



iPhone nel settore aziendale

Scenari di deployment e panoramica sulla configurazione del dispositivo

Luglio 2008

Scoprite come iPhone si integra perfettamente negli ambienti aziendali grazie agli scenari di deployment e alla panoramica sulla configurazione del dispositivo.

- iPhone e Microsoft Exchange Server
- iPhone e Virtual Private Networks (VPN)
- iPhone e WPA2 Enterprise/802.1x
- iPhone e IMAP
- Panoramica sulla configurazione del dispositivo iPhone

iPhone e Microsoft Exchange Server



Supporto Exchange ActiveSync

- Microsoft Exchange Server 2003 Service Pack 2
- Microsoft Exchange Server 2007 Service Pack 1

Policy di sicurezza Exchange ActiveSync

- Remote wipe
- Imposizione della password sul dispositivo
- Lunghezza minima della password
- Password alfanumerica richiesta
- Password complessa richiesta
- Tempo di inattività in minuti

Il software iPhone 2.0 comunica direttamente con Microsoft Exchange Server tramite Microsoft Exchange ActiveSync, offrendo agli utenti e-mail, contatti e calendario Push. Exchange ActiveSync mantiene la connessione tra Exchange Server e iPhone così quando arriva un nuovo messaggio e-mail o un nuovo invito, iPhone si aggiorna all'istante. Se la vostra azienda supporta attualmente Exchange ActiveSync su Exchange Server 2003 o 2007, disponete già dei servizi necessari per supportare il software iPhone 2.0, senza che sia richiesta alcuna ulteriore configurazione. Se disponete di Exchange Server ma l'azienda si affaccia per la prima volta sul mondo Exchange ActiveSync, leggete i passaggi illustrati di seguito per abilitare Exchange ActiveSync.

Configurazione Exchange ActiveSync

Configurazione della rete

- Verificate che la porta 443 sia aperta sul firewall. (Nota: se l'azienda consente Outlook Web Access, la porta 443 è probabilmente già aperta sul firewall).
- Su Exchange Front-End Server, verificate che un certificato server sia installato e abilitate SSL per la directory virtuale Exchange ActiveSync (richiede un'autenticazione SSL di base).
- Su Microsoft Internet Security and Acceleration (ISA) Server, verificate che un certificato server sia installato e aggiornate il DNS pubblico per risolvere adeguatamente le connessioni in ingresso.
- Su Microsoft ISA Server, create un Web Listener e una regola di pubblicazione accesso client web Exchange secondo quanto riportato nella documentazione Microsoft. Questo passaggio è necessario per abilitare Exchange ActiveSync.
- Per tutti i firewall e i dispositivi di rete, impostate il timeout sessione per inattività su 30 minuti (consultate la documentazione Microsoft Exchange per intervalli di heartbeat e timeout alternativi).

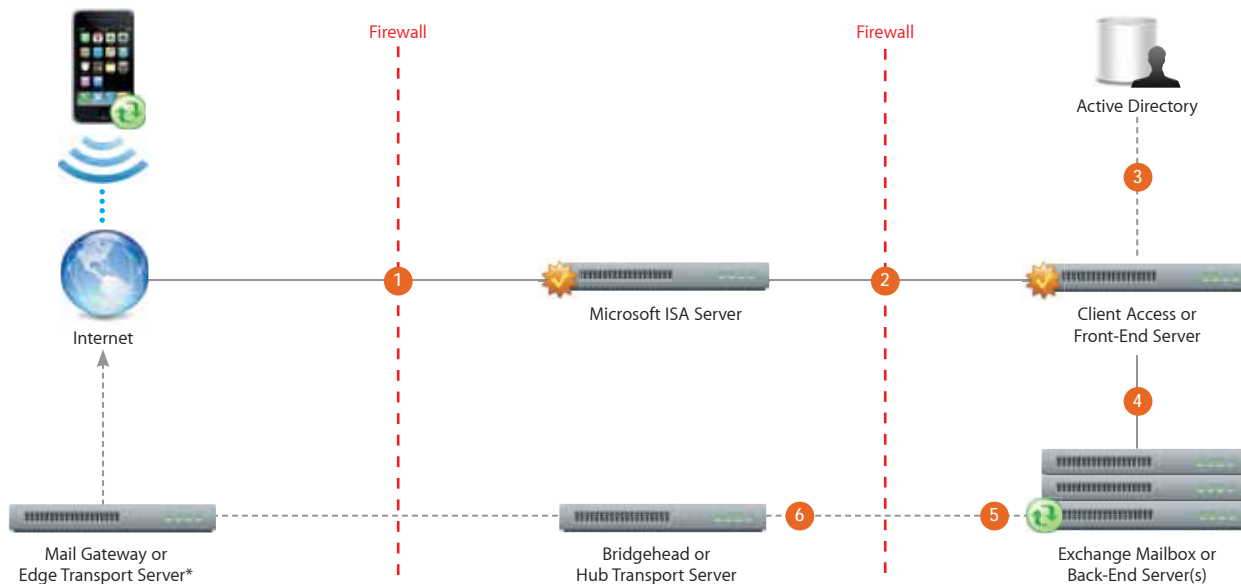
Configurazione dell'account Exchange

Le funzionalità di Exchange ActiveSync sono abilitate per impostazione predefinita per tutti i dispositivi mobili a livello aziendale su Exchange Server 2003 e Exchange Server 2007.

- Abilitate Exchange ActiveSync per utenti/gruppi specifici utilizzando il servizio Active Directory. (Per Exchange Server 2007, è possibile farlo in Exchange Management Console da Recipient Configuration.)
- Configurate funzionalità, policy e impostazioni di sicurezza dei dispositivi mobili utilizzando Exchange System Manager. (Per Exchange Server 2007, è possibile configurare queste funzionalità e impostazioni in Exchange Management Console.)
- In Server 2003, eseguite il download e installate Microsoft Exchange ActiveSync Mobile Administration Web Tool, necessario per il Remote Wipe. (Per Exchange Server 2007, il Remote Wipe può essere inizializzato da Outlook Web Access o Exchange Management Console.)

Scenario di deployment di Exchange ActiveSync

Questo esempio mostra come iPhone si connette a un tipico deployment Microsoft Exchange Server 2003 o 2007.



*A seconda della configurazione di rete, Mail Gateway o Edge Transport Server possono trovarsi all'interno della rete perimetrale (DMZ).

- 1 iPhone richiede accesso ai servizi Exchange ActiveSync sulla porta 443 (HTTPS). (È la stessa porta utilizzata per Outlook Web Access e altri servizi web sicuri, così in molti deployment questa porta è già aperta e configurata per consentire il traffico HTTPS.)
- 2 ISA garantisce l'accesso a Exchange Front-End o Client Access Server. ISA è configurato come un proxy o in molti casi un reverse proxy, per indirizzare il traffico a Exchange Server.
- 3 Exchange esegue l'autenticazione dell'utente in ingresso tramite il servizio Active Directory.
- 4 Se l'utente fornisce le adeguate credenziali e ha accesso ai servizi Exchange ActiveSync, allora Front-End Server stabilirà una connessione alla relativa mailbox su Back-End Server (tramite Active Directory Global Catalog).
- 5 La connessione Exchange ActiveSync viene stabilita. Aggiornamenti e modifiche vengono «spinti» verso iPhone attraverso l'etere e le eventuali modifiche apportate su iPhone verranno rispecchiate su Exchange Server.
- 6 Gli elementi di posta inviati su iPhone vengono sincronizzati con Exchange Server tramite Exchange ActiveSync (fase 5). Per indirizzare la posta in uscita a destinatari esterni, la posta viene generalmente inviata attraverso Bridgehead (o Hub Transport) Server a un Mail Gateway (o Edge Transport Server) esterno tramite SMTP. A seconda della configurazione di rete, Mail Gateway o Edge Transport Server esterni possono trovarsi all'interno della rete perimetrale o al di fuori del firewall.

iPhone e Virtual Private Networks (VPN)



Protocolli VPN

- Cisco IPSec
- L2TP/IPSec
- PPTP

Metodi di autenticazione

- Password (MS-CHAPv2)
- RSA SecurID
- CRYPTOCARD
- Certificati (PKCS1, PKCS12)
- Shared Secret

L'accesso sicuro alle reti aziendali private è disponibile su iPhone tramite i più diffusi protocolli VPN standard di settore. Il software iPhone 2.0 supporta Cisco IPSec, L2TP over IPSec e PPTP. Se la vostra organizzazione supporta uno di questi protocolli, non saranno necessarie ulteriori configurazioni di rete o applicazioni terze parti per connettere iPhone alla vostra VPN.

I deployment Cisco IPSec possono utilizzare l'autenticazione basata su certificato tramite i certificati digitali x.509 standard di settore (PKCS1, PKCS12). Per l'autenticazione basata su token a due fattori, iPhone supporta RSA SecurID nonché CRYPTOCARD. Gli utenti immettono il PIN e la password unica generata tramite token direttamente in iPhone quando stabiliscono una connessione VPN.

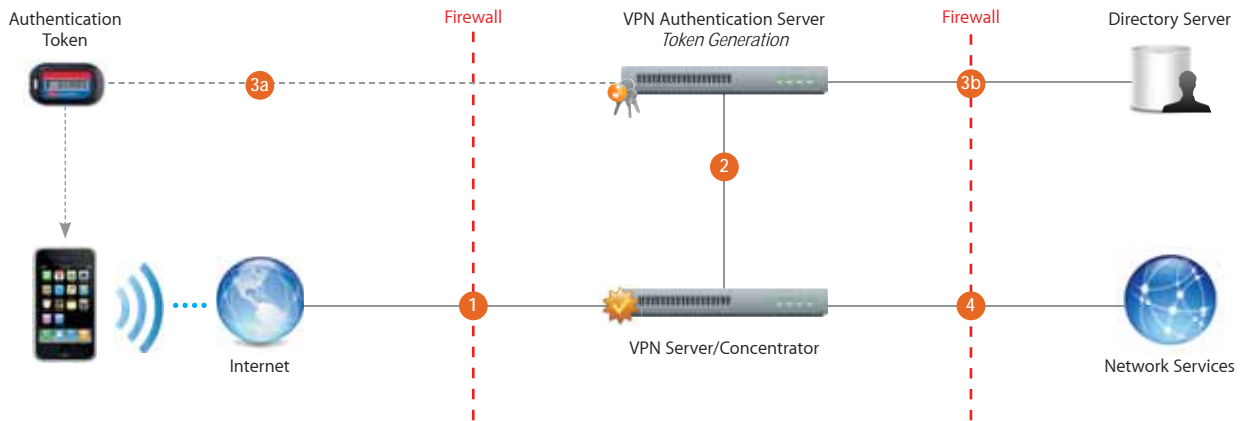
iPhone supporta l'autenticazione Shared Secret per deployment Cisco IPSec e L2TP/IPSec. E per l'autenticazione di base di nome utente e password, iPhone supporta MS-CHAPv2. Indipendentemente dal metodo di autenticazione, le impostazioni VPN preconfigurate possono essere distribuite agli utenti tramite un profilo di configurazione o immesse direttamente in iPhone.

Configurazione VPN

- Poiché iPhone si integra con gran parte delle reti VPN esistenti, è richiesta unicamente una minima configurazione per abilitare l'accesso di iPhone alla vostra rete. Il modo migliore per preparare il deployment consiste nell'assicurarsi che iPhone sia compatibile con i metodi di autenticazione e i protocolli VPN esistenti della vostra azienda.
- Verificate la compatibilità degli standard esistenti con i vostri VPN Concentrator. Consigliamo inoltre di rivedere il percorso di autenticazione al vostro server di autenticazione RADIUS o VPN per assicurarvi che gli standard supportati su iPhone siano abilitati nella vostra attuale implementazione.
- Se prevedete di utilizzare l'autenticazione basata su certificato, assicuratevi che PKI (Public Key Infrastructure) sia configurata per supportare i certificati basati su dispositivo e utente con il processo di distribuzione corrispondente.
- Verificate la compatibilità del formato del certificato e del server di autenticazione. iPhone supporta PKCS1 (.cer, .crt, .der) e PKCS12 (.p12, .pfx).
- Contattate i vostri fornitori per verificare che il vostro software e le vostre apparecchiature siano aggiornati con i più recenti firmware e patch di sicurezza.
- Per ulteriore documentazione sul protocollo e le specifiche Cisco IPSec, visitate www.cisco.com.

Scenario di deployment VPN

Questo esempio illustra un deployment tipico con un VPN Server/Concentrator oltre a un server di autenticazione VPN che controlla l'accesso ai servizi della rete aziendale.



- 1 iPhone richiede accesso ai servizi di rete (generalmente su una connessione PPP).
- 2 Il VPN Server/Concentrator riceve la richiesta e la trasmette al server di autenticazione.
- 3a In un ambiente di autenticazione a due fattori, il server di autenticazione gestisce quindi una generazione di codici token sincronizzata con il key server. Se si esegue il deployment tramite certificato o password, il processo di autenticazione prosegue con la convalida dell'utente.
- 3b Dopo l'autenticazione dell'utente, il server di autenticazione convalida le policy di accesso di utente e gruppo.
- 4 Dopo la convalida delle policy di utente e gruppo, VPN Server fornisce un accesso con tunneling e codificato ai servizi di rete (generalmente via IPSec).

iPhone e WPA2 Enterprise/802.1x



Protocolli di sicurezza wireless

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

Metodi di autenticazione 802.1x

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- PEAPv0 (EAP-MS-CHAPv2)
- PEAPv1 (EAP-GTC)
- LEAP

Il software iPhone 2.0 offre WPA2 Enterprise, che garantisce un accesso sicuro alle reti wireless aziendali da iPhone. WPA2 Enterprise utilizza la codifica AES a 128 bit, un sicuro metodo di codifica basato su blocchi, che offre agli utenti la massima garanzia che i loro dati saranno sempre protetti.

Con il supporto per 802.1x, iPhone può essere integrato in un'ampia gamma di ambienti di autenticazione RADIUS. I metodi di autenticazione wireless 802.1x supportati da iPhone includono EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 e LEAP.

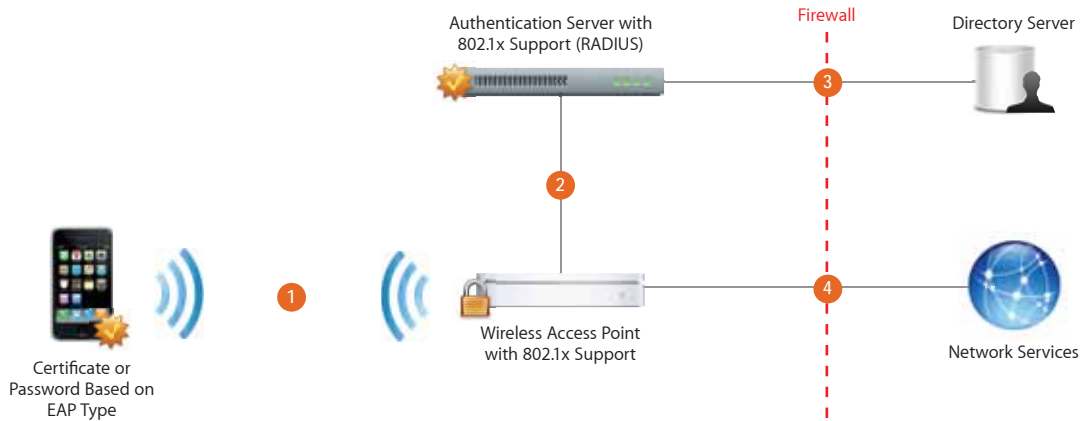
Per una configurazione e un deployment rapidi, le impostazioni di autenticazione, sicurezza e rete WPA2 Enterprise possono essere configurate tramite un profilo di configurazione. Per ulteriori informazioni, consultate il documento Panoramica sulla configurazione del dispositivo iPhone.

Configurazione di WPA2 Enterprise

- Verificate la compatibilità dei dispositivi di rete e selezionate un tipo di autenticazione (Tipo EAP) supportato da iPhone.
- Verificate che 802.1x sia abilitato sul server di autenticazione e, se necessario, installate un certificato server e assegnate i permessi di accesso alla rete a utenti e gruppi.
- Configurate i punti di accesso wireless per l'autenticazione 802.1x e immettete le informazioni corrispondenti del server RADIUS.
- Testate il deployment 802.1x con un Mac o un PC per verificare che l'autenticazione RADIUS sia configurata correttamente.
- Se prevedete di utilizzare l'autenticazione basata su certificato, assicuratevi che PKI (Public Key Infrastructure) sia configurata per supportare i certificati basati su dispositivo e utente con il processo di distribuzione corrispondente.
- Verificate la compatibilità del formato del certificato e del server di autenticazione. iPhone supporta PKCS1 (.cer, .crt, .der) e PKCS12 (.p12, .pfx).
- Contattate i vostri fornitori per verificare che il vostro software e le vostre apparecchiature siano aggiornati con i più recenti firmware e patch di sicurezza.
- Per ulteriore documentazione sugli standard di rete wireless e su Wi-Fi Protected Access (WPA), visitate www.wi-fi.org.

Scenario di deployment WPA2/802.1x Enterprise

Questo esempio illustra un tipico deployment wireless sicuro che sfrutta l'autenticazione basata su RADIUS.



- 1 iPhone richiede accesso ai servizi di rete. Selezionando una rete wireless o configurando l'accesso a uno specifico SSID, iPhone avvia la connessione.
- 2 Dopo che la richiesta è stata ricevuta dal punto di accesso, viene trasmessa al server RADIUS per l'autenticazione.
- 3 Il server RADIUS convalida l'account utente utilizzando il servizio di directory.
- 4 Dopo l'autenticazione dell'utente, il punto di accesso fornisce accesso alla rete con le policy e i permessi indicati dal server RADIUS.

iPhone e IMAP



Soluzioni mail abilitate IMAP o POP

iPhone supporta le soluzioni mail abilitate IMAP4 e POP3 standard di settore su un'ampia gamma di piattaforme server, tra cui Windows, UNIX, Linux e Mac OS X.

Ulteriori informazioni sullo standard IMAP4rev1 sono disponibili al sito www.imap.org.

Con il supporto per il protocollo IMAP per la posta elettronica, iPhone si integra in pressoché tutti gli ambienti di mail server. Se il server supporta IMAP ed è configurato per richiedere autenticazione e SSL, iPhone offre un approccio altamente sicuro e basato su standard al deployment e-mail. In un deployment tipico, iPhone stabilisce un accesso diretto a un server abilitato IMAP sulla porta 993 e un accesso ai server SMTP sulla porta 587. Questi server possono trovarsi all'interno di una sottorete DMZ, dietro un firewall aziendale o in entrambe le posizioni. Con SSL, iPhone supporta la codifica a 128 bit e i certificati root X.509 generati dalle principali authority di certificazione. iPhone supporta inoltre solidi metodi di autenticazione, tra cui gli standard di settore MD5 Challenge-Response e NTLMv2.

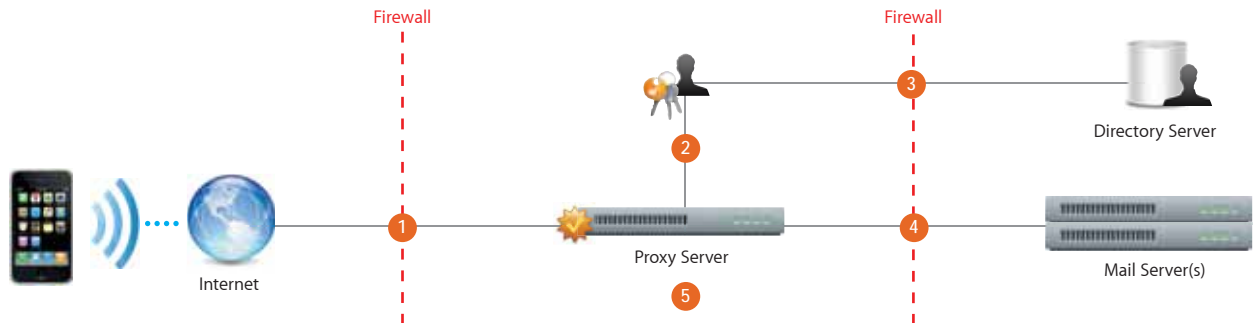
Configurazione della rete IMAP

L'amministratore di rete o IT dovrà completare le seguenti fasi per abilitare l'accesso diretto da iPhone a una soluzione mail abilitata IMAP.

- Aprite la porta 993 per consentire la ricezione di e-mail attraverso il firewall. Il proxy server deve essere impostato su IMAP over SSL. SSL garantisce una codifica sicura della posta elettronica durante la trasmissione wireless.
- Come ulteriore protezione, installate un certificato digitale sul server da una Certificate Authority (CA) fidata come VeriSign. Installare un certificato da una CA è importante per garantire che il proxy server sia un'entità sicura all'interno dell'infrastruttura aziendale.
- Le porte 587, 465 o 25 devono essere aperte per consentire l'invio di e-mail da iPhone. iPhone verifica automaticamente la porta 587, poi la 465 e infine la 25. La porta 587 è la più affidabile e sicura poiché richiede l'autenticazione dell'utente. La porta 25 è da considerarsi la meno sicura poiché è presente da più tempo e pertanto maggiormente soggetta agli attacchi degli hacker. Inoltre, è la porta che alcuni ISP bloccano per impostazione predefinita onde evitare l'invio di posta indesiderata.

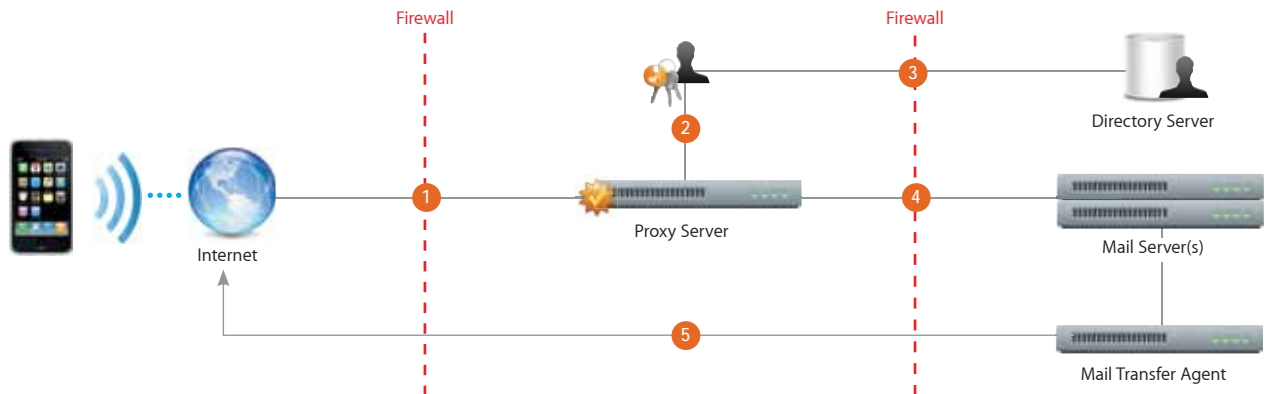
Scenario di deployment IMAP

Ricevere e-mail



- 1 iPhone richiede accesso alla posta sulla porta 993 (IMAP/SSL).
- 2 In seguito, l'utente di iPhone deve essere autenticato dalla rete aziendale. L'operazione viene gestita dal proxy server, che funge da gateway sicuro.
- 3 Il proxy server verifica le informazioni dell'account utilizzando il servizio di directory.
- 4 Dopo l'autenticazione dell'account utente, il proxy server indirizza la richiesta al mail server.
- 5 Messaggi e aggiornamenti vengono recuperati e inviati nuovamente all'utente attraverso la porta 993. Ciò che l'utente vedrà saranno i nuovi messaggi e aggiornamenti su iPhone.

Inviare e-mail



- 1 La posta inviata viene indirizzata attraverso la porta 587 (SSL/TLS).
- 2 Le richieste di invio vengono quindi indirizzate attraverso il proxy server.
- 3 Il proxy server avvia il processo di autenticazione con il servizio Active Directory.
- 4 Dopo che l'utente viene autenticato, il messaggio viene indirizzato attraverso il mail server e una copia posizionata nella cartella dei messaggi inviati dell'utente.
- 5 Il messaggio passa quindi da Mail Transfer Agent e viene inviato attraverso la porta 587 al destinatario esterno tramite SMTP (SSL/TLS).

Panoramica sulla configurazione del dispositivo iPhone

Il deployment di iPhone all'interno della vostra impresa è facile, grazie al software iPhone 2.0. I dispositivi iPhone possono essere configurati tramite dei profili di configurazione creati e distribuiti dal vostro reparto IT. I profili di configurazione sono documenti XML che, una volta installati, forniscono delle informazioni che iPhone utilizza per connettersi e comunicare con i sistemi aziendali.

Componenti dei profili di configurazione



Impostazioni Exchange

Includete le informazioni su server, dominio e account in un profilo di configurazione così gli utenti dovranno unicamente fornire una password per connettersi tramite Microsoft Exchange ActiveSync.



Impostazioni wireless

Sia che stiate configurando iPhone per la connessione a una rete privata sia che invece lo stiate impostando per l'autenticazione RADIUS ai punti di accesso wireless dell'azienda, i profili di configurazione possono essere distribuiti per facilitare le connessioni ai punti di accesso.



Impostazioni VPN

Configurate impostazioni, account, proxy, certificati, token, password, gruppi e Shared Secret del server VPN per le vostre reti private aziendali.



Impostazioni e-mail

Configurate le impostazioni di posta IMAP o POP, inclusi i mail server per la posta in uscita e in entrata.



Policy dei passcode

Protegete i dati della vostra azienda configurando le policy dei passcode dei dispositivi. Impostate il numero minimo di caratteri, il numero di caratteri complessi richiesti, la scadenza del passcode, l'intervallo di blocco del dispositivo e il numero massimo di tentativi.



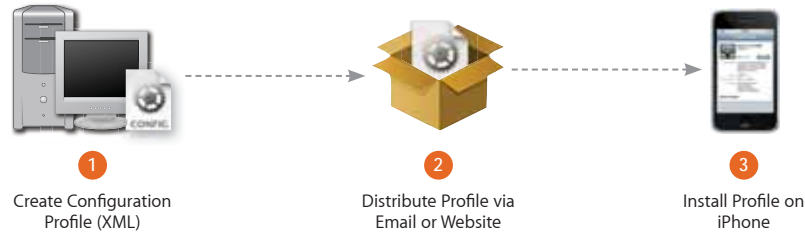
Certificati

Verificate l'identità degli utenti e controllate l'accesso ai servizi chiave dell'azienda quali le reti VPN e WPA2 Enterprise/802.1x su iPhone. Eseguite il deployment dei certificati in formati raw PKCS1 (.cer, .crt, .der) e PKCS12 (.p12, .pfx).



Firme

Aggiungete al vostro profilo di configurazione un'identità così gli utenti sapranno che proviene da una fonte sicura.



1 Creazione dei profili

iPhone Configuration Utility

Una semplice e intuitiva applicazione per gli amministratori IT, iPhone Configuration Utility vi offre la possibilità di creare facilmente dei profili di configurazione. iPhone Configuration Utility è disponibile come applicazione web o come applicazione desktop nativa per Mac OS X.



2 Distribuzione dei profili

Sito web sicuro

- Esportate il profilo da iPhone Configuration Utility.
- Aggiungete il tipo MIME adeguato al vostro web server.
application/x-apple-aspen-config mobileconfig
- Ospitate il profilo di configurazione (non compresso) su un sito sicuro accessibile dagli utenti.

Allegato e-mail

- Esportate il profilo da iPhone Configuration Utility.
- Allegate il profilo di configurazione (non compresso) a un messaggio e-mail e inviatelo agli utenti.



3 Installazione dei profili

Installazione su iPhone

- Se il profilo è ospitato sul Web, navigate nel sito con Safari su iPhone e toccate il documento per avviare l'installazione su iPhone.
- I profili di configurazione inviati come allegati e-mail possono essere installati toccando direttamente il documento dal corpo del messaggio in Mail su iPhone.
- Toccate Install (installa) per accettare le impostazioni. Durante l'installazione, gli utenti devono immettere tutte le informazioni eventualmente necessarie (come la password dell'account) per completare la configurazione del dispositivo.