iPhone und iPad im Unternehmen

Implementierungsbeispiele

Oktober 2011

Informieren Sie sich mit diesen Implementierungsbeispielen, wie sich iPhone und iPad in Unternehmensumgebungen integrieren lassen.

- Microsoft Exchange ActiveSync
- Standardbasierte Dienste
- Virtuelle private Netzwerke
- Wi-Fi
- Digitale Zertifikate
- Sicherheitsaspekte
- Mobile Device Management

Implementierung von iPhone und iPad

Exchange ActiveSync

iPhone und iPad können via Microsoft Exchange ActiveSync (EAS) direkt mit Ihrem Microsoft Exchange Server kommunizieren und ermöglichen damit auch Push-Funktionen für E-Mails, Kalendereereignisse, Kontaktdaten und Aufgaben. Exchange ActiveSync bietet darüber hinaus den Benutzern Zugriff auf die globale Adressliste und den Administratoren Funktionen zur Durchsetzung von Coderichtlinien und für die Fernlöschfunktion. iOS unterstützt sowohl die einfache als auch die zertifikatbasierte Authentifizierung für Exchange ActiveSync. Wenn Ihr Unternehmen derzeit mit Exchange ActiveSync arbeitet, sind die notwendigen Dienste zur Unterstützung von iPhone und iPad bereits vorhanden – es ist keine weitere Konfiguration notwendig. Wenn Ihr Unternehmen Erfahrung mit Exchange Server 2003, 2007 oder 2010 hat, aber noch keine Erfahrung mit Exchange ActiveSync, sollten Sie Folgendes prüfen:

Exchange ActiveSync Konfiguration

Übersicht über die Netzwerkkonfiguration

- Stellen Sie sicher, dass Port 443 in der Firewall geöffnet ist. Wenn Ihr Unternehmen Outlook Web Access erlaubt, ist Port 443 wahrscheinlich bereits geöffnet.
- Vergewissern Sie sich, dass auf dem Exchange Frontend-Server ein Serverzertifikat installiert ist, und aktivieren Sie SSL für das virtuelle Exchange ActiveSync Verzeichnis in IIS.
- Wenn Sie einen Microsoft ISA Server (Internet Security & Acceleration) verwenden, stellen Sie sicher, dass ein Serverzertifikat installiert ist, und aktualisieren Sie den DNS-Server, damit eingehende Verbindungen aufgelöst werden.
- Achten Sie darauf, dass der DNS Ihres Netzwerks sowohl für Intranet- als auch für Internetclients eine einzige Adresse an den Exchange ActiveSync Server liefert, die extern weitergeleitet werden kann. Dies ist notwendig, damit das Gerät die gleiche IP-Adresse für die Kommunikation mit dem Server nutzen kann, wenn beide Arten von Verbindungen aktiv sind.
- Wenn Sie einen Microsoft ISA Server verwenden, erstellen Sie einen Weblistener sowie eine Implementierungsrichtlinie für den Zugriff durch Exchange Webclients. Weitere Informationen hierzu finden Sie in der Microsoft Dokumentation.
- Legen Sie für alle Firewalls und Netzwerkgeräte die Zeitüberschreitung für inaktive Sitzungen auf 30 Minuten fest. Informationen zu den Heartbeat- und Timeout-Intervallen finden Sie in der Microsoft Exchange Dokumentation auf der Website http://technet.microsoft.com/en-us/library/cc182270.aspx.
- Konfigurieren Sie mithilfe des Exchange System Managers die Funktionen für mobile Geräte, die Richtlinien und die Einstellungen für die Gerätesicherheit. Bei Exchange Server 2007 und 2010 verwenden Sie zu diesem Zweck die Exchange Verwaltungskonsole.
- Laden und installieren Sie Microsoft Exchange ActiveSync Mobile Administration Web Tool. Dieses Tool ist für die Fernlöschfunktion erforderlich. Bei Exchange Server 2007 und 2010 kann das Fernlöschen auch mithilfe von Outlook Web Access oder der Exchange Verwaltungskonsole gestartet werden.

Unterstützte Exchange ActiveSync Sicherheitsrichtlinien

- Fernlöschen
- Zwingende Eingabe eines Gerätekennworts
- Mindestlänge für Kennwörter
- Maximalanzahl fehlgeschlagener Kennworteingaben (vor lokalem Löschen)
- Verwendung von Ziffern und Buchstaben vorschreiben
- Inaktivitätszeit in Minuten (1 bis 60 Minuten)

Zusätzliche Exchange ActiveSync Richtlinien (nur bei Exchange 2007 und 2010)

- Einfaches Kennwort zulassen oder ablehnen
- Ablaufdatum für Kennwörter
- Kennwortverlauf
- Intervall für die Aktualisierung von Richtlinien
- Mindestanzahl komplexer Zeichen in einem Kennwort
- Manuelle Synchronisierung beim Roaming vorschreiben
- Kamera zulassen
- Webbrowser zulassen

Weitere Exchange ActiveSync Dienste

- Suche in der global Adressliste
- Kalendereinladungen annehmen und erstellen
- Synchronisierungsaufgaben
- E-Mail Nachrichten markieren
- Abgleich von Markern für Antworten/Weiterleitungen (Exchange Server 2010)
- E-Mail Suche auf Exchange Server 2007 und 2010
- Unterstützung mehrerer Exchange ActiveSync E-Mail Accounts
- Zertifikatbasierte Authentifizierung
- Push-Dienste für E-Mails in ausgewählte Ordner
- Automatische Erkennung

Einfache Authentifizierung (Benutzername und Kennwort)

- Aktivieren Sie (über den Active Directory Dienst) Exchange ActiveSync für bestimmte Benutzer oder Gruppen. Diese sind in Exchange Server 2003, 2007 und 2010 standardmäßig für alle mobilen Geräte auf Unternehmensebene aktiviert. Weitere Informationen hierzu finden Sie in Exchange Server 2007 und 2010 unter „Empfängerkonfiguration“ in der Exchange Verwaltungskonsole.
- Standardmäßig ist Exchange ActiveSync für die einfache Benutzeridentifizierung konfiguriert. Es empfiehlt sich, SSL für die einfache Authentifizierung zu aktivieren, damit die Anmeldedaten bei der Authentifizierung verschlüsselt werden.

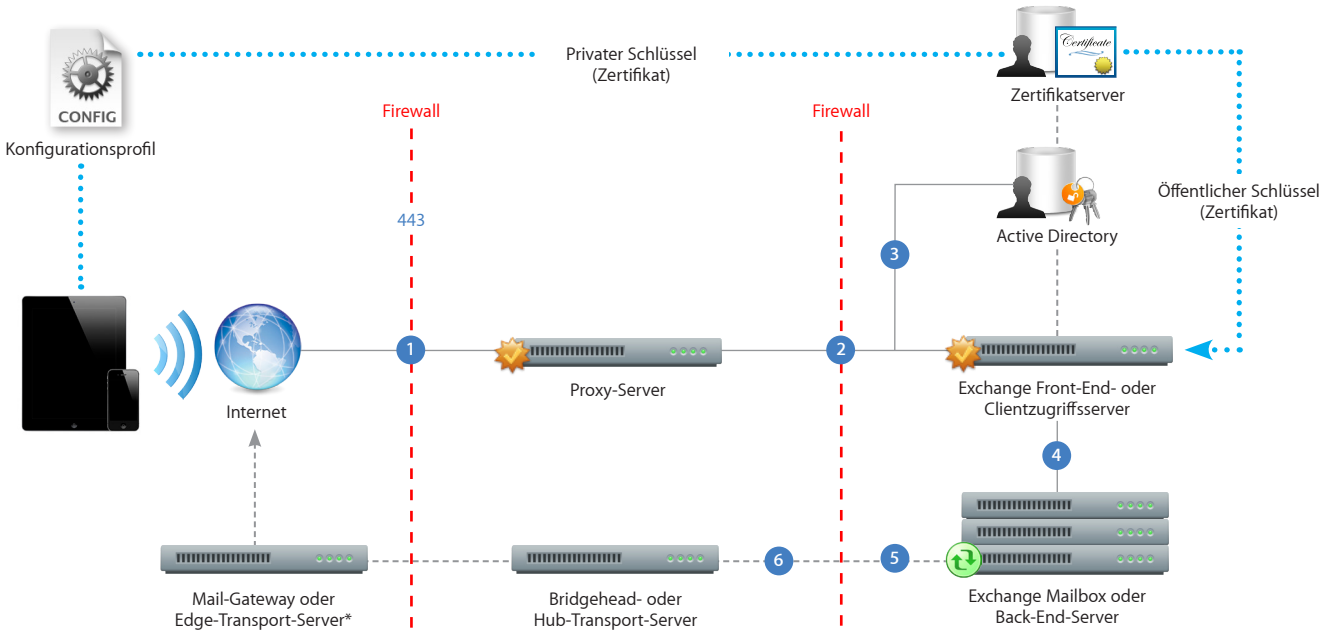
Zertifikatbasierte Authentifizierung

- Installieren Sie die Zertifikatdienste für Unternehmen auf einem Mitgliedsserver oder Domaincontroller in Ihrer Domain (dieser dient als Zertifizierungsserver).
- Konfigurieren Sie IIS auf Ihrem Exchange Front-End-Server oder Clientzugriffsserver so, dass die zertifikatbasierte Authentifizierung im virtuellen Verzeichnis von Exchange ActiveSync akzeptiert wird.
- Um Zertifikate für alle Benutzer zuzulassen oder vorzuschreiben, deaktivieren Sie „Einfache Identifizierung“ und wählen Sie entweder „Client-Zertifikate akzeptieren“ oder „Client-Zertifikate voraussetzen“.
- Erstellen Sie Client-Zertifikate mit Ihrem Zertifizierungsserver. Exportieren Sie den öffentlichen Schlüssel und konfigurieren Sie IIS für die Verwendung dieses Schlüssels. Exportieren Sie den privaten Schlüssel und verwenden Sie ein Konfigurationsprofil für die Bereitstellung dieses Schlüssels für iPhone und iPad. Die zertifikatbasierte Authentifizierung kann nur unter Verwendung eines Konfigurationsprofils konfiguriert werden.

  Für weitere Informationen zu Zertifizierungsdiensten stehen Ihnen Ressourcen von Microsoft zur Verfügung.

Implementierungsbeispiel für Exchange ActiveSync

Dieses Beispiel zeigt die Einbindung von iPhone und iPad in eine typische Microsoft Exchange Server 2003, 2007 oder 2010 Implementierung.



*Abhängig von Ihrer Netzwerkkonfiguration befindet sich das Mail-Gateway oder der Edge-Transport-Server unter Umständen innerhalb des Perimeter-Netzwerks (DMZ).

1. iPhone und iPad fordern über Port 443 (HTTPS) Zugriff auf die Exchange ActiveSync Dienste an. (Dieser Port wird auch für Outlook Web Access und andere sichere Webdienste verwendet. Daher ist er bei vielen Implementierungen bereits geöffnet und dafür konfiguriert, HTTPS-Datenverkehr mit SSL-Verschlüsselung zu ermöglichen.)
2. Der ISA-Server gewährt den Zugriff auf den Exchange Front-End- oder Clientzugriffsserver. Der ISA-Server ist als Proxy oder in vielen Fällen als Reverse-Proxy konfiguriert, um Datenverkehr an den Exchange Server zu leiten.
3. Der Exchange Server authentifiziert den eingehenden Benutzer über den Active Directory Dienst und den Zertifikatserver (bei Verwendung der zertifikatbasierten Authentifizierung).
4. Wenn der Benutzer die korrekten Zugangsdaten bereitstellt und über Zugriffsrechte für die Exchange ActiveSync-Dienste verfügt, stellt der Front-End-Server eine Verbindung zum jeweiligen Postfach auf dem Back-End-Server her (über den globalen Katalog von Active Directory).
5. Die Verbindung zu Exchange ActiveSync wird hergestellt. Aktualisierungen und Änderungen werden per Funk übertragen und sämtliche Änderungen, die auf dem iPhone bzw. iPad vorgenommen werden, werden auf dem Exchange Server nachvollzogen.
6. Gesendete E-Mails werden ebenfalls über Exchange ActiveSync mit dem Exchange Server synchronisiert (Schritt 5). Um ausgehende E-Mails an externe Empfänger zu leiten, werden sie meist über einen Bridgehead-Server (oder einen Hub-Transport-Server) per SMTP an ein externes Mail-Gateway (oder einen Edge-Transport-Server) geleitet. Abhängig von Ihrer Netzwerkkonfiguration befindet sich das externe Mail-Gateway oder der Edge-Transport-Server unter Umständen innerhalb des Perimeter-Netzwerks oder außerhalb der Firewall.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, iPhone, iPad und Mac OS sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Dieses Material dient ausschließlich zu Informationszwecken. Apple übernimmt keine Haftung hinsichtlich der Verwendung. Oktober 2011 L419822B

Implementierung von iPhone und iPad

Standardbasierte Dienste

Durch Unterstützung des IMAP E-Mail Protokolls, der LDAP Verzeichnisdienste und der Protokolle CalDAV und CardDAV für Kalender- und Kontaktdaten kann iOS in praktisch jede Standardumgebung mit E-Mail, Kalender- und Kontaktfunktionen eingebunden werden. Wenn die Netzwerkumgebung so konfiguriert ist, dass eine Benutzeridentifizierung und die SSL-Verschlüsselung erforderlich sind, bieten iPhone und iPad ein extrem sicheres Konzept für den Zugriff auf standardbasierte E-Mail, Kalender und Kontakte des Unternehmens.

In einer typischen Implementierung stellen iPhone und iPad den direkten Zugriff auf IMAP und SMTP Mail Server her. So können E-Mails drahtlos empfangen und gesendet werden, und auch das drahtlose Synchronisieren von Notizen mit IMAP-basierten Servern ist möglich. iOS Geräte können die Verbindung mit den allgemeinen LDAPv3 Verzeichnissen Ihres Unternehmens herstellen. Damit haben die Benutzer Zugriff auf unternehmensinterne Kontakte in den Programmen „Mail“, „Kontakte“ und „Nachrichten“. Die Synchronisierung mit Ihrem CalDAV Server erlaubt es Benutzern von iPhone und iPad, drahtlos Kalendereinladungen zu erstellen und anzunehmen, Kalenderaktualisierungen zu empfangen und Aufgaben mit der App „Erinnerungen“ zu synchronisieren. Und dank der Unterstützung für CardDAV können Ihre Benutzer das vCard Format nutzen und so ihre Kontakte mit Ihrem CardDAV Server synchronisieren. Alle Netzwerkserver können sich innerhalb eines DMZ-Teilnetzes und/oder hinter einer Firmen-Firewall befinden. iOS unterstützt mit SSL 128-Bit Verschlüsselung und X.509 Root-Zertifikate, die von führenden Zertifizierungsstellen ausgestellt wurden.

Netzwerkkonfiguration

Ihr IT- oder Netzwerkadministrator muss die folgenden grundlegenden Schritte ausführen, um den Zugriff vom iPhone und iPad auf IMAP, LDAP, CalDAV und CardDAV Dienste zu ermöglichen:

- Öffnen Sie die entsprechenden Ports in der Firewall. Die üblichen Ports sind 993 (für IMAP Mail), 587 (für SMTP Mail), 636 für LDAP Verzeichnisdienste, 8443 für CalDAV Kalenderfunktionen und 8843 für CardDAV Kontakte. Es empfiehlt sich außerdem, die Kommunikation zwischen Ihrem Proxy-Server und den Back-End-Servern für IMAP, LDAP, CalDAV und CardDAV für die Nutzung von SSL einzurichten und digitale Zertifikate auf Ihren Netzwerkservern durch eine vertrauenswürdige Zertifizierungsstelle (CA) wie etwa VeriSign signieren zu lassen. Dieser wichtige Schritt stellt sicher, dass iPhone und iPad Ihren Proxy-Server als verlässliche Einheit innerhalb Ihrer Unternehmensinfrastruktur erkennen.
- Für das Senden von SMTP E-Mails muss Port 587, 465 oder 25 geöffnet sein. iOS überprüft automatisch Port 587, dann 465 und schließlich 25. Port 587 ist der zuverlässigste und sicherste Port, da er Benutzerauthentifizierung erfordert. Port 25 erfordert keine Benutzerauthentifizierung. Er wird außerdem von einigen Internetanbietern standardmäßig gesperrt, um unerwünschte E-Mails (Spam) zu verhindern.

Gemeinsame Ports

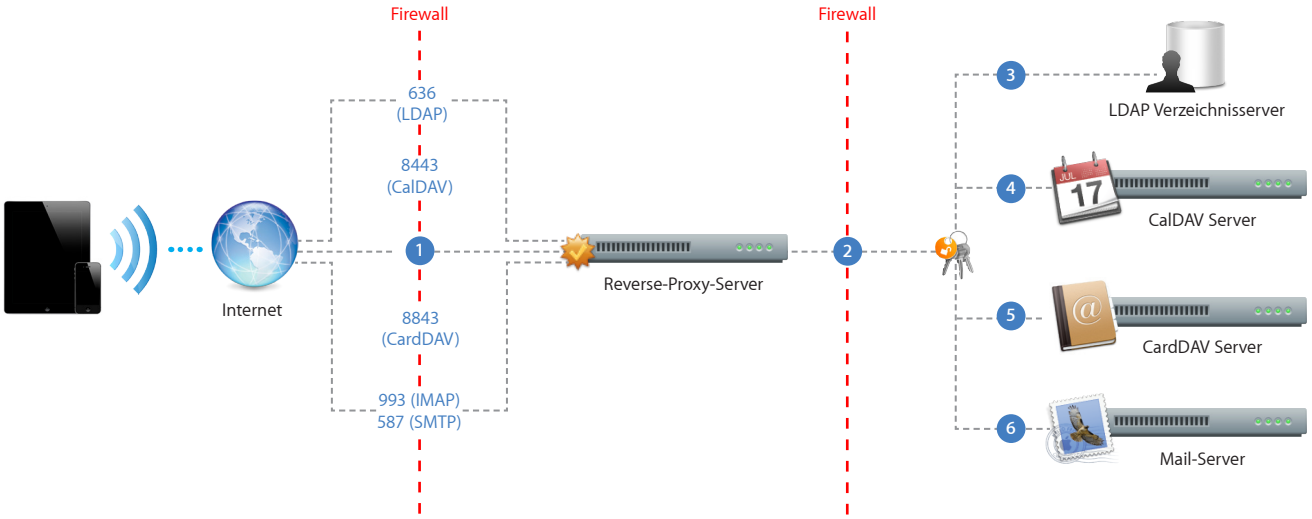
- IMAP/SSL: 993
- SMTP/SSL: 587
- LDAP/SSL: 636
- CalDAV/SSL: 8443, 443
- CardDAV/SSL: 8843, 443

IMAP- oder POP-fähige E-Mail Lösungen
iOS unterstützt standardkonforme IMAP4- und POP3-fähige Mail-Server auf einer Reihe von Serverplattformen wie Windows, UNIX, Linux und Mac OS X.

CalDAV und CardDAV Standards
iOS unterstützt die CalDAV Kalender- und CardDAV Kontaktprotokolle. Beide Protokolle wurden von der IETF standardisiert. Weitere Informationen finden Sie über das CalConnect Consortium unter der Adresse http://caldav.calconnect.org/ und http://carddav.calconnect.org/.

Implementierungsbeispiel

Dieses Beispiel zeigt, wie iPhone und iPad die Verbindung zu einer typischen IMAP, LDAP, CalDAV und CardDAV Implementierung herstellen.



1. iPhone und iPad fordern über die vorgegebenen Ports Zugriff auf die Netzwerkdienste an.
2. Abhängig vom jeweiligen Dienst müssen sich die Benutzer entweder beim Reverse-Proxy oder direkt bei dem Server identifizieren, um Zugriff auf die Unternehmensdaten zu erhalten. In allen Fällen werden die Verbindungen über den Reverse-Proxy weitergeleitet. Dieser fungiert als sicheres Gateway und befindet sich normalerweise hinter der Internet-Firewall des Unternehmens. Nach erfolgter Identifizierung können die Benutzer auf die Unternehmensdaten auf den Back-End-Servern zugreifen.
3. iPhone und iPad bieten Suchdienste für LDAP-Verzeichnisse, wodurch Benutzer nach Kontakten und anderen Adressbuchinformationen auf dem LDAP-Server suchen können.
4. Mit dem CalDAV Protokoll können die Benutzer auf Kalender zugreifen und diese aktualisieren.
5. CardDAV Kontaktdaten werden auf dem Server gespeichert und sind auch lokal auf iPhone und iPad zugänglich. Änderungen an Feldern in den CardDAV Kontakten werden auf dem CardDAV Server synchronisiert.
6. Mit IMAP E-Mail Diensten können auf iPhone und iPad über die Proxy-Verbindung mit dem Mail-Server bereits vorhandene und neue Nachrichten gelesen werden. Ausgehende E-Mails werden zum SMTP-Server gesendet. Dabei werden Kopien im Ordner für gesendete E-Mails des Benutzers abgelegt.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, iPhone, iPad und Mac OS sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. UNIX ist eine eingetragene Marke von The Open Group. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Dieses Material dient ausschließlich zu Informationszwecken. Apple übernimmt keine Haftung hinsichtlich der Verwendung. Oktober 2011 L419827B

Implementierung von iPhone und iPad

Virtuelle private Netzwerke

Der sichere Zugriff auf private Unternehmensnetzwerke wird auf iPhone und iPad mithilfe der VPN-Protokolle (Virtual Private Network) nach dem Industriestandard sichergestellt. Die Benutzer können über den in iOS integrierten VPN-Client oder über Programme anderer Hersteller wie Juniper, Cisco und F5 Networks die Verbindung zu Unternehmensnetzwerken herstellen.

iOS unterstützt ab Werk Cisco IPSec, L2TP über IPSec und PPTP. Wenn Ihr Unternehmen eines dieser Protokolle unterstützt, sind keine zusätzlichen Netzwerkkonfigurationen oder Programme anderer Hersteller erforderlich, um das iPhone und das iPad mit Ihrem VPN zu verbinden.

iOS unterstützt darüber hinaus SSL VPN und ermöglicht somit den Zugriff auf SSL VPN-Server der Juniper SA Serie, von Cisco ASA und F5 BIG-IP Edge Gateway. Die Benutzer laden einfach die von Juniper, Cisco oder F5 entwickelte VPN-Client-App aus dem App Store. Wie andere in iOS unterstützte VPN-Protokolle kann auch SSL VPN entweder manuell auf dem Gerät oder über ein Konfigurationsprofil eingerichtet werden.

iOS unterstützt standardkonforme Technologien wie IPv6, Proxy Server und Split-Tunneling und ermöglicht damit eine leistungsstarke VPN-Kommunikation bei der Verbindung zu Firmennetzwerken. iOS kann mit einer Vielzahl verschiedener Authentifizierungsmethoden arbeiten, z. B. Kennwort, Two-Factor-Token und digitalen Zertifikaten. Zur Optimierung der Verbindung in Umgebungen, in denen die zertifikatbasierte Authentifizierung verwendet wird, stellt iOS die Funktion „VPN On Demand“ bereit. Damit wird beim Herstellen der Verbindung zu bestimmten Domains eine VPN-Sitzung dynamisch aufgebaut.

Unterstützte Protokolle und Authentifizierungsmethoden

SSL VPN
Unterstützt die Benutzerauthentifizierung per Kennwort, Two-Factor-Token und Zertifikaten.

Cisco IPSec
Unterstützt die Benutzerauthentifizierung per Kennwort und Two-Factor-Token sowie die Systemauthentifizierung per gemeinsamem geheimen Schlüssel (Shared Secret) und Zertifikaten.

L2TP over IPSec
Unterstützt die Benutzerauthentifizierung per MS-CHAP v2 Kennwort und Two-Factor-Token sowie die Systemauthentifizierung per gemeinsamem geheimen Schlüssel (Shared Secret).

PPTP
Unterstützt die Benutzerauthentifizierung per MS-CHAP v2 Kennwort und Two-Factor-Token.

VPN On Demand

Für Konfigurationen, die eine zertifikatbasierte Authentifizierung verwenden, unterstützt iOS VPN On Demand. VPN On Demand stellt automatisch eine Verbindung her, wenn auf vordefinierte Domains zugegriffen wird. Dies ermöglicht Benutzern eine nahtlose VPN-Konnektivität.

Diese iOS Funktion erfordert keine zusätzliche Serverkonfiguration. Die Konfiguration von VPN On Demand erfolgt über ein Konfigurationsprofil, kann aber auch manuell auf dem Gerät eingerichtet werden.

Die Optionen für VPN On Demand sind:

Immer (Always)
Stellt für jede Adresse, die mit der angeführten Domain übereinstimmt, eine VPN-Verbindung her.

Nie (Never)
Stellt keine VPN-Verbindung für Adressen her, die zu der angegebenen Domain passen, aber wenn VPN bereits aktiv ist, kann es verwendet werden.

Bei Bedarf herstellen (Establish if needed)
Stellt nur im Fall einer fehlgeschlagenen DNS-Auflösung eine VPN-Verbindung für Adressen her, die zu der angegebenen Domain passen.

Einrichtung von VPNs

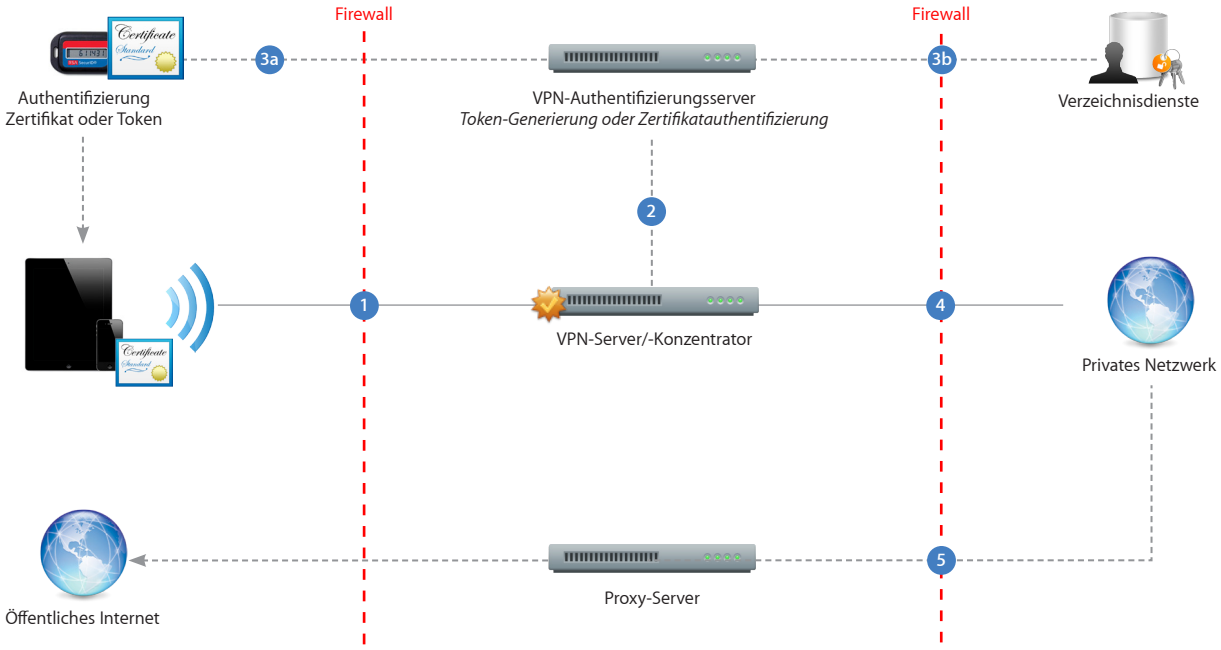
- iOS kann bei minimalem Konfigurationsaufwand mit vielen vorhandenen VPN-Netzwerken integriert werden. Zur Vorbereitung der Implementierung empfiehlt es sich, zunächst zu prüfen, ob die in Ihrem Unternehmen genutzten VPN-Protokolle und Identifizierungsverfahren von iOS unterstützt werden.
- Es empfiehlt sich, den Identifizierungspfad zu Ihrem Authentifizierungsserver zu prüfen, damit sichergestellt ist, dass die von iOS unterstützten Standards innerhalb Ihrer Implementierung aktiviert sind.
- Wenn Sie eine zertifikatbasierte Identifizierung verwenden möchten, muss sichergestellt sein, dass die Infrastruktur für die Public-Key-Infrastruktur (PKI) Schlüssel so konfiguriert ist, dass geräte- und benutzerbasierte Zertifikate vom entsprechenden Schlüsselverteilungsprozess unterstützt werden.
- Wenn Sie URL-spezifische Proxy-Einstellungen konfigurieren möchten, legen Sie eine PAC-Datei auf einen Webserver, auf den mit den grundlegenden VPN-Einstellungen zugegriffen werden kann, und achten Sie darauf, dass er mit dem MIME-Typ application/x-ns-proxy-autoconfig bereitgestellt wird.

Proxy-Konfiguration

Für alle Konfigurationen können Sie außerdem einen VPN-Proxy angeben. Um einen einzigen Proxy für alle Verbindungen zu konfigurieren, verwenden Sie die Einstellung „Manuell“ und geben Sie die Serveradresse, den Port sowie – falls nötig – die Authentifizierungsdaten an. Zur Bereitstellung des Geräts mit einer Auto-Proxy-Konfigurationsdatei unter Verwendung von PAC oder WPAD verwenden Sie die Einstellung „Auto“. Bei PACS geben Sie die URL-Adresse der PACS-Datei an. Bei WPAD ermitteln iPhone und iPad die korrekten Einstellungen per DHCP- und DNS-Abfrage.

Implementierungsbeispiel

Das Beispiel zeigt eine typische Implementierung mit einem VPN-Server/-Konzentrator sowie einem Authentifizierungsserver, der den Zugriff auf die Netzwerkdienste des Unternehmens steuert.



1. iPhone und iPad fordern den Zugriff auf Netzwerkdienste an.
2. Der VPN-Server/-Konzentrator erhält die Anforderung und leitet diese anschließend an den Authentifizierungsserver weiter.
3. In einer Umgebung mit Identifizierung per Two-Factor-Token erstellt der Authentifizierungsserver dann mit dem Schlüsselserver ein zeitsynchronisiertes Identifizierungs-Token. Bei Implementierung einer zertifikatbasierten Authentifizierungsmethode muss vor der Authentifizierung ein Identitätszertifikat ausgegeben werden. Wenn eine Kennwortmethode eingesetzt wird, fährt der Identifizierungsprozess mit der Benutzervalidierung fort.
4. Sobald ein Benutzer identifiziert ist, prüft der Authentifizierungsserver die Benutzer- und Gruppenrichtlinien.
5. Nachdem die Benutzer- und Gruppenrichtlinien überprüft worden sind, gewährt der VPN-Server getunnelten und verschlüsselten Zugriff auf die Netzwerkdienste.
6. Wird ein Proxy-Server verwendet, stellen iPhone und iPad die Verbindung über den Proxy-Server her, um auf Informationen außerhalb der Firewall zugreifen zu können.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, iPhone, iPad und Mac OS sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. App Store ist eine Dienstleistungsmarke der Apple Inc. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Dieses Material dient ausschließlich zu Informationszwecken; Apple übernimmt keine Haftung hinsichtlich der Verwendung. Oktober 2011 L419828B

Implementierung von iPhone und iPad
Wi-Fi

Wireless-Sicherheitsprotokolle

- WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

802.1X Identifizierungsverfahren

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAPv0 (EAP-MS-CHAP v2)
- PEAPv1 (EAP-GTC)
- LEAP

iPhone und iPad können bereits ab Werk eine sichere Verbindung zu Unternehmens- oder anderen Wi-Fi Netzwerken herstellen, sodass Sie sich überall schnell und einfach mit verfügbaren Funknetzwerken verbinden können.

iOS unterstützt standardmäßige Protokolle für drahtlose Netzwerke, einschließlich WPA2 Enterprise. Damit ist sichergestellt, dass drahtlose Unternehmensnetzwerke schnell konfigurierbar und leicht zugänglich sind. WPA2 Enterprise arbeitet mit 128-Bit-AES-Verschlüsselung, einem bewährten blockbasierten Verschlüsselungsverfahren, das ein hohes Maß an Sicherheit für die Unternehmensdaten bietet.

Da iOS den Standard 802.1X unterstützt, lässt es sich in eine Vielzahl von RADIUS-Authentifizierungsumgebungen integrieren. iPhone und iPad unterstützen unter anderem folgende 802.1X Identifizierungsverfahren für Funknetzwerke: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 und LEAP.

Benutzer können das iPhone und das iPad für eine automatische Verbindung mit verfügbaren Wi-Fi Netzwerken konfigurieren. Wi-Fi Netzwerke, die Anmeldedaten oder andere Informationen verlangen, sind aus Wi-Fi Einstellungen oder innerhalb von Apps wie Mail schnell zugänglich, ohne dass eine separate Browsersitzung gestartet werden muss. Und dank der Möglichkeit, ohne hohen Stromverbrauch Verbindungen mit Wi-Fi Netzwerken aufrechtzuerhalten, können Programme Push-Benachrichtigungen per Wi-Fi übertragen.

Die Netzwerk-, Sicherheits-, Proxy- und Authentifizierungseinstellungen können über Konfigurationsprofile vorgenommen werden, um eine schnelle Einrichtung und Anwendung zu ermöglichen.

Einrichtung von WPA2 Enterprise

- Prüfen Sie die Kompatibilität der Netzwerkgeräte und wählen Sie einen Authentifizierungstyp (EAP-Typ), der von iOS unterstützt wird.
- Vergewissern Sie sich, dass 802.1x auf dem Authentifizierungsserver aktiviert ist, installieren Sie gegebenenfalls ein Serverzertifikat und weisen Sie den Benutzern und Gruppen die entsprechenden Berechtigungen für den Netzwerkzugriff zu.
- Konfigurieren Sie die drahtlosen Zugangspunkte (WAP – Wireless Access Points) für die 802.1x Identifizierung und geben Sie die entsprechenden Informationen für den RADIUS-Server ein.
- Wenn Sie eine zertifikatbasierte Identifizierung verwenden möchten, konfigurieren Sie die Public-Key-Infrastruktur (PKI) so, dass geräte- und benutzerbasierte Zertifikate vom entsprechenden Schlüsselverteilungsprozess unterstützt werden.
- Prüfen Sie das Zertifikatformat und die Kompatibilität mit dem Authentifizierungsserver. iOS unterstützt PKCS1 (.cer, .crt, .der) und PKCS12.
- Weitere Dokumentation zu Standards für Funknetzwerke und Wi-Fi Protected Access (WPA) finden Sie unter www.wi-fi.org (nur in englischer Sprache verfügbar).

Implementierungsbeispiel für WPA2 Enterprise/802.1X

Dieses Beispiel zeigt eine typische sichere Implementierung für ein Funknetzwerk, bei der RADIUS-basierte Authentifizierung eingesetzt wird.

1. iPhone und iPad fordern den Zugriff auf das Netzwerk an. Die Verbindung wird aufgebaut, sobald ein Benutzer ein verfügbares drahtloses Netzwerk ausgewählt hat, oder sie wird automatisch gestartet, nachdem ein zuvor konfiguriertes Netzwerk erkannt wurde.
2. Nachdem der Zugangspunkt die Anforderung empfangen hat, wird sie zur Identifizierung an den RADIUS-Server weitergeleitet.
3. Der RADIUS-Server lässt den Benutzeraccount vom Verzeichnisdienst validieren.
4. Sobald der Benutzer authentifiziert ist, gewährt der Zugangspunkt den Netzwerkzugriff gemäß den Richtlinien und Zugriffsrechten, die er vom RADIUS-Server empfängt.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, iPhone, iPad und Mac OS sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Dieses Material dient ausschließlich zu Informationszwecken; Apple übernimmt keine Haftung hinsichtlich der Verwendung. Oktober 2011 L419830B

Implementierung von iPhone und iPad

Digitale Zertifikate

Unterstützte Zertifikat- und Identitätsformate:

- iOS unterstützt X.509 Zertifikate mit RSA-Schlüsseln.
- Die Dateierweiterungen .cer, .crt, .der, .p12 und .pfx werden erkannt.

Root-Zertifikate

Ab Werk enthält iOS eine Reihe vorab installierter Root-Zertifikate. Eine Liste der vorinstallierten Root-Zertifikate des Systems finden Sie im folgenden Apple Support-Artikel: http://support.apple.com/kb/HT4415. Wenn Sie ein nicht vorinstalliertes Root-Zertifikat verwenden, z. B. ein selbst signiertes, von Ihrem Unternehmen erstelltes Root-Zertifikat, können Sie dieses mit einer der im Abschnitt „Verteilen und Installieren von Zertifikaten“ angegebenen Methoden verteilen.

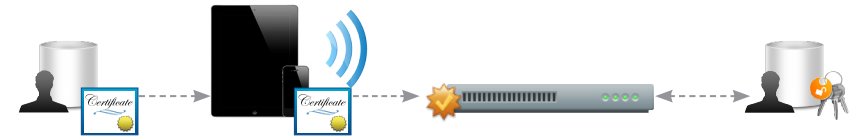
iOS unterstützt digitale Zertifikate und ermöglicht Unternehmenskunden so einen sicheren, effizienten Zugang zu Unternehmensdiensten. Ein digitales Zertifikat setzt sich aus einem öffentlichen Schlüssel, Informationen über den Benutzer und der Zertifizierungsstelle zusammen, die das Zertifikat ausgestellt hat. Digitale Zertifikate sind eine Form der Identifizierung, die optimierte Authentifizierung, Datenintegrität und Verschlüsselung ermöglicht.

Auf iPhone und iPad lassen sich Zertifikate auf verschiedene Arten nutzen. Das Signieren von Daten mit einem digitalen Zertifikat trägt zum Schutz vor Manipulation der Informationen bei. Zertifikate können auch zur zweifelsfreien Garantie der Identität des Autors oder „Unterzeichners“ verwendet werden. Zusätzlich dienen sie auch zum Verschlüsseln von Konfigurationsprofilen und der Netzwerkkommunikation für den weitergehenden Schutz vertraulicher oder privater Informationen.

Verwenden von Zertifikaten in iOS

Digitale Zertifikate

Digitale Zertifikate können zur sicheren Authentifizierung von Benutzern bei Unternehmensdiensten verwendet werden, ohne dass dafür Benutzernamen, Kennwörter oder Software-Token nötig sind. iOS unterstützt die zertifikatsbasierte Authentifizierung für den Zugriff auf Microsoft Exchange ActiveSync, VPN und Wi-Fi Netzwerke.



Serverzertifikate

Digitale Zertifikate können auch dazu genutzt werden, die Kommunikation im Netzwerk zu prüfen und zu verschlüsseln. Dies sorgt für eine sichere Kommunikation mit internen und externen Websites. Der Safari Browser kann die Gültigkeit eines digitalen X.509 Zertifikats prüfen und eine sichere Sitzung mit bis zu 256-Bit AES-Verschlüsselung einleiten. Damit wird überprüft, ob die Identität der Website zulässig und die Kommunikation mit der Website geschützt ist. Auf diese Weise wird das Abfangen persönlicher oder vertraulicher Daten verhindert.

Verteilen und Installieren von Zertifikaten

Das Verteilen von Zertifikaten für iPhone und iPad ist einfach. Bei Empfang eines Zertifikats können die Benutzer durch einfaches Tippen den Inhalt anzeigen und lesen und dann durch nochmaliges Tippen das Zertifikat zu ihrem Gerät hinzufügen. Wenn ein Identitätszertifikat installiert ist, werden die Benutzer zur Eingabe des Kennworts aufgefordert, das als Schutz der Identität dient. Kann die Echtheit eines Zertifikats nicht bestätigt werden, erhalten die Benutzer eine Warnmeldung, bevor das Zertifikat zum Gerät hinzugefügt wird.

Installieren von Zertifikaten über Konfigurationsprofile

Wenn Konfigurationsprofile zum Ausgeben von Einstellungen für Unternehmensdienste wie Exchange, VPN oder Wi-Fi genutzt werden, können für eine optimierte Implementierung auch Zertifikate zum Profil hinzugefügt werden.

Installieren von Zertifikaten via Mail oder Safari

Wenn ein Zertifikat per E-Mail gesendet wird, erscheint es dort als Anhang. Safari kann zum Laden von Zertifikaten von einer Webseite verwendet werden. Sie können ein Zertifikat auf einer sicheren Website bereitstellen und Benutzern die URL-Adresse zur Verfügung stellen, unter der sie das Zertifikat auf ihre Geräte laden können.

Installation via SCEP (Simple Certificate Enrollment Protocol)

SCEP ist darauf ausgelegt, die Zertifikatausgabe bei Implementierungen im großen Maßstab zu vereinfachen. Dies ermöglicht die kabellose Registrierung digitaler Zertifikate auf iPhone und iPad, die danach für die Authentifizierung bei Unternehmensdiensten genutzt werden können. Auch die Registrierung bei einem MDM-Server (Mobile Device Management) wird dadurch ermöglicht.

Informationen zu SCEP und zur kabellosen Registrierung finden Sie unter www.apple.com/iphone/business/resources.

Entfernen und Sperren von Zertifikaten

Zum manuellen Entfernen eines zuvor installierten Zertifikats wählen Sie „Einstellungen" > „Allgemein" > „Profile". Wenn Sie ein Zertifikat entfernen, das für den Zugriff auf einen Account oder ein Netzwerk benötigt wird, kann das Gerät nicht mehr auf die jeweiligen Dienste zugreifen.

Für das drahtlose Entfernen von Zertifikaten kann ein MDM-Server verwendet werden. Dieser Server kann alle Zertifikate auf einem Gerät anzeigen und diejenigen entfernen, die er selbst installiert hat.

Zusätzlich wird das OCSP (Online Certificate Status Protocol) unterstützt, das den Status von Zertifikaten überprüft. Wenn ein OSCP-fähiges Zertifikat verwendet wird, überprüft iOS dieses um sicherzustellen, dass es nicht vor Abschluss der angeforderten Aufgabe gesperrt wurde.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, iPhone, iPad und Mac OS sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Dieses Material dient ausschließlich zu Informationszwecken. Apple übernimmt keine Haftung hinsichtlich der Verwendung. Oktober 2011 L419821B

Implementierung von iPhone und iPad
Sicherheitsaspekte

Gerätesicherheit
- Komplexe Codes
- Ablauf von Codes
- Verlauf der Wiederverwendung von Codes
- Maximale Anzahl an Fehleingaben
- Codezwang für drahtlose Verbindungen
- Progressive Zeitüberschreitung für Codes

iOS, das Betriebssystem, das den Kern von iPhone und iPad bildet, ist auf mehreren Sicherheitsebenen aufgebaut. Dies ermöglicht iPhone und iPad den sicheren Zugriff auf Unternehmensdienste bei gleichzeitigem Schutz wichtiger Daten. iOS sorgt für komplexe Verschlüsselung der Daten bei der Übertragung, bewährte Authentifizierungsmethoden für den Zugriff auf Unternehmensdienste und Hardwareverschlüsselung aller gespeicherten Daten. iOS sorgt auch für sicheren Schutz durch Coderichtlinien, die auch drahtlos bereitgestellt und umgesetzt werden können. Und sollte ein Gerät in falsche Hände gelangen, können Benutzer und IT-Administratoren den Befehl zum Fernlöschen geben, wodurch sämtliche vertraulichen Informationen gelöscht werden.

Wenn es um die Sicherheit von iOS beim Einsatz in Unternehmen geht, sind die folgenden Konzepte relevant:
- **Gerätesicherheit:** Methoden zur Verhinderung unbefugter Nutzung des Geräts
- **Datensicherheit:** Schutz gespeicherter Daten, auch bei Verlust oder Diebstahl eines Geräts
- **Netzwerksicherheit:** Netzwerkprotokolle und Verschlüsselung der Daten bei der Übertragung
- **Sicherheit von Apps:** Sichere Plattform von iOS

Diese Funktionen arbeiten Hand in Hand und stellen so eine sichere Plattform für das mobile Computing bereit.

Gerätesicherheit

Die Etablierung strenger Richtlinien für den Zugriff auf iPhone und iPad ist entscheidend für den Schutz von Unternehmensinformationen. Gerätecodes sind der primäre Schutz gegen unbefugten Zugriff und können auch per drahtloser Übertragung konfiguriert und umgesetzt werden. iOS Geräte nutzen den eindeutigen, von jedem einzelnen Benutzer festgelegten Code zum Generieren einer komplexen Verschlüsselung, die zusätzlichen Schutz für Mail und vertrauliche Programmdaten auf dem Gerät gewährt. Zusätzlich bietet iOS sichere Methoden zum Konfigurieren des Geräts in Unternehmensumgebungen, in denen bestimmte Einstellungen, Richtlinien und Einschränkungen vorliegen müssen. Diese Methoden stellen für autorisierte Benutzer flexible Möglichkeiten bereit, um ein Standardniveau an Schutz herzustellen.

Coderichtlinien
Ein Gerätecode verhindert, dass unbefugte Benutzer auf Daten zugreifen oder sich anderweitig Zugang zum Gerät verschaffen. Um Ihrem Sicherheitsbedarf Rechnung zu tragen, stellt iOS eine umfangreiche Auswahl an Codeanforderungen bereit, darunter Zeitüberschreitungsintervalle sowie Zuverlässigkeit und Änderungshäufigkeit des Codes.

Die folgenden Coderichtlinien werden unterstützt:
- Zwingende Eingabe eines Gerätecodes
- Einfacher Wert zulässig
- Verlangen eines alphanumerischen Werts
- Mindestlänge für Codes
- Mindestanzahl komplexer Zeichen
- Maximale Gültigkeitsdauer für Codes
- Zeit bis zur automatischen Sperre
- Codeverlauf
- Nachfrist für Gerätesperre
- Maximale Anzahl Fehlversuche

Unterstützte konfigurierbare Richtlinien und Einschränkungen:

Gerätefunktionalität
- Installieren von Apps erlauben
- Siri erlauben
- Verwendung der Kamera erlauben
- FaceTime erlauben
- Bildschirmfoto erlauben
- Automatisches Synchronisieren beim Roaming erlauben
- Wählen per Spracheingabe erlauben
- In-App-Käufe erlauben
- Store-Kennwort für alle Einkäufe verlangen
- Gaming mit mehreren Spielern zulassen
- Hinzufügen von Freunden im Game Center erlauben

Programme
- Verwendung von YouTube erlauben
- Verwendung des iTunes Store erlauben
- Verwendung von Safari erlauben
- Safari Sicherheitseinstellungen festlegen

iCloud
- Datensicherung erlauben
- Synchronisierung von Dokumenten und Schlüsselwerten erlauben
- Fotostream erlauben

Sicherheit und Datenschutz
- Senden von Diagnosedaten an Apple erlauben
- Akzeptieren nicht verlässlicher Zertifikate durch den Benutzer erlauben
- Verschlüsselte Backups erzwingen.

Inhaltsbewertungen
- Ungeeignete/anstößige Musik und Podcasts erlauben
- Wertungsbereich festlegen
- Zulässige Inhaltswertungen festlegen

Durchsetzung von Richtlinien

Die oben beschriebenen Richtlinien können auf iPhone und iPad auf mehrere Arten festgelegt werden. Richtlinien können als Teil eines Konfigurationsprofils verteilt und von den Benutzern installiert werden. Ein Profil kann so definiert werden, dass es nur mit einem Administratorkennwort gelöscht werden kann. Alternativ kann festgelegt werden, dass es auf dem Gerät gesperrt wird und nicht entfernt werden kann, ohne den gesamten Inhalt des Geräts zu löschen. Darüber hinaus können Codeeinstellungen auch zentral konfiguriert werden. Dazu dienen MDM-Lösungen (Mobile Device Management), mit denen Richtlinien per Push-Technologie direkt an das Gerät gesendet werden können. Auf diese Weise können die Richtlinien ohne Eingriff der Benutzer durchgesetzt und aktualisiert werden.

Ist das Gerät hingegen für den Zugriff auf einen Microsoft Exchange Account konfiguriert, werden die Exchange ActiveSync Richtlinien drahtlos auf das Gerät gepusht. Beachten Sie, dass die verfügbaren Richtlinien von der Exchange Version (2003, 2007 oder 2010) abhängig sind. Unter *Exchange ActiveSync und iOS Geräte* finden Sie einen kurzen Überblick über die für Ihre jeweilige Konfiguration unterstützten Richtlinien.

Sichere Gerätekonfiguration

Konfigurationsprofile sind XML-Dateien, die für die Gerätesicherheit relevante Richtlinien und Einschränkungen, VPN-Konfigurationsdaten, Wi-Fi Einstellungen, E-Mail und Kalenderaccounts sowie Authentifizierungsdaten enthalten, die es dem iPhone und dem iPad ermöglichen, mit den Systemen Ihres Unternehmens zusammenzuarbeiten. Die Möglichkeit, Coderichtlinien zusammen mit Geräteeinstellungen in einem Konfigurationsprofil festzulegen, stellt sicher, dass die Geräte im Unternehmen korrekt und gemäß den Sicherheitsstandards Ihres Unternehmens konfiguriert werden. Da sich Konfigurationsprofile sowohl verschlüsseln als auch sperren lassen, können die Einstellungen nicht entfernt, verändert oder weitergegeben werden.

Konfigurationsprofile können sowohl signiert als auch verschlüsselt werden. Durch Signieren eines Konfigurationsprofils wird sichergestellt, dass die dadurch vorgegebenen Einstellungen in keiner Weise geändert werden können. Durch die Verschlüsselung eines Konfigurationsprofils wird der Inhalt des Profils geschützt. Es kann nur auf dem Gerät installiert werden, für das es erstellt wurde. Konfigurationsprofile werden über CMS (Cryptographic Message Syntax, gemäß RFC 3852) verschlüsselt, wobei 3DES und AES-128 unterstützt werden.

Bei der erstmaligen Ausgabe verschlüsselter Konfigurationsprofile müssen diese per USB Synchronisierung mit dem Konfigurationsprogramm oder per kabelloser Registrierung übertragen werden. Zusätzlich kann die nachfolgende Verteilung verschlüsselter Konfigurationsprofile per E-Mail Anhang, über eine Website, auf die die Benutzer Zugriff haben, oder mithilfe der Push-Funktion von MDM-Lösungen erfolgen.

Geräteinschränkungen

Die Einschränkungen bestimmen, auf welche Funktionen die Benutzer auf dem Gerät zugreifen können. Normalerweise handelt es sich dabei um netzwerkfähige Programme wie Safari, YouTube und den iTunes Store, aber auch Funktionen wie die Installation von Programmen oder die Verwendung der Kamera können eingeschränkt werden. Mit diesen Einschränkungen können Sie das Gerät für Ihren Bedarf konfigurieren und den Benutzern die Nutzung des Geräts gemäß den Unternehmensvorgaben gestatten. Die Einschränkungen können manuell auf den einzelnen Geräten konfiguriert, mithilfe eines Konfigurationsprofils durchgesetzt oder mithilfe von MDM-Lösungen per Fernzugriff festgelegt werden. Darüber hinaus können Einschränkungen der Webnutzung oder Kamera ebenso wie Coderichtlinien kabellos über Microsoft Exchange Server 2007 und 2010 umgesetzt werden.

Zusätzlich zum Festlegen von Einschränkungen und Richtlinien auf dem Gerät kann die IT-Abteilung das iTunes Schreibtischprogramm konfigurieren und steuern. Hierzu gehört das Sperren des Zugriffs auf ungeeignete bzw. anstößige Inhalte, das Festlegen, auf welche Netzwerkdienste der Benutzer innerhalb von iTunes zugreifen darf und ob er neue Softwareaktualisierungen installieren darf. Weitere Informationen dazu enthält der Artikel *Deploying iTunes for iOS Devices*.

Datensicherheit

Datensicherheit
- Hardwareverschlüsselung
- Datenschutz
- Fernlöschen
- Lokales Löschen
- Verschlüsselte Konfigurationsprofile
- Verschlüsselte iTunes Backups

Der Schutz der auf iPhone und iPad gespeicherten Daten ist für jede Umgebung mit sensiblen Unternehmens- oder Kundendaten wichtig. Zusätzlich zur Datenverschlüsselung während der Übertragung unterstützen iPhone und iPad die Hardwareverschlüsselung für alle auf dem Gerät gespeicherten Daten und die zusätzliche Verschlüsselung von E-Mail und Programmdaten für verbesserten Datenschutz.

Es ist wichtig, Geräte bei Verlust oder Diebstahl zu deaktivieren und die darauf befindlichen Daten zu löschen. Es empfiehlt sich auch festzulegen, dass nach einer bestimmten Anzahl von ungültigen Codeeingaben sämtliche Daten auf dem Gerät gelöscht werden. Mit dieser Maßnahme lassen sich unbefugte Zugriffe auf das Gerät verhindern.

Verschlüsselung
iPhone und iPad bieten eine hardwarebasierte Verschlüsselung. Die Hardwareverschlüsselung verwendet 256-Bit AES-Codierung, um die Daten auf dem Gerät zu schützen. Die Verschlüsselung ist immer aktiv und kann von den Benutzern nicht deaktiviert werden.

Auch Daten, die über iTunes auf dem Computer eines Benutzers gesichert werden, können verschlüsselt werden. Diese Funktion kann vom Benutzer aktiviert oder durch Einstellungen für Geräteeinschränkungen in Konfigurationsprofilen erzwungen werden.

iOS unterstützt S/MIME in E-Mails und ermöglicht damit das Anzeigen und Senden verschlüsselter E-Mails auf iPhone und iPad. Mithilfe von Einschränkungen kann auch verhindert werden, dass E-Mails zwischen verschiedenen Accounts bewegt oder dass auf einem Account empfangene Mails von einem anderen Account aus weitergeleitet werden.

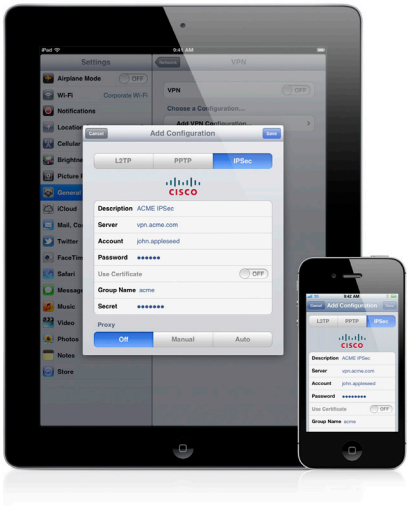
Datenschutz
Aufbauend auf der Hardwareverschlüsselung von iPhone und iPad können die auf dem Gerät gespeicherten E-Mails und Anhänge mit der integrierten Datenschutzfunktion von iOS noch weiter geschützt werden. Für den Datenschutz auf iPhone und iPad wird der für jedes Gerät eindeutige Code mit der Hardwareverschlüsselung kombiniert, um einen zuverlässigen Schlüssel zu erstellen. Dieser Schlüssel verhindert den Zugriff auf Daten, wenn das Gerät gesperrt ist, und sorgt dafür, dass vertrauliche Daten selbst bei Verlust oder Diebstahl des Gerätes geschützt sind.

Zu ihrer Aktivierung muss auf dem Gerät lediglich ein Code eingerichtet werden. Ein wirksamer Schutz der Daten bedingt die Verwendung eines starken Codes. Es ist deshalb wichtig, dass bei der Festlegung von Coderichtlinien Codes mit mehr als vier Stellen erfordert und durchgesetzt werden. Benutzer können im Bereich „Code“ der Einstellungen überprüfen, ob der Datenschutz auf ihrem Gerät aktiviert ist. Lösungen zur Verwaltung mobiler Geräte (Mobile Device Management) können auch diese Geräteinformation abfragen.

Diese Datenschutz-APIs stehen auch den Entwicklern zur Verfügung und können verwendet werden, um firmeninterne Daten oder Daten in kommerziellen Apps zu schützen.

Progressive Zeitüberschreitungsintervalle für Codes
iPhone und iPad können so konfiguriert werden, dass nach mehreren ungültigen Eingaben des Gerätecodes alle Daten automatisch gelöscht werden. Gibt ein Benutzer wiederholt einen falschen Code ein, wird iOS für zunehmend längere Zeitspannen gesperrt. Nach zu vielen Fehlversuchen werden sämtliche Daten und Einstellungen auf dem Gerät gelöscht.

Fernlöschen
iOS unterstützt die Funktion „Fernlöschen“. Geht ein Gerät verloren oder wird es gestohlen, kann der Administrator oder Gerätebesitzer den Befehl „Fernlöschen“ ausgeben, der alle Daten entfernt und das Gerät deaktiviert. Ist auf dem Gerät ein Exchange Account konfiguriert, kann der Administrator den Fernlöschbefehl über die Exchange Management Console (Exchange Server 2007) oder das Exchange ActiveSync Mobile Administration Web Tool (Exchange Server 2003 oder 2007) ausgeben. Benutzer von Exchange Server 2007 können Fernlöschbefehle auch mithilfe von Outlook Web Access geben. Fernlöschbefehle können auch durch MDM-Lösungen ausgelöst werden, selbst wenn keine Exchange Unternehmensdienste genutzt werden.



Lokales Löschen
Geräte können so konfiguriert werden, dass nach einigen fehlgeschlagenen Code-Eingaben alle Daten automatisch gelöscht werden. Diese Maßnahme bietet Schutz bei Attacken mit dem Ziel, Zugriff auf das Gerät zu erhalten. Ist ein Gerätecode festgelegt, können Benutzer den Löschvorgang direkt in den Einstellungen aktivieren. Standardmäßig löscht iOS die Daten auf dem Gerät nach zehn fehlgeschlagenen Code-Eingaben automatisch. Wie auch bei anderen Coderichtlinien kann die maximale Anzahl fehlgeschlagener Versuche mittels eines Konfigurationsprofils eingestellt, von einem MDM-Server vorgegeben oder drahtlos über Microsoft Exchange ActiveSync Richtlinien festgelegt werden.

iCloud
iCloud speichert Musik, Fotos, Apps, Kalender, Dokumente und mehr, und per Push-Funktion werden alle diese Daten automatisch auf alle Geräte eines Benutzers übertragen. iCloud sichert auch Informationen, einschließlich Geräteeinstellungen, App-Daten sowie SMS- und MMS-Nachrichten täglich via Wi-Fi. iCloud sichert Ihren Inhalt durch Verschlüsselung, wenn dieser im Internet gesendet wird. Die Daten werden in verschlüsseltem Format gespeichert und zur Authentifizierung werden sichere Tokens verwendet. Darüber hinaus können iCloud Features wie Fotostream, Synchronisierung von Dokumenten und Backup auch über ein Konfigurationsprofil deaktiviert werden. Weitere Informationen zu Sicherheit und Datenschutz bei iCloud finden Sie unter http://support.apple.com/kb/HT4865.

Netzwerksicherheit

Netzwerksicherheit
- Cisco IPSec, L2TP, PPTP VPN integriert
- SSL VPN via App Store Apps
- SSL/TLS mit X.509 Zertifikaten
- WPA/WPA2 Enterprise mit 802.1X
- Zertifikatbasierte Authentifizierung
- RSA SecurID, CRYPTOCard

Mobile Benutzer müssen von überall auf der Welt auf Netzwerke mit Unternehmensdaten zugreifen können. Dabei muss sichergestellt werden, dass die Benutzer über die entsprechenden Zugriffsrechte verfügen und dass die Daten während der Übertragung zuverlässig geschützt sind. iOS setzt bewährte Technologien ein, um diese Sicherheitsziele sowohl für Wi-Fi als auch für Mobilfunk-Datenverbindungen zu erreichen.

Zusätzlich zu Ihrer vorhandenen Infrastruktur wird jede FaceTime Sitzung und jede iMessage Konversation komplett verschlüsselt. iOS erstellt eine eindeutige ID für jeden Teilnehmer und sorgt dafür, dass jede Kommunikation korrekt verschlüsselt, geroutet und verbunden wird.

VPN-Protokolle
- Cisco IPSec
- L2TP/IPSec
- PPTP
- SSL VPN

VPN
In vielen Unternehmensumgebungen wird eine Form virtueller privater Netzwerke (VPN) verwendet. Solche sicheren Netzwerkdienste sind bereits implementiert, sodass die Einbindung von iPhone oder iPad nur minimalen Einrichtungs- und Konfigurationsaufwand erfordert.

Dank seiner Unterstützung für Cisco IPSec, L2TP und PPTP lässt sich iOS in zahlreiche gängige VPN-Technologien integrieren. iOS unterstützt SSL VPN über Programme von Juniper, Cisco und F5 Networks. Die Unterstützung dieser Protokolle bietet die höchste Stufe der IP-basierten Verschlüsselung für die Übertragung vertraulicher Daten.

Authentifizierungsmethoden
- Kennwort (MSCHAPv2)
- RSA-SecurID
- CRYPTOCard
- digitale X.509 Zertifikate
- Shared Secret

802.1X Identifizierungsprotokolle
- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, PEAP v1
- LEAP

iOS ermöglicht sicheren Zugriff auf bestehende VPN-Umgebungen und umfasst darüber hinaus bewährte Methoden zur Authentifizierung von Benutzern. Die Authentifizierung durch digitale Zertifikate, die auf dem X.509 Standard basieren, bietet den Benutzern einen effizienten Zugriff auf Unternehmensressourcen und eine gangbare Alternative zur Verwendung von hardwarebasierten Token. Zusätzlich kann iOS aufgrund der Authentifizierung durch Zertifikate VPN On Demand nutzen, was den VPN-Authentifizierungsvorgang transparent macht und zugleich einen zuverlässig geschützten Zugriff auf Netzwerkdienste ermöglicht. In Firmenumgebungen, die ein Two-Factor-Token erfordern, lässt sich iOS mit RSA SecurID und CRYPTOCard integrieren.

Unterstützte Zertifikatformate
iOS unterstützt X.509 Zertifikate mit RSA-Schlüsseln. Die Dateierweiterungen .cer, .crt und .der werden erkannt.

iOS unterstützt die Konfiguration von Netzwerk-Proxys sowie das Split-IP-Tunneling. Dadurch wird Datenverkehr an öffentliche oder private Netzwerkdomains gemäß Ihren spezifischen Unternehmensrichtlinien umgeleitet.

SSL/TLS
iOS unterstützt SSL Version 3 sowie TLS (Transport Layer Security) Version 1.0, 1.1. und 1.2, die nächste Generation der Sicherheitsstandards für das Internet. Safari, Kalender, Mail und weitere Internetprogramme starten diese Technologien automatisch, um die verschlüsselte Datenübertragung zwischen iOS und Unternehmensdiensten sicherzustellen.

WPA/WPA2
iOS unterstützt WPA2 Enterprise, um authentifizierten Zugriff auf Ihr drahtloses Unternehmensnetzwerk bereitzustellen. WPA2 Enterprise nutzt die 128-Bit AES-Verschlüsselung und gibt damit den Benutzern die größte Gewähr dafür, dass ihre Daten geschützt bleiben, wenn sie Informationen über eine Wi-Fi Netzwerkverbindung senden und empfangen. Da das iPhone und das iPad den Standard 802.1X unterstützen, lassen sie sich in eine Vielzahl von RADIUS-Authentifizierungsumgebungen integrieren.

Sicherheit von Apps

Sicherheit von Apps
- Laufzeitschutz
- Zwingende Codesignierung
- Schlüsselbunddienste
- CommonCrypto APIs
- Programmdatenschutz

Bei der Entwicklung von iOS spielte die Sicherheit eine zentrale Rolle. Der „Sandbox"-Ansatz für den Programmlaufzeitschutz und die verbindliche Programmsignierung stellen sicher, dass Programme nicht verändert werden können. iOS verfügt außerdem über ein sicheres Framework, das die sichere Speicherung der Identifikationsdaten für Programm- und Netzwerkdienste in einem verschlüsselten Schlüsselbund unterstützt. Für Entwickler bietet es eine allgemeine Verschlüsselungsarchitektur zum Verschlüsseln von Programmdatenspeichern.

Laufzeitschutz
Die Programme werden auf dem Gerät in einer „Sandbox" ausgeführt, damit sie nicht auf Daten zugreifen können, die durch andere Programme gespeichert wurden. Hinzu kommt, dass die Systemdateien, Ressourcen und der Betriebssystemkern vom Programmbereich des Benutzers abgeschirmt sind. Muss ein Programm auf die Daten eines anderen Programms zugreifen, ist dies nur mit den von iOS bereitgestellten APIs und Diensten möglich. Auch das Generieren von Code wird verhindert.

Zwingende Codesignierung
Alle iOS Apps müssen signiert werden. Die ab Werk auf dem Gerät vorhandenen Apps wurden von Apple signiert. Programme anderer Hersteller signiert der jeweilige Entwickler mit einem von Apple ausgestellten Zertifikat. Dies gewährleistet, dass die Apps nicht manipuliert oder verändert wurden. Außerdem erfolgen Laufzeitprüfungen während der Programmausführung, um sicherzustellen, dass ein Programm seit der letzten Verwendung nicht unzuverlässig geworden ist.

Die Verwendung individueller oder unternehmensinterner Programme kann anhand eines Bereitstellungsprofils gesteuert werden. Benutzer müssen das Bereitstellungsprofil installieren, um das Programm ausführen zu können. Bereitstellungsprofile können mithilfe von MDM-Lösungen per Fernzugriff installiert oder entzogen werden. Administratoren können außerdem die Nutzung eines Programms auf bestimmte Geräte beschränken.

Sicheres Authentifizierungs-Framework
iOS bietet einen sicheren verschlüsselten Schlüsselbund für die Speicherung digitaler Identitäten, Benutzernamen und Kennwörter. Schlüsselbunddaten sind partitioniert, damit Programme einer anderen Identität nicht auf Zugangsdaten zugreifen können, die durch ein Programm eines anderen Anbieters gespeichert wurden. Auf diese Weise können Identifizierungsdaten auf iPhone und iPad für die gesamte Bandbreite von Programmen und Diensten innerhalb eines Unternehmens geschützt werden.

Allgemeine Verschlüsselungsarchitektur
App-Entwickler haben Zugriff auf Verschlüsselungs-APIs, mit denen sie ihre App-Daten noch besser schützen können. Die symmetrische Verschlüsselung erfolgt mit bewährten Methoden wie AES, RC4 oder 3DES. Darüber hinaus bieten iPhone und iPad Hardwarebeschleunigung für die AES-Verschlüsselung und SHA1-Hashing, sodass die maximale Programmleistung erzielt wird.

Programmdatenschutz
Die Programme können auch die Vorzüge der integrierten Hardwareverschlüsselung auf iPhone und iPad nutzen, um den Schutz sensibler Programmdaten zu erhöhen. Entwickler können bestimmte Dateien für den Datenschutz kennzeichnen und das System anweisen, den Inhalt der Datei für das Programm und für mögliche Eindringlinge unzugänglich zu machen, wenn das Gerät gesperrt ist.

Verwaltete Apps
Ein MDM-Server kann Apps anderer Anbieter aus dem App Store verwalten, aber auch unternehmenseigene Programme. Durch die Kennzeichnung einer App als verwaltete App kann der Server festlegen, ob die App und die dazugehörigen Daten durch den MDM-Server vom Gerät entfernt werden können. Darüber hinaus kann der Server das Sichern der Daten verwalteter Apps in iTunes und iCloud unterbinden. Auf diese Weise kann die IT-Abteilung Apps, die ggf. vertrauliche geschäftliche Informationen enthalten, mit einem höheren Maß an Steuerungsmöglichkeiten verwalten, als dies bei Apps der Fall wäre, die der Benutzer direkt geladen hat.

Zum Installieren einer verwalteten App sendet der MDM-Server einen Installationsbefehl an das Gerät. Verwaltete Apps können nur mit Genehmigung eines Benutzers installiert werden. Weitere Informationen zu verwalteten Apps finden Sie im *Mobile Device Management Overview* unter www.apple.com/business/mdm.

Revolutionäre Geräte, durch und durch sicher

iPhone und iPad schützen Daten durch Verschlüsselung bei der Übertragung, auf dem Gerät selbst sowie während der Datensicherung in iCloud oder iTunes. Unabhängig davon, ob der Benutzer auf Unternehmens-E-Mails zugreift, eine private Website besucht oder sich beim Unternehmensnetzwerk authentifiziert, bietet iOS die Gewähr, dass nur dazu befugte Benutzer Zugriff auf vertrauliche Unternehmensdaten haben. Durch die Unterstützung von Netzwerkfunktionen auf Unternehmensniveau und umfassenden Methoden zur Vermeidung von Datenverlust haben Sie die Gewissheit, dass Sie mit iOS Geräten bewährte Methoden für die Sicherheit mobiler Geräte und den Datenschutz implementieren.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, FaceTime, iPad, iPhone, iTunes und Safari sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. iCloud und iTunes Store sind Dienstleistungsmarken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. App Store ist eine Dienstleistungsmarke der Apple Inc. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Oktober 2011 L422500B

Implementierung von iPhone und iPad

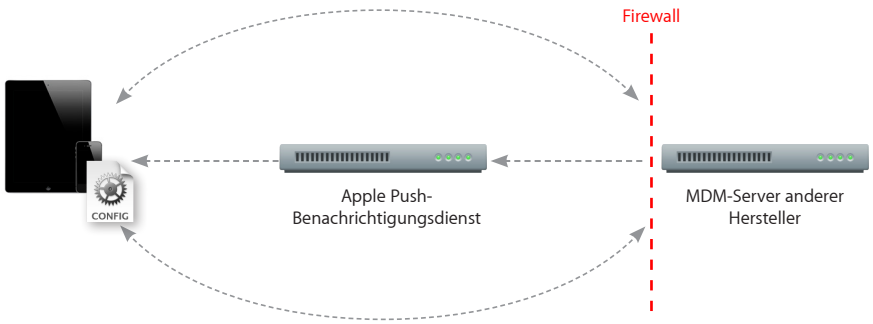
Mobile Device Management

iOS unterstützt Mobile Device Management (MDM) und ermöglicht Unternehmen somit die Verwaltung einer skalierter Implementierungen von iPhone und iPad im Unternehmen. Die MDM-Funktionen basieren auf vorhandenen iOS Technologien (wie Konfigurationsprofile, kabellose Registrierung und Apple Dienst für Push-Benachrichtigungen) und können in unternehmensinterne Lösungen oder Lösungen anderer Hersteller integriert werden. Dies eröffnet IT-Abteilungen die Möglichkeit, iPhone und iPad sicher in einer Unternehmensumgebung zu registrieren, drahtlos Einstellungen zu konfigurieren und zu aktualisieren, die Einhaltung von Unternehmensrichtlinien zu überwachen und die Geräte sogar per Fernzugriff zu löschen oder zu sperren.

Verwalten von iPhone und iPad

Die Verwaltung von iOS Geräten erfolgt über eine Verbindung zu einem MDM-Server. Dieser Server kann intern von der IT-Abteilung erstellt oder bei einem anderen Anbieter gekauft werden. Das Gerät nimmt Verbindung zum Server auf, um festzustellen, ob Aufgaben anstehen, und reagiert mit den erforderlichen Aktionen. Diese Aufgaben umfassen unter anderem die Aktualisierung der Richtlinien, die Bereitstellung der angefragten Geräte- oder Netzwerkinformationen sowie das Löschen von Einstellungen und Daten.

Die meisten Verwaltungsfunktionen laufen im Hintergrund ab, ohne dass ein Eingreifen des Benutzers erforderlich ist. Aktualisiert eine IT-Abteilung zum Beispiel ihre VPN-Infrastruktur, kann der MDM-Server die neuen Account-Informationen auf dem iPhone bzw. iPad drahtlos konfigurieren. Beim nächsten Zugriff auf das VPN ist der Account bereits richtig konfiguriert, und der Mitarbeiter muss weder das Supportteam anrufen noch die Einstellungen manuell verändern.



iOS und SCEP
iOS unterstützt das SCEP (Simple Certificate Enrollment Protocol). Bei SCEP handelt es sich um einen Internetentwurf der IETF (Internet Engineering Task Force). SCEP soll eine einfachere Handhabung der Zertifikatverteilung für groß angelegte Implementierungen ermöglichen. Es erlaubt die kabellose Registrierung von Identitätszertifikaten beim iPhone und iPad, die für die Authentifizierung gegenüber Unternehmensdiensten verwendet werden können.

MDM und der Apple Dienst für Push-Benachrichtigungen

Wenn ein MDM-Server Verbindung zum iPhone oder iPad aufnehmen will, sendet er im Hintergrund mit dem Apple Dienst für Push-Benachrichtigungen eine entsprechende Benachrichtigung an das Gerät, die es zur Anmeldung am Server auffordert. Beim Benachrichtigen des Geräts werden keine proprietäre Informationen an den oder vom Apple Dienst für Push-Benachrichtigungen übertragen. Die einzige Aufgabe, die die Push-Benachrichtigung ausführt, besteht in der Beendigung des Ruhezustands des Geräts, sodass dieses beim MDM-Server angemeldet werden kann. Alle Konfigurationsinformationen, Einstellungen und Abfragen gehen über eine verschlüsselte SSL/TLS-Verbindung zwischen Gerät und MDM-Server direkt vom Server an das iOS Gerät. iOS verarbeitet sämtliche MDM-Abfragen und -Aktionen im Hintergrund und begrenzt auf diese Weise die Beeinträchtigung der Nutzungsqualität des Geräts (Batterielaufzeit, Leistung und Zuverlässigkeit).

Damit der Server für Push-Benachrichtigungen Befehle vom MDM-Server erkennt, muss auf dem Server ein Zertifikat installiert werden. Dieses Zertifikat muss vom Apple Push Certificates Portal angefordert und geladen werden. Sobald das Zertifikat für Apple Push-Benachrichtigungen auf den MDM-Server geladen wurde, kann die Registrierung der Geräte beginnen. Weitere Informationen zum Anfordern eines Zertifikats für Apple Push-Benachrichtigungen für MDM finden Sie unter www.apple.com/business/mdm.

Konfiguration des Apple Push-Benachrichtigungsdiensts
Wenn sich MDM-Server und iOS Geräte hinter einer Firewall befinden, ist ggf. Aufwand für die Netzwerkkonfiguration erforderlich, damit der MDM-Dienst korrekt funktionieren kann. Zum Senden von Benachrichtigungen vom MDM-Server an den Apple Push-Benachrichtigungsdienst muss der TCP-Port 2195 geöffnet sein. Damit der Feedback-Dienst erreichbar ist, muss TCP-Port 2196 ebenfalls geöffnet sein. Für Geräte, die die Verbindung zum Push-Dienst via Wi-Fi herstellen, muss TCP-Port 5223 geöffnet sein.

Der IP-Adressbereich für den Push-Dienst ist veränderlich. Es wird davon ausgegangen, dass ein MDM-Server die Verbindung nicht auf Basis der IP-Adresse, sondern des Hostnamens herstellt. Der Push-Dienst verwendet ein Lastausgleichsschema, das bei gleichem Hostnamen zu unterschiedlichen IP-Adressen führen kann. Dieser Hostname lautet gateway.push.apple.com (bzw. gateway.sandbox.push.apple.com bei der Entwicklungsumgebung für Push-Benachrichtigungen). Außerdem wird der gesamte Adressblock 17.0.0.0/8 Apple zugewiesen, sodass Firewall-Regeln zum Definieren dieses Bereichs erstellt werden können.

Weitere Informationen erhalten Sie bei Ihrem MDM-Anbieter oder in der *Developer Technical Note TN2265* in der iOS Developer Library unter der Adresse http://developer.apple.com/library/ios/#technotes/tn2265/_index.html.

Registrierung

Sobald der MDM-Server und das MDM-Netzwerk konfiguriert sind, besteht der erste Schritt der Verwaltung von iPhone oder iPad in der Registrierung des Geräts beim MDM-Server. Dadurch wird eine Beziehung zwischen dem Gerät und dem Server erstellt, die eine bedarfsorientierte Verwaltung des Geräts ohne weitere Benutzerinteraktion ermöglicht.

Die Registrierung kann drahtlos oder durch Anschließen von iPhone oder iPad via USB an einen Computer erfolgen. Die meisten Lösungen arbeiten allerdings mit der kabellosen Profilregistrierung. Manche MDM-Anbieter verwenden eine App zum Starten dieses Prozesses, andere leiten die Registrierung ein, indem sie die Benutzer an ein Webportal verweisen. Jede dieser Methoden hat Vorteile, und beide werden verwendet, um die kabellose Registrierung via Safari auszulösen.

Übersicht über das Registrierungsverfahren
Die drahtlose Registrierung umfasst Phasen, die sich zu einem automatisierten Arbeitsablauf kombinieren lassen und einen maximal skalierbaren Weg zur sicheren Registrierung von Geräten in einer Unternehmensumgebung bieten. Zu diesen Phasen zählen:

1. Benutzerauthentifizierung
Die Benutzerauthentifizierung stellt sicher, dass eingehende Registrierungsanfragen von autorisierten Benutzern stammen und dass die Geräteinformationen des Benutzers vor der Zertifikatsregistrierung erfasst werden. Administratoren können die Registrierung über ein Webportal, per E-Mail oder SMS an die Benutzer oder auch mithilfe einer App in Gang setzen.

2. Zertifikatsregistrierung
Nach erfolgter Benutzeridentifizierung generiert iOS eine zertifikatbasierte Registrierungsanforderung unter Verwendung des Simple Certificate Enrollment Protocol (SCEP). Diese Anforderung zur Zertifikatsregistrierung kommuniziert direkt mit der Zertifizierungsstelle (CA) des Unternehmens und lässt zu, dass iPhone und iPad im Gegenzug ein Identitätszertifikat von der Zertifizierungsstelle erhalten.

3. Gerätekonfiguration
Sobald ein Identitätszertifikat installiert wurde, kann das Gerät drahtlos verschlüsselte Konfigurationsinformationen empfangen. Diese Informationen können nur auf dem dafür bestimmten Gerät installiert werden und enthalten die Einstellungen, die für die Verbindung zum MDM-Server benötigt werden.

Am Ende des Registrierungsprozesses wird dem Benutzer ein Installationsbildschirm angezeigt, der erklärt, welche Zugriffsrechte der MDM-Server auf das Gerät haben wird. Akzeptiert der Benutzer die Installation des Profils, wird sein Gerät automatisch registriert, ohne dass er etwas unternehmen muss.

Sobald iPhone und iPad als verwaltete Geräte registriert sind, können sie dynamisch mit Einstellungen konfiguriert, nach Informationen abgefragt oder vom MDM-Server per Fernlöschen bereinigt werden.

Konfiguration

Zum Konfigurieren eines Geräts mit Accounts, Richtlinien und Einschränkungen sendet der MDM-Server so genannte Konfigurationsprofile an das Gerät. Diese Dateien werden automatisch installiert. Konfigurationsprofile sind XML-Dateien, die Konfigurationsdaten und Einstellungen enthalten, die es dem Gerät ermöglichen, mit Ihren Unternehmenssystemen zu arbeiten. Dazu gehören Account-Informationen, Coderichtlinien, Einschränkungen und andere Geräteeinstellungen. Zusammen mit dem beschriebenen Registrierungsprozess bietet die Konfiguration der IT-Abteilung die Gewissheit, dass nur autorisierte Benutzer Zugriff auf die Unternehmensdienste erhalten und die Geräte in Übereinstimmung mit den vorgegebenen Richtlinien konfiguriert werden.

Da sich Konfigurationsprofile sowohl signieren als auch verschlüsseln lassen, können die Einstellungen nicht geändert oder weitergegeben werden.

Unterstützte konfigurierbare Einstellungen

Benutzer

- Exchange ActiveSync
- IMAP/POP E-Mail
- Wi-Fi
- VPN
- LDAP
- CardDAV
- CalDAV
- Abonnierte Kalender

Coderichtlinien

- Code auf Gerät zwingend erforderlich
- Einfacher Wert zulässig
- Verlangen eines alphanumerischen Werts
- Mindestlänge für Codes
- Mindestanzahl komplexer Zeichen
- Maximale Gültigkeitsdauer für Codes
- Zeit bis zur automatischen Sperre
- Codeverlauf
- Nachfrist für Gerätesperre
- Maximale Anzahl Fehlversuche

Sicherheit und Datenschutz

- Senden von Diagnosedaten an Apple erlauben
- Akzeptieren nicht verlässlicher Zertifikate durch den Benutzer erlauben
- Verschlüsselte Backups erzwingen

Weitere Einstellungen

- Zertifikate
- Webclips
- SCEP Einstellungen
- APN Einstellungen

Gerätefunktionalität

- Installieren von Apps erlauben
- Siri erlauben
- Verwendung der Kamera erlauben
- FaceTime erlauben
- Bildschirmfoto erlauben
- Manuelles Synchronisieren beim Roaming erlauben
- Wählen per Spracheingabe erlauben
- In-App-Käufe erlauben
- Store-Kennwort für alle Einkäufe verlangen
- Gaming mit mehreren Spielern zulassen
- Hinzufügen von Freunden im Game Center erlauben

Programme

- Verwendung von YouTube erlauben
- Verwendung des iTunes Store erlauben
- Verwendung von Safari erlauben
- Safari Sicherheitseinstellungen festlegen

iCloud

- Datensicherung erlauben
- Synchronisierung von Dokumenten und Schlüsselwerten erlauben
- Fotostream erlauben

Wertung von Inhalten

- Ungeeignete/anstößige Videos und Podcasts erlauben
- Wertungsbereich festlegen
- Zulässige Inhaltswertungen festlegen

Abfragen von Geräten

Zusätzlich zur Konfiguration kann ein MDM-Server auch verschiedene Informationen bei den Geräten abfragen. Anhand dieser Informationen kann sichergestellt werden, dass die Geräte die Richtlinien kontinuierlich einhalten.

Unterstützte Abfragen

Geräteinformation
- Eindeutige Kennung des Geräts (UDID)
- Name des Geräts
- iOS Version und Build-Nummer
- Modellname und -nummer
- Seriennummer
- Kapazität und freier Speicherplatz
- IMEI
- Modem-Firmware
- Batteriestatus

Netzwerkinformationen
- ICCID
- Bluetooth® und Wi-Fi MAC Adressen
- Aktuelles Betreibernetz
- Betreibernetz des Teilnehmers
- Version der Betreibereinstellungen
- Telefonnummer
- Einstellung für Daten-Roaming (ein/aus)

Informationen zu Konformität und Sicherheit
- Installierte Konfigurationsprofile
- Installierte Zertifikate mit Ablaufdatum
- Liste aller vorgegebenen Einschränkungen
- Möglichkeit zur Hardwareverschlüsselung
- Code vorhanden

Programme
- Installierte Programme (App-ID, Name, Version, Größe und Datenumfang von Apps)
- Installierte Bereitstellungsprofile mit Ablaufdatum

Verwaltung

MDM (Mobile Device Management) umfasst eine Reihe von Funktionen, die ein MDM-Server auf iOS Geräten ausführen kann. Zu diesen Aufgaben gehören das Installieren und Entfernen von Konfigurations- und Bereitstellungsprofilen, das Verwalten von Apps, das Beenden der MDM-Beziehung und das Fernlöschen eines Geräts.

Verwaltete Einstellungen
Bei der Einleitung der Gerätekonfiguration pusht ein MDM-Server Konfigurationsprofile auf das iPhone bzw. iPad. Diese Profile werden im Hintergrund installiert. Im Lauf der Zeit müssen die Einstellungen und Richtlinien, die bei der Registrierung festgelegt wurden, ggf. aktualisiert oder geändert werden. Um diese Änderungen vorzunehmen, kann ein MDM-Server jederzeit neue Konfigurationsprofile installieren und vorhandene Profile ändern oder entfernen. Außerdem müssen möglicherweise kontextspezifische Konfigurationen auf iOS Geräten installiert werden, je nach Standort oder Aufgabe des Benutzers im Unternehmen. Reist beispielsweise ein Benutzer ins Ausland, kann MDM veranlassen, dass das Synchronisieren der E-Mails manuell und nicht automatisch erfolgen muss. Ein MDM-Server kann sogar Sprach- oder Datendienste per Fernzugriff deaktivieren, um zu verhindern, dass bei einem Benutzer Roaming-Gebühren eines Mobilfunkanbieters anfallen.

Verwaltete Apps
Ein MDM-Server kann Apps anderer Anbieter aus dem App Store verwalten, aber auch unternehmenseigene Programme. Der Server kann verwaltete Apps und die dazugehörigen Daten bei Bedarf entfernen oder angeben, ob die Apps gelöscht werden sollen, wenn das MDM-Profil entfernt wird. Darüber hinaus kann der MDM-Server das Sichern der Daten verwalteter Apps in iTunes und iCloud unterbinden.

Zum Installieren einer verwalteten App sendet der MDM-Server einen Installationsbefehl an das Gerät des Benutzers. Verwaltete Apps können nur mit Zustimmung eines Benutzers installiert werden. Wenn ein MDM-Server die Installation einer verwalteten App aus dem App Store anfordert, werden die Kosten der App dem iTunes Account erstattet, der zum Zeitpunkt der Installation der App verwendet wurde. Bei kostenpflichtigen Apps muss der MDM-Server einen VPP-Gutscheincode (Volume Purchasing Program) ausstellen und senden. Weitere Informationen zu VPP finden Sie auf der folgenden Webseite: www.apple.com/business/vpp/. Apps aus dem App Store können nicht auf einem Benutzergerät installiert werden, wenn der App Store deaktiviert wurde.

Entfernen oder Fernlöschen von Geräten

Wenn ein Gerät verloren geht, gestohlen wird, ein Richtlinienverstoß vorliegt oder ein Mitarbeiter das Unternehmen verlässt, kann ein MDM-Server verschiedene Maßnahmen zum Schutz von Unternehmensinformationen treffen.

Ein IT-Administrator kann die MDM-Beziehung zu einem Gerät beenden, indem er das Konfigurationsprofil entfernt, das die MDM-Serverinformationen enthält. Dabei werden alle Accounts, Einstellungen und Apps entfernt, für deren Installation das Profil verantwortlich war. Die IT-Abteilung kann aber auch das MDM-Konfigurationsprofil beibehalten und MDM nur dazu nutzen, die spezifischen Konfigurationsprofile, Bereitstellungsprofile und verwalteten Apps zu entfernen, die gezielt gelöscht werden sollen. Bei dieser Vorgehensweise wird das Gerät weiterhin von MDM verwaltet, und eine erneute Registrierung nach Wiederherstellung der Richtlinien ist nicht notwendig.

Mit beiden Methoden kann die IT-Abteilung dafür sorgen, dass Informationen nur für die jeweils berechtigten Benutzer und Geräte verfügbar sind, und es ist sichergestellt, dass Unternehmensdaten entfernt werden, ohne dass die privaten Daten eines Benutzers (z. B. Musik, Fotos oder persönliche Apps) davon betroffen sind.

Zum dauerhaften Löschen aller Medien und Daten auf dem Gerät und anschließendem Zurücksetzen auf die Werkseinstellungen kann MDM die Funktion „Fernlöschen“ auf dem iPhone und iPad ausführen. Wenn ein Benutzer versucht, das Gerät wiederzufinden, hat die IT-Abteilung auch die Möglichkeit, das Gerät per Fernzugriff zu sperren. Damit wird das Display gesperrt, und zur Aufhebung der Sperre muss der Benutzer den Code des Geräts eingeben.

Sollte ein Benutzer lediglich seinen Code vergessen haben, kann ein MDM-Server den Code vom Gerät entfernen. Der Benutzer wird dann aufgefordert, innerhalb von 60 Minuten einen neuen Code zu erstellen.

Unterstützte Verwaltungsbefehle

Verwaltete Einstellungen

- Konfigurationsprofil installieren
- Konfigurationsprofil entfernen
- Daten-Roaming
- Sprach-Roaming (nicht bei allen Mobilfunkanbietern verfügbar)

Verwaltete Apps

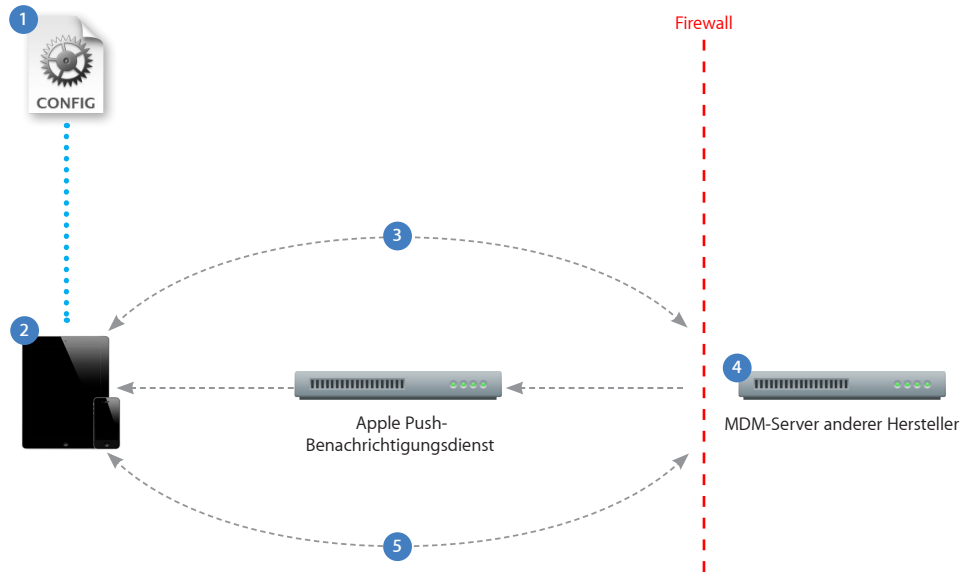
- Verwaltete App installieren
- Verwaltete App entfernen
- Alle verwalteten Apps auflisten
- Bereitstellungsprofil installieren
- Bereitstellungsprofil entfernen

Sicherheitsbefehle

- Fernlöschen
- Fernsperren
- Löschen des Sicherheitscodes

Überblick über Ablauf

Dieses Beispiel beschreibt die Basisimplementierung eines MDM-Servers (Mobile Device Management).



1. Ein Konfigurationsprofil mit MDM-Serverinformationen wird an das Gerät gesendet. Der Benutzer wird informiert, was der Server verwalten und/oder abfragen wird.
2. Der Benutzer installiert das Profil und akzeptiert damit, dass sein Gerät verwaltet wird.
3. Mit der Installation des Profils erfolgt auch die Registrierung des Geräts. Der Server überprüft das Gerät und erlaubt den Zugriff.
4. Der Server fordert das Gerät per Push-Benachrichtigung auf, sich für Aufgaben oder Abfragen am Server anzumelden.
5. Das Gerät stellt via HTTPS eine Direktverbindung zum Server her. Der Server sendet dem Gerät Befehle oder Abfragen.

Weitere Informationen zum Mobile Device Management finden Sie auf der folgenden Webseite: www.apple.com/business/mdm.

© 2011 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, FaceTime, iPad, iPhone, iTunes und Safari sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. iCloud und iTunes Store sind Dienstleistungsmarken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. App Store ist eine Dienstleitungsmarke der Apple Inc. Der Bluetooth® Schriftzug und das Logo sind eingetragene Marken der Bluetooth SIG, Inc., die von Apple in Lizenz verwendet wird. UNIX ist eine eingetragene Marke von The Open Group. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen an den Produktspezifikationen sind vorbehalten. Oktober 2011 L422501B