilizat pentru autentificarea Wi-Fi, VPN sau EAS.

- Dacă utilizezi un certificat SSL static care nu depinde de utilizator, alege **Încărcare** ca sursa de acreditare şi încărcă certificatul.
- Dacă generezi certificate pentru fiecare utilizator sau dispozitiv din CA, asigură-te că sursa de acreditare este o **Autoritate de certificare definită** şi alege şablonul adecvat al certificatului.

  ▶ După ce ai terminat setările de Acreditare sau setările profilului SCEP, nu **Salvați şi Publicați**. Selectează o altă sarcină utilă în acest profil pentru **Wi-Fi**, **VPN**, sau **EAS**, în funcție de scopul pentru care este utilizat certificatul.



▶ Specifică toate setările pentru sarcina utilă aleasă. Asigură-te că tipul de autentificare utilizează un certificat şi că certificatul folosit în Acreditări sau profilul SCEP este ales.

- Dacă autentificarea în CA necesită încredere (de obicei, pentru autoritățile de certificare interne),

asigură-te că ai încărcat şi selectat pentru a utiliza un Certificat de autorizare CA Root.

▶ Când ai terminat, dă click pe **Salvare şi Publicare**.

Pentru informații suplimentare sau asistență în configurarea certificatelor în Vodafone Secure Device Manager, contactează organizația locală de asistență Vodafone.

Semnarea şi criptarea S/MIME a emailului

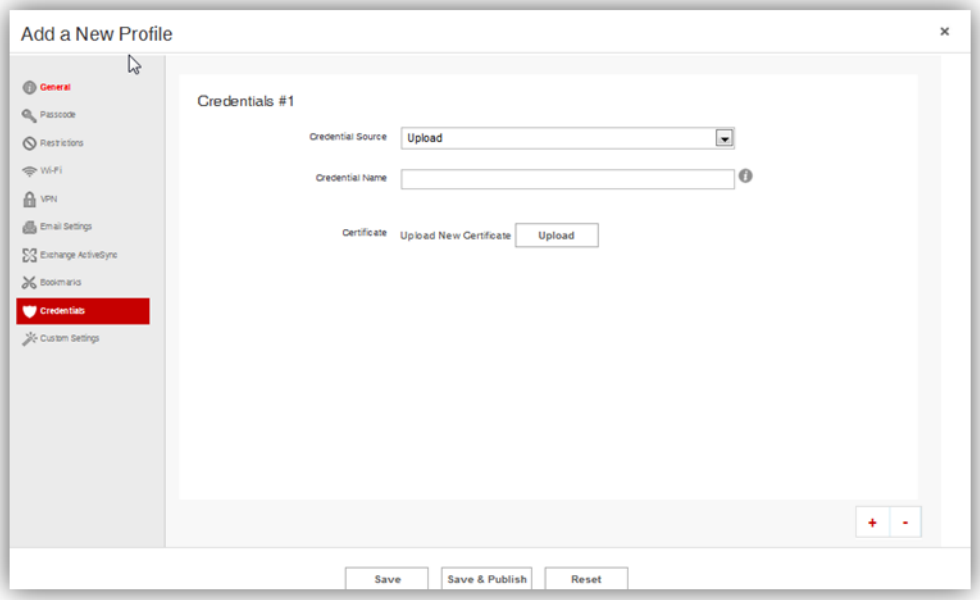
S / MIME este un standard pentru criptarea şi semnarea în cheie publică care a devenit un standard pentru semnarea şi criptarea e-mailului. Vodafone poate distribui în mod automat certificatele şi configura e-mailul sau Exchange ActiveSync pentru a utiliza semnarea şi criptarea S/MIME fără nicio interacțiune cu utilizatorul.

O privire de ansamblu asupra procesului este după cum urmează:

▶ Asigură-te că Autoritatea de certificare şi Şabloanele de certificare sunt configurate corespunzător apoi crează un profil adecvat pentru platforma ta (numai pentru dispozitive iOS5).

- Dacă utilizezi un certificat SSL static care este utilizat pentru toate dispozitivele, poți sări peste acest pas şi încărca certificatul în Vodafone pentru distribuție.

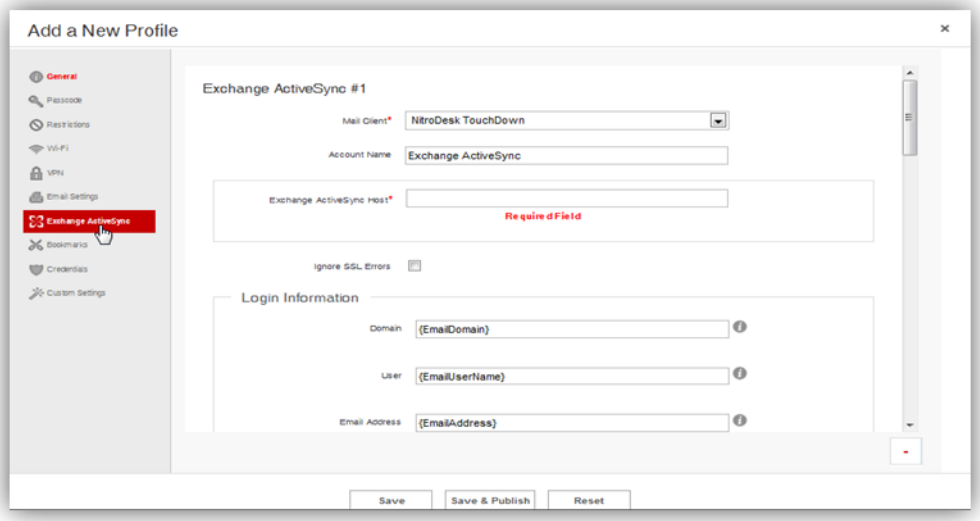
▶ Completează toate setările generale de profil şi apoi alege fie **Acreditări**, fie **SCEP** în funcție de tipul de CA configurat anterior.



▶ De pe fiecare pagină specifică toți parametrii pentru a selecta certificatul corespunzător pentru a fi utilizat pentru semnarea sau criptarea S/MIME.

- Dacă utilizezi un certificat SSL static care nu depinde de utilizator, alege **Încărcare** ca sursa de acreditare şi încărcă certificatul.
- Dacă generezi certificate pentru fiecare utilizator sau dispozitiv din CA, asigură-te că sursa de acreditare este o **Autoritate de certificare definită** şi alege şablonul adecvat al certificatului.

▶ După ce ai terminat setările de Acreditare sau setările profilului SCEP, nu **Salvați şi Publicați**. Selectează o altă sarcină utilă în acest profil pentru **Email**, sau **EAS**, în funcție de tipul infrastructurii emailului.



- Specifică toate setările pentru sarcina utilă aleasă şi asigură-te că ai bifat **Utilizare S/MIME**. De asemenea, asigură-te că certificatul care a selectat acreditările sau sarcina utilă SCEP este utilizat fie pentru semnare, fie pentru criptare, după cum s-a arătat.
- Când ai terminat, dă click pe **Salvare şi Publicare**.

Pentru informații suplimentare sau asistență în configurarea certificatelor cu Vodafone, poți lua legătura cu asistența Vodafone.

Integrarea Emailului

10.1.8 Email (SMTP)

1. Mesajele email trimise din Consola de administrare VSDM sunt transmise prin gateway-ul de e-mail corporativ, definit în setările de e-mail (SMTP), meniul de setări. Utilizatorii pot primi notificări prin e-mail pentru o varietate de motive, inclusiv:

2. Utilizator înscriere & activarea dispozitivului

3. Abonamente rapoarte

4. Mesaje dispozitiv

5. Notificări aplicații cumpărate (VPP)

Pentru a configura setările de Email:

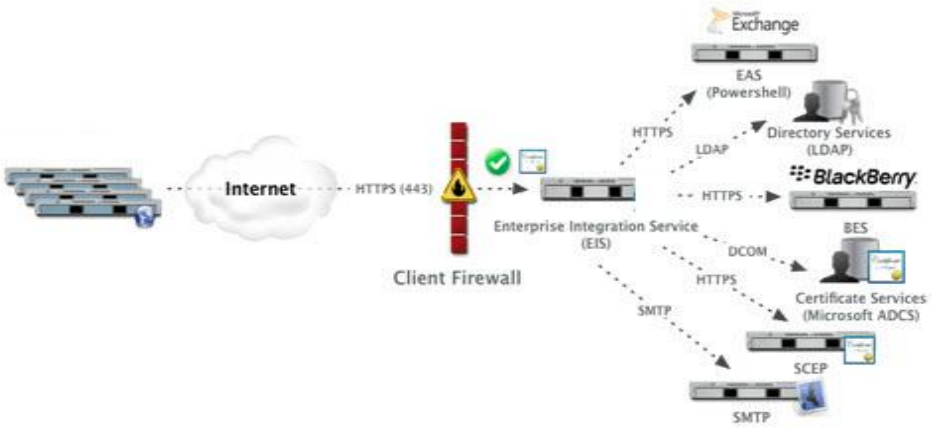
- Navighează la **Configurare→Setări sistem→Sistem→Email** (SMTP).

Următoarele câmpuri trebuie să fie definite în ecranul de setări al Emailului (SMTP):

- **Server** – Adresa serverului pentru Serverul de email corporativ (SMTP).
- **Activare SSL** – Dacă este bifat, serverul de e-mail corporativ comunică în siguranță cu serverul Vodafone prin SSL. Valoarea implicită este falsă (de-bifată).
- **Port** – Portul prin care serverul de e-mail corporativ comunică cu serverul Vodafone. Portul implicit este 25.
- **Necesită acreditări** – Dacă este bifată, traficul SMTP pentru serverul de e-mail corporativ necesită autorizare. Numele de utilizator şi parola nu sunt necesare dacă autorizația nu este activată.
- **Expirare în secunde** – Definită în secunde, această valoare determină timp înainte de expirarea conexiunii dintre serverul de e-mail corporativ şi serverul Vodafone.
- **Numele expeditorului** – Numele expeditorului care este afişata pe toate mesajele trimise din serverul Vodafone.
- **Adresa de email a expeditorului** – Adresa de email a expeditorului care este afişată pe toate mesajele trimise din serverul Vodafone.

Serviciul de Integrare Enterprise

Când foloseș ti Vodafone in the cloud, integrarea în sistemele enterprise poate fi perfect încapsulată în traficul https criptat, retransmis de către unul sau mai multe noduri (releu EIS / terminal EIS).



Aceasta include comunicarea cu:

- SMTP (Releu de Email)
- Servicii directoare (LDAP / AD)
- Servicii de certificare Microsoft (PKI)
- Protocolul Simplu de Înscriere a Certificatului (SCEP PKI).
- Carcasa pentru energie Exchange (Pentru anumite gateway-uri securizate de e-mail)
- BES (Utilizatorii Sync şi informații privind dispozitivele mobile)

Vodafone Secure Device Manager solicită modulului Serviciului de Integrare Enterprise (EIS) să faciliteze integrarea în oricare dintre sistemele de mai sus în spatele firewall-ului companiei fără a fi nevoie de tunele VPN sau de a deschide porturi pentru sistemele dorite.

Notă: Funcționalitatea este o componentă suplimentară care trebuie utilizată în locația clientului şi necesită Servicii profesionale. Disponibilitatea poate varia în funcție de piețele locale.

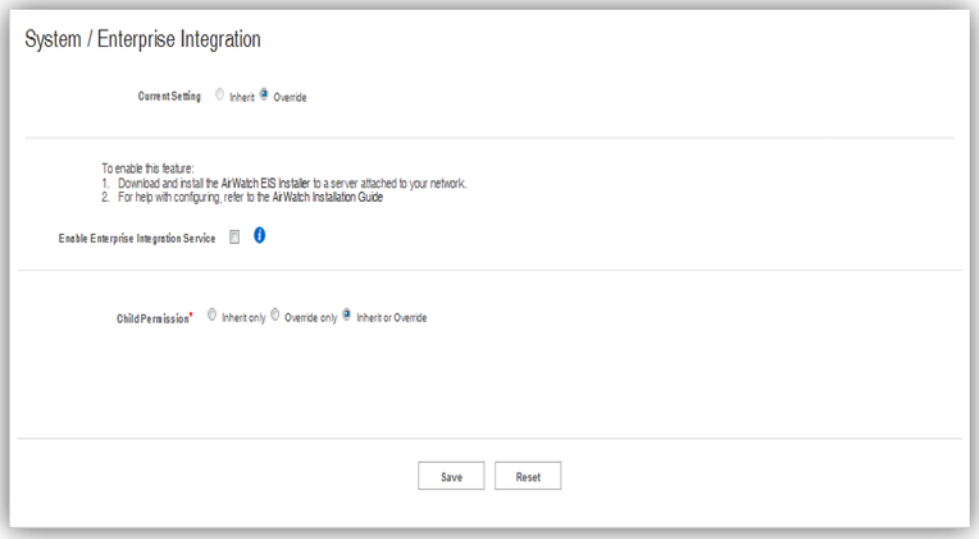
10.1.9 Configurarea EIS

Pentru a configura EIS ai nevoie de:

- Un server accesibil din Vodafone SaaS (permite cereri inbound de la 205.139.50.0 / 23 la portul 443).
- Accesul intern la sisteme pentru a integra (conexiuni configurate în Setările corespunzătoare ale sistemului)
- Un cont de admin pentru EIS. Asigură-te că rolul contului are permisiunea de a "Permite accesul de la distanță" localizat în **Servicii de la distanță→ Securitate.**

Pentru instalare, utilizează fie fişierele disponibile pentru descărcare din pagina **Setări sistem** sau fişierele primite de la suportul Vodafone. Secțiunea de Integrare Enterprise din Setări de sistem este configurată automat în timpul instalării EIS în spatele firewall-ului. Utilizează aceste setări dacă trebuie să ajustezi ceva după ce configurarea a fost inițializată de EIS după instalare, sau dacă nu poți urmări acest proces automatizat. Pentru a începe configurarea EIS:

- Navighează la **Configurare→Setări sistem→Sistem→Integrare Enterprise**.



- Selectează Certificat pentru criptarea la nivel de mesaj prin HTTPS, sau adaugă autentificarea HTTP cu nume de utilizator / parolă care pot fi setate aici şi ajustate pe pagina de configurare a serverului EIS.
- Activarea sau Dezactivarea serviciilor pe care Vodafone trebuie să le integreze prin EIS.

Notă: Vodafone SaaS oferă deja livrare email folosind SMTP, dar puteți de asemenea activa EIS pentru a folosi propriul dvs. server SMTP (se poate face conform detaliilor din **Setări sistem**→ **Sistem** → **Email** (SMTP)).

- Folosind opțiunea **Advansat** ,puteți restabili integrarea regulată (directă) (fără a utiliza EIS), prin dezactivarea unor portaluri, printre care:

- Servicii dispozitiv
- Portal self-service
- Oricare alte componente

Notă: Certificatul generat în timpul configurării automate are amprenta localizată aici; aceasta poate fi ştearsă şi reînnoită dacă este necesar.

Dacă EIS nu se poate conecta la API în timpul instalării, generează un script de configurare (criptat):

- Generează certificatul, **Salvați** pagina şi dă click pe **Refresh**.
- Exportă setările pentru serverul EIS (aceasta îț i solicită să setezi o parolă).
- Descarcă fişierul XML şi importați-l în configurația EIS (aceasta configurează automat serverul EIS).

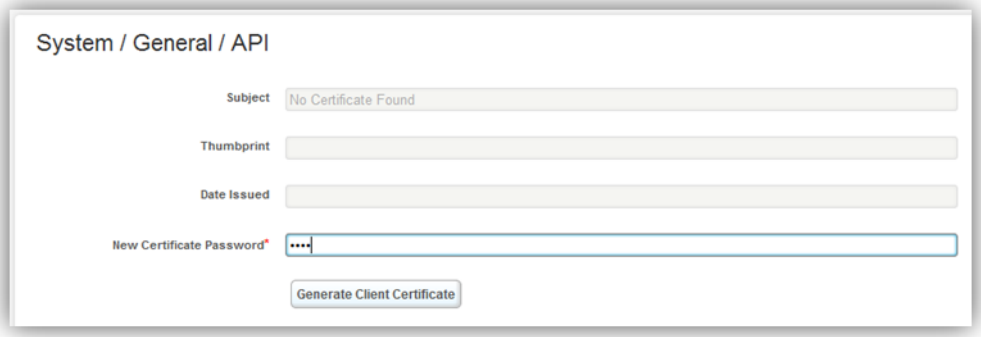
Utilizarea VSDM API

Pagina **API** din **Setări sistem** stabileşte securitatea Grupurilor tale de locație pentru a utiliza certificatele. Odată ce aceasta este configurată, sistemele de integrare pot utiliza certificatul pentru a comunica în siguranță cu mediul prin intermediul VSDM API.

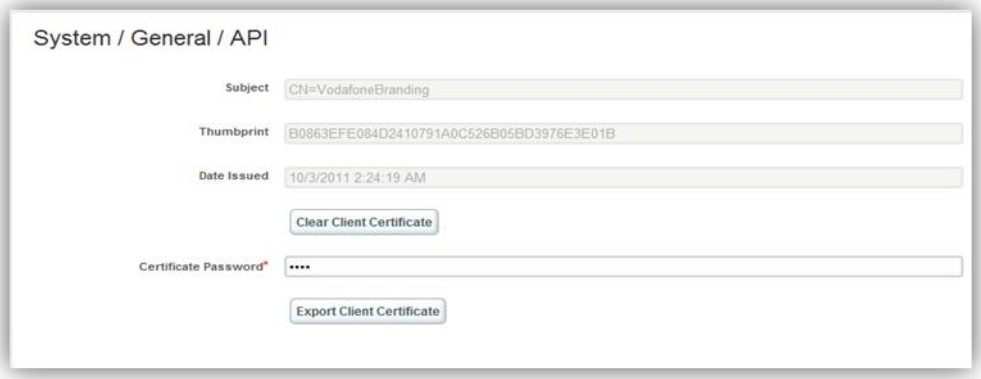
- Cel mai des întâlnit exemplu de sistem de integrare este Vodafone Secure Email Gateway. Pentru a monitoriza şi controla un Secure Email Gateway dintr-un grup de locație specific, un certificat API este necesar în timpul procesului de instalare.

Pentru a genera un certificat API pentru mediul tău:

- Navighează **Setări sistem** → **Grup de locație**



- Introdu parola în câmpul **Parolă certificat nou** şi apoi dă click pe **Generare Certificat Client**. Certificatul API este acum disponibil.



- Pentru a utiliza certificatul API într-un sistem de integrare (cum ar fi Secure Email Gateway), trebuie să-l exporţi. Re-introdu **parola certificatului** şi dă click pe **Exportare Certificat Client.**
- Certificatul este acum gata şi poate fi folosit pe calculatorul tău şi în sistemul integrat.

Cele mai bune practici

- Ca parte a sistemului iniţial de configurare Vodafone, administratorii trebuie să configureze mai multe setări de bază ale sistemului (în pagina Setări Sistem din Consola de administrare VSDM), care permit integrarea între serverul Vodafone şi infrastructura corporativă). Aceste setări nu trebuie să fie schimbate odată ce acestea sunt configurate.