CENTRIFY WHITE PAPER

# Improving Mobile Device Security and Management with Active Directory

## An overview of mobile device market trends, challenges and approaches to securing and managing smart phones and tablets across the enterprise


**Abstract**

As more and more workers bring personal devices to work for increased productivity and mobile access organizations must quickly respond to the security and compliance risks posed by largely unmanaged access to corporate information. Enterprises can expect to see tablet sales alone increase by 250% in 2012, primarily iPads, which users are connecting to corporate email and other network services at unprecedented rates. To address these trends IT organizations need to deploy comprehensive and cost-effective solutions that secure and manage all the devices that are part of this 'consumerization of IT' trend — iOS and Android smart phones and tablets and Mac OS laptops.

Given the increasing proliferation of mobile devices, mobile security and device management is gaining greater significance and priority within IT organizations. Over the last few years large numbers of vendors have rushed in to attempt to address this need, but unfortunately first generation Mobile Device Management solutions have been designed and built to force enterprises to deploy complex new infrastructure that creates yet another management and policy silo that is difficult to manage. Enterprises are now looking for second generation mobile management solutions that will let them manage mobile devices in a straightforward and "friction-less" way that leverages their existing infrastructure, skill sets and processes.

With the release of Centrify DirectControl for Mobile, Centrify is stepping in to address this significant pain point of providing IT the control and visibility over mobile devices that they require while delivering this robust mobile management capability in a way that leverages the investments that IT organizations have already made. Centrify's innovative approach to mobile device security and management uses a cloud-based service to seamlessly leverage an organizations existing on-premise Active Directory infrastructure. This enables Group Policy-based management of mobile devices using Active Directory management tools that administrators and helpdesk staff are already familiar with. And Centrify's comprehensive integration with Active Directory secures and manages Mac OS, Linux and UNIX systems as well — this can increase an organizations return on investment and significantly lowers costs.

*Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.*

*Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2004-2012 Centrify Corporation. All rights reserved. WP-026-2012-02-02*

*Centrify, DirectControl and DirectAudit are registered trademarks and Centrify Suite, DirectAuthorize, DirectSecure and DirectManage are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Contents

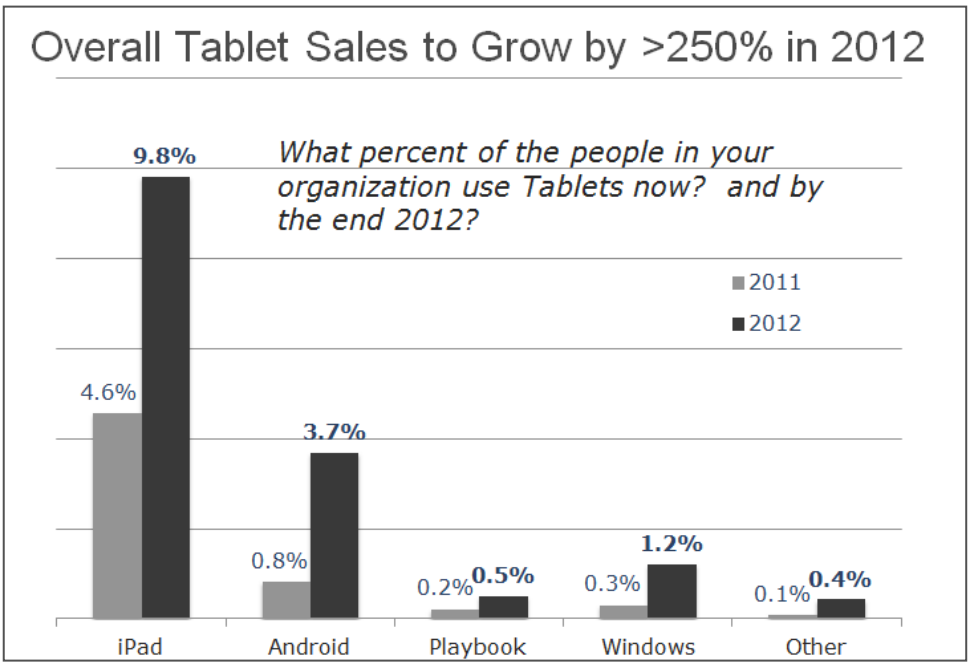
Introduction ..... 4
Mobile Device Security and Management Challenges ..... 5
Management Silos ..... 6
Security risks ..... 7
Compliance pressures ..... 7
Operational and administrative costs ..... 7
The Case for User and Device Identity Centralization ..... 8
Active Directory: The Clear Choice for Heterogeneous Mobile Device Management ..... 8
Centrify DirectControl for Mobile ..... 9
Active Directory and Group Policy-based device management ..... 9
Cloud-based service ..... 10
Self-service and automation ..... 11
Unified platform for mobile devices, Mac OS X and more ..... 11
Inventory devices and even detect jail-broken ones ..... 11
Conclusion ..... 13
Resources ..... 13
Appendix Common Mobile Device Settings ..... 14

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

# Introduction

It has been a decade long trend — users increasingly bringing their own devices into the workplace, first Mac OS X systems then smart phones and now tablet devices. Most companies still have not dealt with these waves of new devices in a comprehensive fashion and many firms are not even aware of the real number of personal devices that are being used to access corporate network services such as email, WiFi and VPN connections. There can't be a more telling statistic than one quoted in a recent IDC study that reported 40% of IT decision makers say they let workers access corporate information from employee-owned devices, but 70% of employees indicated they access corporate networks this way. And the use of personally owned devices is only growing — according to one study there will be close to 15 billion network connected devices (e.g. smart phones, notebooks and tablets) by 2015. This translates into 7 connected devices per U.S. citizen by this date. Given this explosion in new devices and device types IT organizations are appropriately concerned about how they can cost effectively secure and manage the multiple devices their employees and contractors want to use for mobility and productivity.

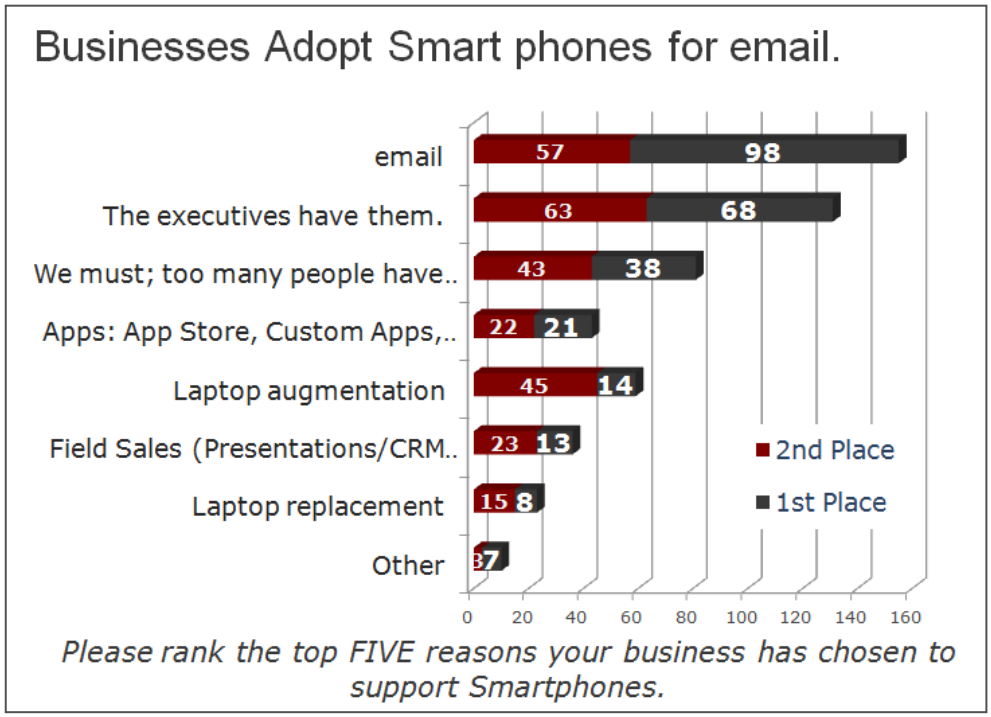
Analysts and industry press have dubbed these trends the 'consumerization of IT' to describe a newly empowered set of workers that use their own devices and cloud-based applications to be more responsive to customers and to increase their own productivity and work flexibility. To get a handle on these trends organizations have the immediate task of locking down the current wave of consumer tablet devices, primarily iPads but also Android tablets, which are now entering the enterprise at unprecedented rates. These devices are more capable and often hold more sensitive information than smart phones and therefore may pose a higher security risk.




**Securing tablets is high priority for enterprise IT security staff given capabilities that are closer to a personal computer. (Enterprise Device Alliance Survey published September 2011)**

In addition, smart phones users continue on to connect to enterprise networks at an accelerated pace with access to corporate email as the overwhelming driver. And a significant percentage of organizations are expecting even larger numbers of employee-owned Mac OS computers in their enterprises while the number of Windows personal computers are projected to decline slightly (according to the same Enterprise Device Alliance survey).

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.




**Enterprises allow smart phones primarily to provide timely access to email. (EDA Survey)**

Clearly, IT teams must quickly adapt to the rapid and often unmanaged access of corporate network resources by an increasingly heterogeneous number of employee-owned devices in order to ensure security, corporate and regulatory compliance. And, of course, they must do this in an environment of limited budgets and constrained staffing.

To address these trends organizations need to make a complete accounting of all the challenges associated with personally owned devices facing them if they want to implement a comprehensive solution not only for today's needs but also for the future.

## Mobile Device Security and Management Challenges

How your organization responds to the influx of iOS and Android devices will have a lot to do with the security and compliance posture you are establishing within your organization. In general organizations fall into three broad categories when responding to the employee-owned device challenge:

1) "My device or no device" — Some organizations see the flood of new devices and device types as an unauthorized incursion on their IT operations and security policies that will lessen security and compliance and increase costs. These organizations try to put the brakes on the BYOD trend by mandating a corporate standard operating system and device type with the hope they can focus on a device preferred by IT, but this approach is not popular with users who value device choice. It has been shown that the "just say no" approach increases the risk of data breaches and non-compliance.

2) "Head in the sand" — These IT organizations are not aware of the consumerization trends that are already happening in their environment. They may have pockets of users, primarily executives, that get support from IT for their devices but they are unaware of the extent of users that access their network with smart phones and tablets. These organizations are accepting an unmanaged mobile environment and therefore face unknown risks since they lack visibility and control over mobile devices that hold sensitive company information.

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

3) "Let's make a deal" — Analysts consider organizations that embrace the consumerization trend and proactively plan for a reasonable level of heterogeneity of devices to be best-in-class. Being proactive can lower costs and risks. These organizations have a policy-based approach that permits users to choose from the most popular mobile operating systems and device form factors. In exchange, IT gets to secure and manage devices in a way that allows them to mitigate the risk of data loss and apply best practices for provisioning, password policies, WiFi and VPN access and more.

In fact, one study from Aberdeen Research found that of the three responses to the "bring your own device" trend the proactive, "embrace user-driven" heterogeneity is the most secure and least costly of the three responses. This makes sense; if users are not actively trying to circumvent IT controls because they want to use their own device they are less likely to cause issues that result in security incidents and support costs.

While most enterprises today cannot be described as "proactive" recent surveys show that most IT organizations already agree that moving to a corporate policy that embraces consumer devices in the workplace is inevitable and will be an integral part of how they conduct business in the future. The benefit for IT organizations to accelerate their efforts is they become an enabler for strategic initiatives, such as worker mobility, that are transforming their businesses.

**The support of personally owned mobile devices is inevitable and if managed properly will bring increased productivity.**

Given that most organizations are beginning the move away from either a laissez-faire or strict policing environment to a *trust, but verify* model for policy control there are critical challenges that any mobile device security and management solution must address to avoid a never-ending cycle of helpdesk overload, operational complexity and expensive new infrastructures.

## Management Silos

Heterogeneity is not new to mobile devices. The same trends brought significant numbers of Macs into the enterprise and before that the data center became increasingly cross-platform as Linux systems where deployed in large numbers along with UNIX variants and Windows servers. The problem organizations should avoid when leveraging the advantages of a diverse set of platforms and devices is silos of identity, policy and device management that fragment the IT environment into islands with multiple incompatible point solutions making the implementation of a company-wide policy framework extremely complex.

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Add on top of this private, public and hybrid cloud deployment models and the goal of consistent and unified access management becomes difficult if not impossible to achieve. In order to ensure simplicity and true lifecycle management of devices, organizations need to centralize identity and device management into a single authoritative and robust identity and policy infrastructure.

### Security risks

A fractured identity and device management environment increases the risk that an orphaned account or retired device does not get de-provisioned. And users get frustrated with multiple passwords and different security policies because the administrative task of implementing a consistent security policy across multiple point products is just too hard. Without a single credential that ties together all the user's devices, policies and access rights users are more likely to attempt to circumvent security controls or outright reject corporate management of their personal devices.

### Compliance pressures

Supporting a diverse population of mobile devices should not add complexity and delays in demonstrating compliance to the myriad of compliance requirements such as Sarbanes-Oxley, PCI DSS and HITECH/HIPAA. If the auditing process requires the manual consolidation of data from multiple identity systems by IT staff then compliance reporting becomes a time-intensive and expensive process. If organizations can't quickly demonstrate compliance the entire organization can risk an audit finding and can even incur fines. Centralizing identity and access management across personal computers and mobile devices streamlines the compliance process and lowers on-going audit costs.

### Operational and administrative costs

A major cost for most IT organizations is helpdesk calls related to password resets (Gartner estimates that 45% of all helpdesk calls are password reset requests) which means adding a separate identity store and new management console for mobile devices will inevitably increase helpdesk costs. In addition, helpdesks are increasingly fielding calls regarding mobile device problems. Maintaining multiple identity stores and a separate device management system also results in time consuming and error-prone administrative processes as administrators manage multiple consoles that may display inconsistent data for the same user. Leveraging a single identity and device management infrastructure and single, unique user credential for access from any device to any resource maximizes operational efficiency and minimizes administrative costs.

**Focus: Problems with the Single Purpose Mobile Device Management Approach**

Many vendors have jumped into mobile device management as the market explodes with the growth in iOS and Android smart phones and tablets. While some of these products seem to offer a short term fix to the influx of personal devices in the enterprise they bring with them legacy approaches and costly new infrastructures that are hard to deploy and manage. Before an organization buys into an single purpose MDM approach they should consider the following issues:

- Single purpose MDM products do not fully leverage existing infrastructure requiring enterprises to setup separate databases just for mobile device management.
- They force help desk staff to learn and use multiple consoles for example one to disable the user and another to wipe the device.
- Have intrusive deployment requirements including components that must be deployed in the DMZ and the opening of additional firewall ports.
- Are expensive to test and acquire costing IT staff precious time just to evaluate and are costly to buy ($75 or more per device).
- Most importantly they only manage mobile devices and can't address Mac OS, Linux and other platforms.

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

## The Case for User and Device Identity Centralization

Faced with the challenges described above IT organizations have several options as they fashion a strategy for mobile security and device management.

- Deploy standalone point products for mobile devices that further fragment the organizations identity environment and dedicate even more resources to managing an inefficient environment. Many organizations may feel this is their only option since they have failed to find a solution that fits their budget and does not require intrusive and impractical changes to their network environment and business practices.

- Synchronize identity stores across mobile devices, Mac OS and Windows systems. These solutions add yet another complex new infrastructure into the mix. Adding complexity which can only deliver lowest common denominator capabilities across identity systems and still force administrators to manage multiple consoles and increase on-going maintenance for IT operations staff. The result is a cobbled together infrastructure that has many points of failure.

- Centralize the management of mobile devices, Mac OS and other systems into a robust and secure on-premise directory system that can control and manage systems and devices inside and outside the enterprise. This approach when leveraging an existing infrastructure, skillsets and processes already in place in an IT organization offers compelling productivity benefits, increased security, improved compliance reporting and cost savings.

## Active Directory: The Clear Choice for Heterogeneous Mobile Device Management

The vast majority of organizations have given their users Active Directory accounts to enable corporate email and control access to network resources such and file shares. Clearly, Active Directory is a strategic IT platform in the corporate environment.

Active Directory has critical advantages for establishing a centralized and authoritative directory for identity, policy and access management, advantages not found in any other directory:

- Fault tolerant, distributed and high availability deployment model with automated DNS lookup service and one-way trust.

- Built-in support for Kerberos authentication and single sign-on.

- A fully featured and integrated Certificate Authority (Microsoft CA) that makes it easy to support PKI-based authentication for email, WiFi and VPN and encryption of data-in-transit.

- Group Policy for centralized security enforcement of computer objects based on type, organizational unit or functional grouping.

- A rich ecosystem of administrative tools already familiar to an organizations helpdesk and IT staff that makes supporting the identity and device access management lifecycle easy.

Clearly, the most practical approach is to fully leverage Active Directory for centralized management of mobile devices and non-Windows systems (Mac OS and Linux) for true lifecycle management of all the devices (laptops, tables and smart phones) users adopt for personal and business use. Organizations efficiently manage Windows systems using their Active Directory infrastructure today – Mac OS X systems, iOS and Android devices can be supported using the same robust and secure authentication, provisioning and Group Policy enforcement enterprises

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

rely on for Windows. There has not been single solution that would empower enterprises to leverage Active Directory for all their identity, device and access management — until now — the introduction of Centrify DirectControl for Mobile now makes it possible to secure and manage mobile devices within your Active Directory infrastructure and changes the way IT organizations view mobile device security and management by integrating into existing infrastructure, while also utilizing existing processes and skillsets.

## Centrify DirectControl for Mobile

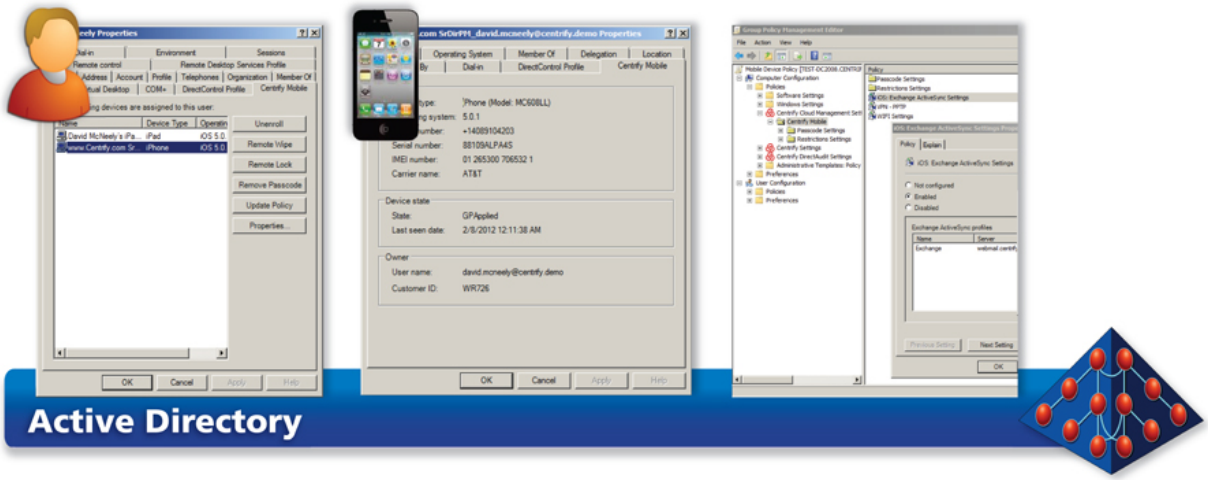
Centrify DirectControl for Mobile is an easy-to-deploy, cloud-based service lets you centrally secure and manage smart phones and tablets using your existing Active Directory infrastructure. DirectControl for Mobile uses familiar Group Policy tools together with the Centrify Cloud Service to enforce security settings over a trusted, over-the-air connection and secure access to corporate network services. And Centrify delivers the industry's only solution that secures and manages not only popular mobile devices but Mac OS X, UNIX and Linux systems as well.

DirectControl for Mobile benefits customers with a deep integration with Active Directory (unlike other products that only use Active Directory as an authentication check in the enrollment process and still require setup of yet another database for user and device information). Centrify's solution stores all the device objects and policy within Active Directory. This native and centralized approach to mobile device security and management brings a combination of advantages that only Centrify can provide:

- Active Directory and Group Policy-based device management
- Cloud-based service
- Self-service and automation
- Unified platform for mobile devices, Mac OS X and more
- Inventory devices and even detect jail-broken ones

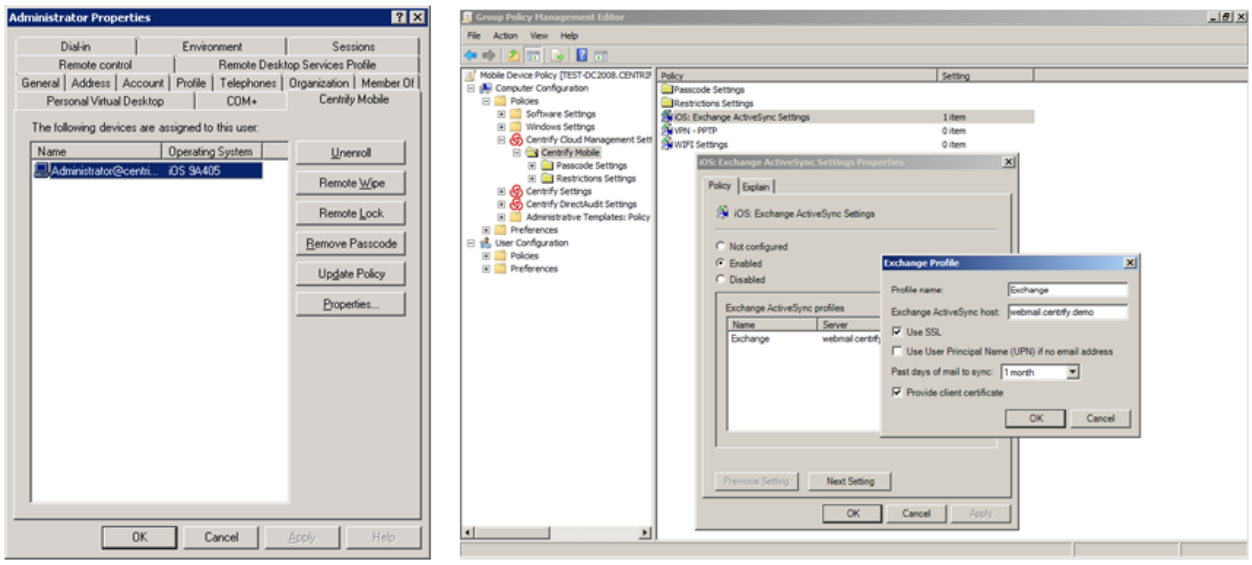
### Active Directory and Group Policy-based device management

Centrify uses your on-premise Active Directory infrastructure and Group Policy-based management tools to let you easily enforce and update mobile security settings, lock or remotely wipe devices, and secure access to email networks.




**DirectControl for Mobile supports familiar Active Directory management tools, ADUC and Group Policy Object Editor, so administrators can see which devices are assigned to a user, the properties of each device and manage policies across all devices**.

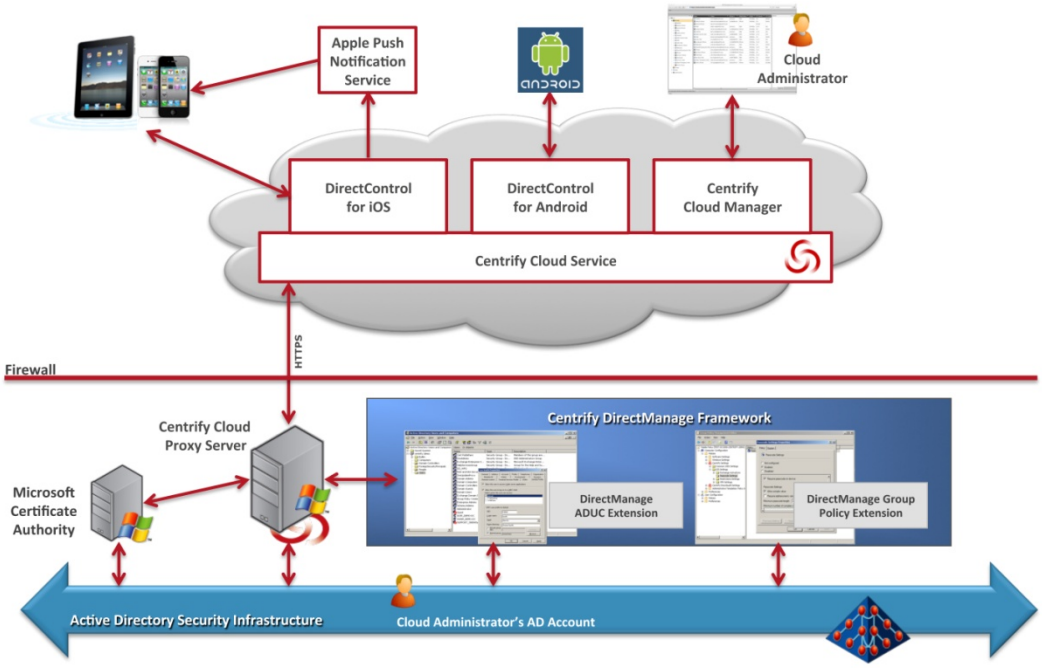
© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.




**Centralized administration within Active Directory of all device security settings, profiles, certificates and restrictions means even large populations of mobile devices are easy to manage for security and compliance — with the added benefit of leveraging existing technology, skillsets and processes.**

## Cloud-based service

The Centrify Cloud Service seamlessly allows your on-premise Active Directory environment to easily manage mobile devices over a trusted, over-the-air connection, whether or not a device is connected to the corporate network, thereby making deployment even easier and further eliminating the need for costly new infrastructure.




**The Centrify Cloud Service and Cloud Proxy Server makes integration with your on-premise Active Directory infrastructure easy so you can quickly secure and manage mobile devices.**

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

It's important to understand that device settings are defined by the platform supplier, Apple iOS for example, effectively leveled the playing field for MDM vendors by providing a common Application Programming Interface (API) that all mobile security vendors must use. This means that the control of security settings and device restrictions (See Appendix) are the same for all MDM vendors.

Organizations need to focus on solutions that provide the simplest and most scalable deployment model that can fully leverage existing infrastructure investments. DirectControl for Mobile accomplishes this without requiring any additional software deployed in the DMZ and doesn't require opening of firewall ports that increase network vulnerabilities. And only Centrify DirectControl supports other consumer oriented, end user devices such as Mac OS X systems.

The deployment of DirectControl for Mobile is extremely fast and simple, with the Active Directory infrastructure already in place, the only requirement is to install and configure the Centrify Cloud Proxy which takes less than an hour irregardless of the number of devices to be managed. Once this is accomplished users are empowered to perform self-service enrollment that will install their mobile device profiles using a secure over-the-air connection.

## Self-service and automation

Centrify DirectControl for Mobile quickly brings large populations of authorized devices under management with user self-service enrollment and automated configuration of each user's authentication credentials, email, WiFi and VPN settings, thereby greatly reducing helpdesk volumes associated with mobile devices.

**Self-service enrollment using a web-based form or app and automated configuration of profiles make the setup and enforcement of device and security settings easy for administrators and users.**

## Unified platform for mobile devices, Mac OS X and more

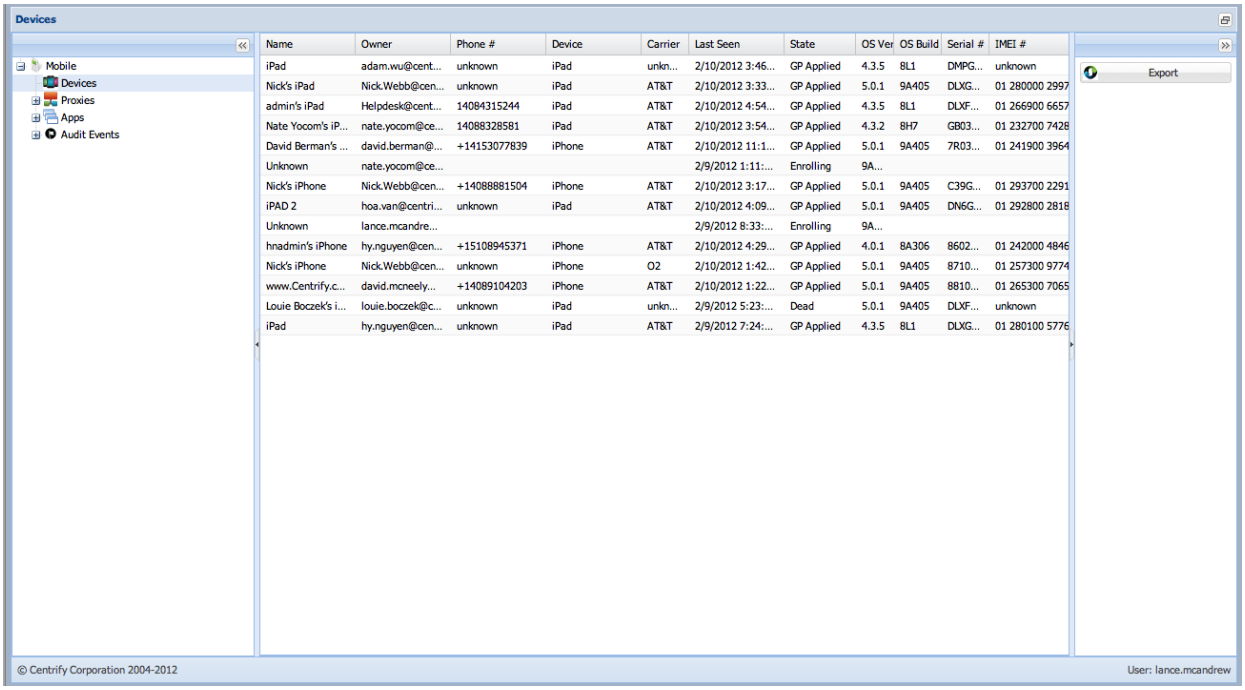
Centrify is the industry's only Active Directory integration solution that secures and manages not only iOS and Android devices but also Mac OS X, UNIX and Linux systems. Centrify is the leader in providing enterprises with a unified platform for Active Directory-centric identity and access management. With a suite of integrated solutions supporting over 300 platform releases across Linux,UNIX and Mac OS Centrify is the only solution provider that can support the needs of small, medium and large enterprises.

## Inventory devices and even detect jail-broken ones

Centrify DirectControl for Mobile simplifies reporting of enrolled devices, installed applications and device update status across the entire organization, with the ability to detect and block enrollment of jail-broken devices. Because DirectControl for Mobile uniquely integrates with Active Directory the process of creating a computer

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

object tied to the assigned users Active Directory credential is automatic. This makes the inventory of devices by group, device type and user role simple for administrators to provide to management.




| Name | Owner | Phone # | Device | Carrier | Last Seen | State | OS Ver | OS Build | Serial # | IMEI # |
|---|---|---|---|---|---|---|---|---|---|---|
| iPad | adam.wu@cent... | unknown | iPad | unkn... | 2/10/2012 3:46... | GP Applied | 4.3.5 | 8L1 | DMPG... | unknown |
| Nick's iPad | Nick.Webb@cen... | unknown | iPad | AT&T | 2/10/2012 3:33... | GP Applied | 5.0.1 | 9A405 | DLXG... | 01 280000 2997 |
| admin's iPad | Helpdesk@cent... | 14084315244 | iPad | AT&T | 2/10/2012 4:54... | GP Applied | 4.3.5 | 8L1 | DLXF... | 01 266900 6657 |
| Nate Yocom's iP... | nate.yocom@ce... | 14088328581 | iPad | AT&T | 2/10/2012 3:54... | GP Applied | 4.3.2 | 8H7 | GB03... | 01 232700 7428 |
| David Berman's ... | david.berman@... | +14153077839 | iPhone | AT&T | 2/10/2012 11:1... | GP Applied | 5.0.1 | 9A405 | 7R03... | 01 241900 3964 |
| Unknown | nate.yocom@ce... | | | | 2/9/2012 1:11:... | Enrolling | 9A... | | | |
| Nick's iPhone | Nick.Webb@cen... | +14088881504 | iPhone | AT&T | 2/10/2012 3:17... | GP Applied | 5.0.1 | 9A405 | C39G... | 01 293700 2291 |
| iPAD 2 | hoa.van@centri... | unknown | iPad | AT&T | 2/10/2012 4:09... | GP Applied | 5.0.1 | 9A405 | DN6G... | 01 292800 2818 |
| Unknown | lance.mcandre... | | | | 2/9/2012 8:33:... | Enrolling | 9A... | | | |
| hnadmin's iPhone | hy.nguyen@cen... | +15108945371 | iPhone | AT&T | 2/10/2012 4:29... | GP Applied | 4.0.1 | 8A306 | 8602... | 01 242000 4846 |
| Nick's iPhone | Nick.Webb@cen... | unknown | iPhone | O2 | 2/10/2012 1:42... | GP Applied | 5.0.1 | 9A405 | 8710... | 01 257300 9774 |
| www.Centrify.c... | david.mcneely... | +14089104203 | iPhone | AT&T | 2/10/2012 1:22... | GP Applied | 5.0.1 | 9A405 | 8810... | 01 265300 7065 |
| Louie Boczek's i... | louie.boczek@c... | unknown | iPad | unkn... | 2/9/2012 5:23:... | Dead | 5.0.1 | 9A405 | DLXF... | unknown |
| iPad | hy.nguyen@cen... | unknown | iPad | AT&T | 2/9/2012 7:24:... | GP Applied | 4.3.5 | 8L1 | DLXG... | 01 280100 5776 |

**Centralization in Active Directory makes inventory of devices and applications simple.**

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

## Conclusion

Centrify's unique, easy-to-deploy, architecture ensures your on-premise Active Directory infrastructure can be securely leveraged to quickly bring corporate and personally owned devices into line with security best practice and compliance.

- Centrify uses your on-premise Active Directory infrastructure and Group Policy-based management tools to let you easily enforce and update mobile security settings, lock or remotely wipe devices, and secure access to email, VPN and WiFi networks.

- The Centrify Cloud Service seamlessly allows your on-premise Active Directory environment to easily manage mobile devices over a trusted, over-the-air connection, whether or not a device is connected to the corporate network, thereby making deployment even easier and further eliminating the need for costly new infrastructure.

- Centrify is the industry's only Active Directory integration solution that secures and manages not only iOS and Android devices but also Mac OS X, UNIX and Linux systems, as well as web and enterprise applications.

## Resources

Centrify Mobile Security Management Microsite

www.centrify.com/mobile

Centrify DirectControl for Mobile

http://www.centrify.com/downloads/public/centrify_ds024_directcontrol_for_mobile.pdf

Centrify DirectControl for Mobile for Videos Demonstrations

http://www.centrify.com/mobile/directcontrol-for-mobile-demos.asp

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

# Appendix Common Mobile Device Settings

**Passcode Settings**

- require passcode on device
- allow simple value
- require alphanumeric value
- minimum passcode length
- minimum number of complex characters
- maximum passcode age (days)
- auto-lock (minutes)
- passcode history
- grace period for device lock
- maximum number of failed attempts

**Restrictions**

- allow installing apps
- allow use of camera
- allow screen capture
- allow automatic sync while roaming
- allow voice dialing
- allow in-app purchase
- allow multi-player gaming
- allow adding Game Center friends
- force encrypted backups
- allow use of YouTube
- allow use of iTunes Music Store
- allow use of Safari
- allow explicit music and Podcasts
- ratings region
- allowed movies content rating
- allowed TV shows content ratings
- allowed apps content rating

**Protocols settings**

**Authentication settings**

**Proxy settings**

*Some settings are device OS specific

**Exchange ActiveSync Settings**
(support for one or more Exchange Mailboxes)
Each Mailbox supports:

- Profile Name
- Exchange ActiveSync host
- Use SSL
- Use User Principal Name (UPN) if no email address
- Past days of mail to sync (drop down box)
- Provide client certificate (serves both to trigger PKI cert auto-issuance as well as to configure the system to use PKI for Exchange authentication)

**VPN - PPTP Settings**
(support for one or more VPN-PPTP configurations)
General settings

- Connection name
- Server
- User authentication (Password or RSA SecurID)
- Encryption level (None, Automatic, Maximum [128bit])
- Send all traffic
- Proxy settings for each connection
- None, Manual, Automatic

**WiFi Settings**
(support for one or more WiFi settings)

General settings

- SSID
- auto-join
- hidden network
- security type
- password

© 2012 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.