

datasheet

Een datasheet over

MobiDM & iOS4 (iPhone 4 en iPad)

De Apple iPhone heeft mondiaal inmiddels een ijzersterke positie verworven. De Apple iPad, die 'tablet-computing' op de kaart heeft gezet, is een blijver. Beide apparaten zijn voorbeelden van de 'bring your own' trend, waarbij de gebruiker als consument bepaalt welk apparaat hij zal gebruiken voor zakelijke doeleinden.

Mei 2011

Introductie

De Apple iPhone heeft mondiaal inmiddels een ijzersterke positie verworven. De Apple iPad, die 'tablet-computing' op de kaart heeft gezet, is een blijver. Beide apparaten zijn voorbeelden van de 'bring your own' trend, waarbij de gebruiker als consument bepaalt welk apparaat hij zal gebruiken voor zakelijke doeleinden.

Veel iPads zijn als privé-bezit aangeschaft, maar worden daarnaast ook zakelijk gebruikt. Daarom laten organisaties vaker eigen zakelijke Apps voor het iOS-platform ontwikkelen. Ook zijn zij begonnen met het beheren van deze krachtige mobiele apparaten.

Deze ontwikkelingen zorgen voor nieuwe uitdagingen zoals:

- Hoe kunnen iOS apparaten veilig zakelijk worden ingezet?
- Hoe kunnen zakelijke applicaties worden beheerd en geïmplementeerd?
- Hoe wordt toegang tot bedrijfsinformatie beschermd?
- Hoe kunnen iOS apparaten worden gecontroleerd, maar wel gebruiksvriendelijk?
- Hoe kunnen op afstand toestellen worden uitgerold, beheerd en geconfigureerd?
- Hoe kunnen alle versies van iPhone/iPad - OS 3.x, 3GS, 4.0 worden beheerd?

MobiDM biedt antwoord op al deze vragen, en meer: MobiDM zorgt namelijk voor volledig beheer van mobiele toestellen van het type iOS3, iOS4 en andere reguliere mobiele besturingssystemen. Het is zelf-service, eenvoudig, effectief en heeft diverse beveiligingsopties..

MobiDM & iOS4: Via Officieel MDM Protocol

MobiDM combineert een volledige set van beheers- en beveiligingsmogelijkheden op basis van het Apple MDM protocol die hier nader worden toegelicht.

MobiDM & iOS4: Beheersmogelijkheden

MobiDM maakt het mogelijk om eenvoudig zakelijke applicaties in te zetten en te beheren. Met behulp van de MobiDM Appstore kan de beheerder nieuwe zakelijke applicaties op afstand beschikbaar maken voor een of meerdere gebruikers (toestel of toestellen). De toestellen worden op afstand beheerd en beheerders kunnen taken versturen of updates verzenden zonder de gebruiker te belasten. Updates van bestaande applicaties, wijzigingen in de instellingen of andere taken worden naadloos aangestuurd door MobiDM en uitgevoerd door het toestel.

Implementatie van Apps

Met behulp van MobiDM kunnen zakelijke applicaties worden gedistribueerd naar een iOS-toestel (gebruiker) of een groep van iOS-toestellen (gebruikers); op afstand, door middel van het draadloze of mobiele netwerk. Gebruikers kunnen de zakelijke (afgedwongen) en aanbevolen applicaties downloaden via de speciale Enterprise App Store. Het is ook mogelijk om de installatie van afgedwongen applicaties te herroepen. Het installatieproces van applicaties kan worden bijgehouden, zodat controle en betrouwbaarheid gegarandeerd kan worden bij geïnstalleerde applicaties. Zodra de speciale MobiDM client is geïnstalleerd, heeft de gebruiker direct toegang tot de MobiDM Enterprise App Store. De beheerder kan ook links publiceren naar applicaties uit de Apple App Store. De Enterprise App Store kan bovendien gebruikt worden om automatische updates van software te sturen naar het toestel.

Gebruikers vinden de door de beheerder beschikbaar gestelde applicaties in de MobiDM Enterprise App Store. Technisch wordt hier gebruik gemaakt van de Afaia client van Sybase SAP. Door de beheerder afgedwongen applicaties worden altijd geïmplementeerd; aanbevolen applicaties kunnen worden aangekozen door de gebruikers om te implementeren op het toestel.

Geen actie van de gebruiker vereist

MobiDM ondersteunt het officiële Apple MDM protocol. Hierin zijn instellingen, profielen en configuraties voor iOS toestellen opgenomen. Er is dan ook geen noodzaak meer om de iPhone Configuration Utility (iPCU) te gebruiken, maar binnen MobiDM bestaat deze mogelijkheid wel.

Zodra een relatie 'handshake' is gerealiseerd tussen MobiDM en het toestel, zal alleen de beheerder gemachtigd zijn om het toestel met behulp van de MDM-protocol te beheren. Daarna kunnen diverse belangrijke taken eenvoudig worden uitgevoerd; tevens zonder gebruik te hoeven maken van ActiveSync. Toestellen kunnen worden gewist of op afstand worden geblokkeerd, waarbij toestellen uiteraard kunnen worden verwijderd uit de MobiDM-portal. Indien de relatie 'handshake' tussen MobiDM en een toestel wordt beëindigd, zullen de instellingen en de Exchange-account informatie direct worden verwijderd uit het toestel.

Vanaf de MobiDM portal kunnen alle officiële 'Apple MDM' taken worden gepusht naar de toestellen, zoals de volgende instellingen:

- **APN settings**
- **Exchange settings**
- **Certificates**
- **Set restrictions of apps**
- **Wi-Fi settings**
- **VPN settings**

Het zogenoemde SCEP is gebruikt om een relatie 'handshake' op te zetten tussen het toestel en MobiDM. De gebruiker moet deze MDM relatie eenmalig accepteren, en eenmaal toegevoegd aan MobiDM is er geen verdere actie van de gebruiker vereist. De gebruiker kan deze relatie beëindigen, maar dan worden direct alle beheerapplicaties, toestelconfiguratie en exchange informatie, inclusief PIM2 worden verwijderd.

MobiDM & iOS4: Beveiligingsmogelijkheden

iOS Remote Wipe - Kill Pill

Toestellen kunnen kwijt raken of gestolen worden, inclusief waardevolle bedrijfsinformatie die daarop is opgeslagen. Om te voorkomen dat deze informatie dan uit lekt, kan zowel de gebruiker als de beheerder een 'kill-pill' sturen naar het toestel. Het toestel wordt dan compleet gewist, alle data wordt verwijderd en de instellingen worden teruggezet naar de fabrieksinstellingen. Ook ondersteunt MobiDM het afdwingen van beveiliging op het toestel met betrekking tot toegang tot bedrijfsinformatie of netwerken.

iOS Inventory

De beheerder is met MobiDM in staat het toestel nauwkeurig te monitoren. Vanuit beheer- en beveiligingsoogpunt is het belangrijk om informatie te hebben over een toestel dat is verbonden met het netwerk en over welke applicaties geïnstalleerd en in gebruik zijn.

Jailbreak detectie

Vanuit beveiligingsbeleid bestaat de eis voor het gebruik van een wachtwoord door de gebruiker om pas dan toegang te krijgen tot een toestel. MobiDM is in staat om het wachtwoord te resetten of om de gebruiker te dwingen dit te wijzigen. Zoals eerder aangegeven, kunnen nieuwe of gewijzigde instellingen en taken op afstand worden gestuurd naar het toestel. De huidige status van de wijzigingen wordt gerapporteerd naar de server, zodat de beheerder de beschikking heeft over up-to-date informatie. Daarnaast merkt MobiDM op wanneer sprake is van jailbreaking. Dan verschijnt de status prominent naast het toestel in de Portal. Het overzicht van de status van het toestel (zoals IMEI-nummer, SIM-nummer, Jailbreak status, provider, etc) is up-to-date, omdat MobiDM regelmatig in verbinding staat met de toestellen. Deze informatie wordt bijgewerkt na elke connectie en wordt weergegeven aan de gebruiker en de beheerder in de MobiDM-portal.

Hoe kan ik ... ?

Een iPhone of iPad zakelijk uitrollen:

De beheerder stuurt de gebruiker een tekstbericht (alleen iPhone) en/of een e-mail die een verwijzing bevat naar de vereiste software om te installeren. Om naast activatie van het MDM protocol ook gebruik te maken van de Enterprise App Store dienen 3 stappen te worden doorlopen op de 'activatie-website':

1. Er dient een 'handshake' te worden gerealiseerd tussen het toestel en de MobiDM portal. Feitelijk wordt er een profiel op het toestel geïnstalleerd. Hierna ondersteunt het toestel direct de mogelijkheden van het Apple MDM protocol. Wie gebruik wil gaan maken van de Enterprise App Store, dient ook stap 2 en 3 te doorlopen.
2. Wanneer de eerste stap voltooid is, opent u de Apple App Store op uw toestel en selecteert u de Afaia app. Klik op de knop "Install" om Afaia te installeren.
3. Zodra de Afaia client is geïnstalleerd, zal ook deze ingesteld en gekoppeld moeten worden aan MobiDM. Hiervoor gaat u terug naar de activatie website en klikt u op de laatste button van uw scherm om de koppeling tot stand te brengen.

Let op: de installatie van de MobiDM Enterprise App Store client is optioneel; deze client biedt de volgende extra functionaliteiten:

- **Extra jailbreak detectie**
- **MobiDM Enterprise Appstore: App selectie, download en updates**
- **Exchange Access Controle door optioneelde client periodiek te laten verbinden**

Certificaten voor iOS4 distribueren:

De beheerder kan certificaten toevoegen aan een iPhone Configuration Utility (iPCU) profiel en dit vervolgens uploaden in de MobiDM portal en hiermee een taak aanmaken. Vervolgens kan deze taak worden verstuurd worden naar een geselecteerde groep van gebruikers.

Een aantal screenshots van de MobiDM Client App:



Voor individuele, gebruiks-specifieke certificaat-distributie is een speciale plug-in oplossing beschikbaar.

Voor meer informatie kunt u met ons contact opnemen op sales@veliq.com of +31 10 20 60 208.

Feature list

Passcode Settings	WIFI Settings	Restrictions	Exchange
<ul style="list-style-type: none"> • Require Passcode <ul style="list-style-type: none"> • Allow Simple Value • Require Alphanumeric Value • Minimum Passcode Length • Minimum Complex Characters • Maximum Number of Failed Attempts – device is wiped • Maximum Passcode Age – in Days • Passcode Lock – in minutes • Grace Period for device lock • Passcode History 	<ul style="list-style-type: none"> • Service Set Identifier - SSID of the wireless network <ul style="list-style-type: none"> • Hidden Network • Security Type • Password • Accepted EAP Types • EAP-FAST Protected Access • Authentication Settings • Identity Certificate • Certificates for validating the authentication server for the Wi-Fi connection. • Trusted authentication servers • Allow Trust Exceptions <ul style="list-style-type: none"> • SSID • Hidden Network • Encryption Type 	<ul style="list-style-type: none"> • Allow Explicit Content • Allow Use of Safari • Allow Use of YouTube • Allow Use of iTunes • Allow Installing Apps • Allow Use of Camera • Allow Screen Capture <ul style="list-style-type: none"> • Allow Voice Dialing • Force Encrypted Backups • Allow Multiplayer Games • Set Safari Security Preferences <ul style="list-style-type: none"> • Force Fraud Warning • Allow Java Script • Allow Pop Ups • Accept Cookies • Allow inApp Purchases • Content Rating • Disable Push while Roaming 	<ul style="list-style-type: none"> • Account Name <ul style="list-style-type: none"> • Exchange Active Sync Host • User • Email Address • Use SSL • Domain • Password • Credential Name • Number of Past Days to Sync User is prompted for values not set
VPN Settings	Email	LDAP/CalDAV/Calendars/Web Clip	Advanced
<ul style="list-style-type: none"> • Connection Name • Connection Type • Server IP or Name • Account • Authentication Type • Shared Secret Entry • Send All Traffic Through VPN Setting <ul style="list-style-type: none"> • Proxy <p>VPN's Supported</p> <ul style="list-style-type: none"> • L2TP/IP • PPTP • Cisco IPsec 	<ul style="list-style-type: none"> • Account Description <ul style="list-style-type: none"> • Account Type – IMAP or POP • Path Prefix • Account Name • Email Address • Mail Server and Port • Username • Use Password Authentication • Use SSL <ul style="list-style-type: none"> • Incoming Username • Outgoing Username 	<ul style="list-style-type: none"> • LDAP Connection Settings • CalDAV Connection Settings • Calendar Connection Settings • Web Clip Settings • Certificate Payload • SCEP Payload <ul style="list-style-type: none"> • CardDAV 	<ul style="list-style-type: none"> • APN <ul style="list-style-type: none"> • AP Username • AP Password • Proxy Server and Port