iPhone OS

Guía de integración en empresas

Segunda edición, para la versión 3.2 o posterior

Apple
1 Infinite Loop
Cupertino, CA 95014
408-996-1010
www.apple.com

Publicado simultáneamente en Estados Unidos y Canadá.

E019-1835/2010-04

Contenido

El iPhone en la empresa

Aprenda a integrar el iPhone, el iPod touch y el iPad en los sistemas de su empresa.

Destinada a administradores de sistemas, esta guía proporciona información sobre la integración y el mantenimiento del iPhone, el iPod touch y el iPad en entornos empresariales.

Novedades de iPhone OS 3.0 y versiones posteriores para las empresas

El sistema iPhone OS 3.x incluye numerosas mejoras, entre las que se incluyen las siguientes, de especial interés para los usuarios de empresas:

- Es posible la sincronización inalámbrica con calendarios CalDAV.
- Compatibilidad con servidor LDAP para buscar contactos en Mail, Agenda y SMS.
- Los perfiles de configuración pueden encriptarse y bloquearse en un dispositivo, de forma que, para eliminarlos, sea necesaria una contraseña de administrador.
- La Utilidad Configuración iPhone le permite añadir y eliminar perfiles de configuración encriptados directamente en los dispositivos conectados a su ordenador por USB.
- Compatibilidad de la revocación de certificados con el protocolo OCSP (Online Certificate Status Protocol).
- Ahora es posible establecer conexiones VPN basadas en certificados por petición.
- Se permite la configuración de proxy VPN a través de un perfil de configuración y servidores de VPN.
- Los usuarios de Microsoft Exchange pueden invitar a reuniones a otros usuarios. Los usuarios de Microsoft Exchange 2007 también pueden ver el estado de las respuestas.
- Compatibilidad con la autenticación basada en certificados de cliente de Exchange ActiveSync.
- Compatibilidad con políticas EAS adicionales y con el protocolo EAS 12.1.

- Posibilidad de seleccionar restricciones de dispositivo adicionales, incluida la posibilidad de especificar el tiempo que un dispositivo puede permanecer desbloqueado, desactivar la cámara e impedir que los usuarios puedan realizar capturas de pantalla del dispositivo.
- Es posible buscar en los mensajes de correo electrónico y eventos de calendario locales. En el caso de IMAP, MobileMe y Exchange 2007, también es posible buscar en los mensajes alojados en el servidor.
- Posibilidad de designar carpetas de correo electrónico adicionales para la entrega de correo electrónico push.
- Posibilidad de especificar los ajustes de proxy APN mediante un perfil de configuración.
- Los clips web se pueden instalar mediante un perfil de configuración.
- Se ha añadido la compatibilidad con 802.1x EAP-SIM.
- Los dispositivos se pueden autenticar e inscribir de forma remota mediante un servidor SCEP (Simple Certificate Enrollment Protocol).
- iTunes puede almacenar copias de seguridad de dispositivos con formato encriptado.
- La Utilidad Configuración iPhone admite la creación de perfiles mediante scripts.
- La Utilidad Configuración iPhone 2.2 es compatible con el iPad, el iPhone y el iPod touch. Para utilizarla, se requiere Mac OS X 10.6 Snow Leopard. También es compatible con Windows 7.

Requisitos del sistema

En esta sección se proporciona una visión general de los requisitos del sistema y de los componentes disponibles para integrar el iPhone, el iPod touch y el iPad en los sistemas de su empresa.

iPhone e iPod touch

Los dispositivos iPhone y iPod touch que utilice con la red de su empresa deben tener actualizado el sistema iPhone OS 3.1.x.

iPad

El iPad debe actualizarse a iPhone OS 3.2.x.

iTunes

Se requiere iTunes 9.1 o posterior para configurar un dispositivo. iTunes también es necesario para instalar actualizaciones de software del iPhone, el iPod touch y el iPad. Además, iTunes se puede utilizar para instalar aplicaciones y sincronizar música, vídeo, notas u otros datos con un Mac o un PC.

Para utilizar iTunes, necesita un Mac o un PC que disponga de un puerto USB 2.0 y que cumpla los requisitos mínimos que se indican en el sitio web de iTunes. Consulte www.apple.com/es/itunes/download/.

Utilidad Configuración iPhone

La Utilidad Configuración iPhone le permite crear, encriptar e instalar perfiles de configuración, rastrear e instalar perfiles de datos y aplicaciones autorizadas, y obtener información de los dispositivos (como los registros de consola).

Utilidad Configuración iPhone necesita uno de los elementos siguientes:

- Mac OS X 10.5 Snow Leopard
- Windows XP Service Pack 3 con .NET Framework 3.5 Service Pack 1
- Windows Vista Service Pack 1 con .NET Framework 3.5 Service Pack 1
- Windows 7 con .NET Framework 3.5 Service Pack 1

Utilidad Configuración iPhone funciona tanto con las versiones de Windows de 32 bits como con las de 64 bits.

Puede descargar el instalador de .Net Framework 3.5 Service Pack 1 desde: http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7

La utilidad le permite crear un mensaje de Outlook con un perfil de configuración como archivo adjunto. Además, puede asignar nombres de usuario y direcciones de correo electrónico desde la agenda de su ordenador a los dispositivos que haya conectado a la utilidad. Estas dos características necesitan disponer de Outlook y no son compatibles con Outlook Express. Para usar estas funciones en ordenadores con Windows XP, puede que necesite instalar la actualización de 2007 Microsoft Office System: Ensamblados de interoperabilidad primarios redistribuibles. Esta actualización es necesaria si se instaló Outlook antes del .NET Framework 3.5 Service Pack 1.

El instalador de ensamblados de interoperabilidad primarios Primary Interop Assemblies está disponible en: http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513

Microsoft Exchange ActiveSync

El iPhone, el iPod touch y el iPad son compatibles con las siguientes versiones de Microsoft Exchange:

- Exchange ActiveSync para Exchange Server (EAS) 2003 Service Pack 2
- Exchange ActiveSync para Exchange Server (EAS) 2007

Para obtener compatibilidad con las políticas y funciones de Exchange 2007, es necesario instalar el Service Pack 1.

Políticas de Exchange ActiveSync compatibles

Son compatibles las siguientes políticas de Exchange:

- Uso obligatorio de contraseña en el dispositivo
- Longitud mínima de la contraseña
- Número máximo de intentos fallidos de introducción de la contraseña
- Requerir números y letras
- Tiempo de inactividad en minutos

También son compatibles las siguientes políticas de Exchange 2007:

- Permitir o prohibir contraseña sencilla
- Caducidad de contraseñas
- Historial de contraseñas
- Intervalo de actualización de políticas
- Número mínimo de caracteres complejos en contraseña
- Exigir sincronización manual durante la itinerancia
- Permitir cámara
- Requerir encriptación de dispositivo

Para obtener una descripción de cada política, consulte la documentación de Exchange ActiveSync.

El iPhone 3GS, el iPod touch (modelos de otoño de 2009 con 32 GB o más) y el iPad admiten la política de Exchange de requerir la encriptación del dispositivo (RequireDeviceEncryption). El iPhone, el iPhone 3G y otros modelos del iPod touch no admiten la encriptación de dispositivos, por lo que no podrán conectarse a servidores Exchange que la requieran.

Si activa la política "Exigir números y letras" en Exchange 2003 o la política "Requerir una contraseña alfanumérica" en Exchange 2007, el usuario deberá introducir un código del dispositivo que contenga al menos un carácter complejo.

El valor especificado por la política de tiempo de inactividad (MaxInactivityTimeDeviceLock o AEFrequencyValue) se utiliza para ajustar el valor máximo que los usuarios pueden seleccionar en Ajustes > General > "Bloqueo automático" y en Ajustes > General > Bloqueo con código > Solicitar.

Barrido remoto

Es posible eliminar de forma remota el contenido de un iPhone, un iPod touch o un iPad. El barrido borra todos los datos e información de configuración del dispositivo. El dispositivo se borra y restaura con los ajustes de fábrica originales de forma segura.

Importante: En el iPhone y el iPhone 3G, el barrido sobrescribe los datos del dispositivo y puede tardar aproximadamente una hora en completarse por cada 8 GB de capacidad del dispositivo. Conecte el dispositivo a una fuente de alimentación antes del barrido. Si el dispositivo se apaga por falta de batería, el proceso de barrido se reanudará cuando el dispositivo se conecte a una fuente de alimentación. En el iPhone 3GS y el iPad, el barrido elimina la clave de encriptación de los datos (que está encriptada mediante el sistema de encriptación AES de 256 bits) y se produce de forma instantánea.

Con Exchange Server 2007 es posible iniciar un barrido remoto mediante Exchange Management Console, Outlook Web Access o la herramienta de administración web de servicios móviles de Exchange ActiveSync.

Con Exchange Server 2003 es posible iniciar un barrido remoto mediante la herramienta de administración web de servicios móviles de Exchange ActiveSync.

Los usuarios también pueden borrar un dispositivo de su posesión seleccionando "Borrar contenidos y ajustes" en el menú Restaurar del panel de ajustes General. Los dispositivos también pueden configurarse para que inicien automáticamente un barrido tras varios intentos fallidos de emplear el código.

Si recupera un dispositivo que se había barrido porque se había perdido, utilice iTunes para restaurarlo con la copia de seguridad más reciente del dispositivo.

Microsoft Direct Push

El servidor Exchange proporciona correo electrónico, contactos y eventos de calendario al iPhone y al iPad Wi-Fi + 3G de forma automática si hay una conexión de datos móviles o Wi-Fi disponible. El iPod touch y el iPad Wi-Fi no tienen una conexión de telefonía móvil, por lo que solo reciben notificaciones push cuando están activos y conectados a una red Wi-Fi.

Función Autodiscover de Microsoft Exchange

El servicio Autodiscover de Exchange Server 2007 es compatible. Cuando se configura un dispositivo manualmente, la función Autodiscover utiliza su dirección de correo electrónico y contraseña para determinar automáticamente la información del servidor Exchange correcto. Para obtener información acerca de cómo activar el servicio Autodiscover, consulte http://technet.microsoft.com/es-es/library/cc539114.aspx.

Lista global de direcciones de Microsoft Exchange

El iPhone, el iPod touch y el iPad obtienen la información de contacto del directorio corporativo del servidor Exchange de su empresa. Cuando realice una búsqueda en Contactos, podrá acceder al directorio de modo que se obtenga automáticamente la información necesaria para completar las direcciones de correo electrónico a medida que las escribe.

Características compatibles adicionales de Exchange ActiveSync

Además de las funciones y características que ya hemos descrito, el sistema iPhone OS permite:

- Crear invitaciones a calendarios. Con Microsoft Exchange 2007, también puede visualizar el estado de las respuestas a sus invitaciones.
- Determinar el estado Libre, Ocupado, Por confirmar o Fuera para los eventos de calendario.
- Buscar mensajes de correo electrónico en el servidor. Se necesita Microsoft Exchange 2007.
- Autenticación basada en certificados de cliente de Exchange ActiveSync.

Características de Exchange ActiveSync no compatibles

No todas las funciones de Exchange son compatibles, como por ejemplo:

- Gestión de carpetas
- Apertura en un correo electrónico de enlaces a documentos almacenados en servidores Sharepoint
- Sincronización de tareas
- Ajuste de mensajes de respuesta automática "fuera de la oficina"
- Marcado de mensajes para seguimiento

VPN

El sistema iPhone OS trabaja con servidores VPN compatibles con los siguientes protocolos y métodos de autenticación:

- L2TP/IPsec con autenticación de usuario mediante MS-CHAPV2 Password, RSA SecurID y CryptoCard, y autenticación automática mediante secreto compartido.
- PPTP con autenticación de usuario mediante MS-CHAPV2 Password, RSA SecurID y CryptoCard.
- Cisco IPsec con autenticación de usuario mediante contraseña, RSA SecurID o CryptoCard, y autenticación automática mediante secreto compartido y certificados. En el Apéndice A puede consultar los servidores VPN Cisco compatibles y las recomendaciones para su configuración.

Cisco IPsec con autenticación basada en certificados admite la VPN por petición para los dominios que se especifiquen durante la configuración. Para obtener más información, consulte “Ajustes VPN” en la página 39.

Seguridad de red

El sistema iPhone OS es compatible con los siguientes estándares de seguridad para redes inalámbricas 802.11i definidos por la Wi-Fi Alliance:

- WEP
- WPA Personal
- WPA Empresa
- WPA2 Personal
- WPA2 Empresa

Además, el sistema iPhone OS es compatible con los siguientes métodos de autenticación 802.1X para redes WPA Empresa y WPA2 Empresa:

- EAP-TLS
- EAP -TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, PEAP v1
- LEAP

Certificados e identidades

El iPhone, el iPod touch y el iPad pueden utilizar certificados X.509 con claves RSA. Se reconocen las extensiones de archivo .cer, .crt y .der. Safari, Mail, VPN y otras aplicaciones efectúan evaluaciones de cadenas de certificados.

Utilice archivos P12 (estándar PKCS #12) que contengan una sola identidad. Se reconocen las extensiones de archivo .p12 y .pfx. Cuando se instala una identidad, se solicita al usuario la contraseña que la protege.

Los certificados necesarios para establecer la cadena de certificados a un certificado raíz fiable pueden instalarse manualmente o mediante perfiles de configuración. No es necesario añadir los certificados raíz que Apple ya ha incluido en el dispositivo. Para ver una lista de los sistemas raíz preinstalados, consulte el siguiente artículo de soporte técnico de Apple: http://support.apple.com/kb/HT3580?viewlocale=es_ES.

Los certificados pueden instalarse con seguridad de forma remota mediante SCEP. Consulte "Información general sobre el proceso de registro y configuración mediante autenticación" en la página 25 para obtener más información.

Cuentas de correo electrónico

El iPhone, el iPod touch y el iPad son compatibles con los sistemas de correo electrónico estándar IMAP4 y POP3 en diversas plataformas de servidor, como Windows, UNIX, Linux y Mac OS X. También puede usar IMAP para acceder al correo electrónico de las cuentas Exchange además de la cuenta Exchange que utiliza con la tecnología "direct push".

Cuando un usuario busca en su correo, tiene la posibilidad de seguir buscando en el servidor de correo electrónico. Esta función también está disponible con Microsoft Exchange Server 2007 y con la mayoría de las cuentas basadas en IMAP.

La información de la cuenta de correo electrónico del usuario, incluido su ID de usuario y su contraseña de Exchange, se almacenan de forma segura en el dispositivo.

Servidores LDAP

El iPhone, el iPod touch y el iPad pueden recuperar información de contactos de los directorios de servidor LDAPv3 de su empresa. Puede acceder a los directorios cuando realice búsquedas en Contactos y se accede a ellos de forma automática para completar las direcciones de correo electrónico a medida que se escriben.

Servidores CalDAV

El iPhone, el iPod touch y el iPad pueden sincronizar datos de calendario con el servidor CalDAV de su empresa. Los cambios en el calendario se actualizan regularmente entre el dispositivo y el servidor.

También puede suscribirse a calendarios publicados de solo lectura, como pueden ser calendarios de días festivos o los calendarios de planificación de un compañero de trabajo.

Las cuentas CalDAV no permiten la creación y el envío de invitaciones de calendario nuevas desde un dispositivo.

Otros recursos

Además de esta guía, las siguientes publicaciones y sitios web proporcionan información útil:

- Página web del iPhone en la empresa: www.apple.com/es/iphone/enterprise/
- Página web "El iPad en la empresa": www.apple.com/es/ipad/business/
- Visión general sobre Exchange: http://technet.microsoft.com/es-es/library/bb124558.aspx
- Implementación de Exchange ActiveSync: http://technet.microsoft.com/es-es/library/aa995962.aspx
- Biblioteca de documentación técnica de Exchange 2003: http://technet.microsoft.com/es-es/library/bb123872(EXCHG.65).aspx
- Administración de la seguridad de Exchange ActiveSync: http://technet.microsoft.com/es-es/library/bb232020(EXCHG.80).aspx
- Página web de Wi-Fi para la empresa: www.wi-fi.org/enterprise.php (en inglés)
- Conectividad VPN del iPhone a los dispositivos de seguridad adaptable (ASA) de Cisco: www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html
- *Manual del usuario del iPhone*, disponible para su descarga en www.apple.com/es/support/iphone/; para ver el manual en el iPhone, pulse el favorito "iPhone Manual del usuario" en Safari o vaya a http://help.apple.com/iphone/
- Presentación del iPhone: www.apple.com/es/iphone/guidedtour/
- *Manual del usuario del iPod touch*, disponible para su descarga en www.apple.com/es/support/ipodtouch; para ver el manual en el iPod touch, pulse en el favorito "*iPod touch Manual del usuario*" en Safari o vaya a http://help.apple.com/ipodtouch/

- Presentación del iPod touch: www.apple.com/es/ipodtouch/guidedtour/
- *Manual del usuario del iPad*, disponible para su descarga en www.apple.com/es/support/ipad; para ver el manual en el iPad, pulse en "iPad Manual del usuario" en Safari o vaya a http://help.apple.com/ipad/
- Presentación del iPad: www.apple.com/ipad/guided-tours/

Distribución del iPhone y el iPod touch

1

En este capítulo se explica de forma general cómo distribuir el iPhone, el iPod touch y el iPad en su empresa.

El iPhone, el iPod touch y el iPad están diseñados para integrarse con facilidad con los sistemas de su empresa, incluidos Microsoft Exchange 2003 y 2007, redes inalámbricas seguras basadas en 802.1X y redes privadas virtuales Cisco IPsec. Como sucede con cualquier solución empresarial, una buena planificación y un buen conocimiento de las opciones de distribución hacen el proceso más sencillo y eficaz, tanto para usted como para los usuarios.

Cuando planifique la distribución del iPhone, el iPod touch y el iPad, tenga en cuenta lo siguiente:

- ¿Cómo se activarán los iPhone y iPad (modelos Wi-Fi + 3G) de su empresa para el servicio de telefonía móvil inalámbrica?
- ¿A qué servicios de red, aplicaciones y datos de empresa necesitan acceder los usuarios?
- ¿Qué políticas desea implantar en relación con los dispositivos para proteger datos sensibles de la empresa?
- ¿Desea configurar uno a uno y de forma manual los dispositivos o utilizar un proceso sistematizado para configurar todo un grupo de dispositivos?

Las características concretas de su entorno empresarial, las políticas informáticas, el operador inalámbrico y los requisitos en materia de ordenadores y comunicación influyen a la hora de diseñar la estrategia de distribución.

Activación de dispositivos

Cada iPhone debe activarse con su operador inalámbrico antes de poder utilizarse para realizar y recibir llamadas, enviar mensajes de texto o conectarse a la red de datos de telefonía móvil. Póngase en contacto con su operador para conocer las tarifas de voz y datos y las instrucciones de activación, tanto para clientes particulares como para empresas.

Usted o el usuario deben instalar una tarjeta SIM en el iPhone. Tras instalar la tarjeta SIM es necesario conectar el iPhone a un ordenador con iTunes para completar el proceso de activación. Si la tarjeta SIM ya está activada, el iPhone está preparado para su uso inmediato; en caso contrario, iTunes le guiará a través del proceso de activación de una nueva línea de servicio.

El iPad debe conectarse a un ordenador que tenga iTunes instalado para activar el dispositivo. En el caso del iPad Wi-Fi + 3G en EE UU, debe registrarse y gestionar (o cancelar) un plan de datos de AT&T con el iPad. Vaya a Ajustes > Datos móviles > Ver cuenta. El iPad está desbloqueado, por lo que puede utilizar el operador que desee. Póngase en contacto con su operador para configurar una cuenta y obtener una tarjeta micro-SIM compatible. En EE UU, con el iPad Wi-Fi + 3G se incluyen tarjetas micro-SIM compatibles con AT&T.

Aunque el iPod touch y el iPad Wi-Fi carecen de servicio de telefonía móvil y tarjeta SIM, para activarlos también es necesario conectarlos a un ordenador con iTunes.

Puesto que se necesita iTunes para completar el proceso de activación, deberá decidir si desea instalar iTunes en el Mac o PC de cada uno de los usuarios o si prefiere completar la activación de todos los dispositivos con su propia instalación de iTunes.

Tras la activación, no se precisa iTunes para utilizar el dispositivo con los sistemas de su empresa, aunque sí para sincronizar música, vídeos y favoritos web con un ordenador. iTunes también es necesario para descargar e instalar actualizaciones de software para los dispositivos, así como para instalar las aplicaciones de empresa.

Para obtener más información acerca de la activación de dispositivos y el uso de iTunes, consulte capítulo 4.

Preparación del acceso a los servicios de red y los datos empresariales

El software iPhone OS 3.x permite utilizar de forma segura correo electrónico, contactos y calendarios push con su solución actual de Microsoft Exchange Server 2003 o 2007, así como la Lista global de direcciones, el barrido remoto y la aplicación de políticas de códigos de dispositivo. También permite a los usuarios conectarse de forma segura a recursos de la empresa mediante redes inalámbricas WPA Empresa y WPA2 Empresa utilizando la autenticación inalámbrica 802.1X o VPN con los protocolos PPTP, LT2P sobre IPsec o Cisco IPsec.

Aunque su empresa no utilice Microsoft Exchange, sus usuarios pueden utilizar el iPhone o el iPod touch para sincronizar el correo electrónico de forma inalámbrica con la mayoría de los servidores y servicios estándar basados en POP e IMAP. También pueden utilizar iTunes para sincronizar eventos de calendario y contactos desde iCal y la Agenda en Mac OS X, o desde Microsoft Outlook en un PC con Windows. Para el acceso inalámbrico a calendarios y directorios, los protocolos CalDAV y LDAP son compatibles.

A la hora de decidir a qué servicios de red podrán acceder los usuarios, consulte la información de los siguientes apartados.

Microsoft Exchange

El iPhone se comunica directamente con su servidor Microsoft Exchange mediante Microsoft Exchange ActiveSync (EAS). Exchange ActiveSync mantiene una conexión entre Exchange Server y el iPhone o el iPad Wi-Fi + 3G para que, cuando se reciba un mensaje de correo electrónico nuevo o una invitación, el dispositivo se actualice inmediatamente. El iPod touch y el iPad Wi-Fi no tienen una conexión de telefonía móvil, por lo que solo reciben notificaciones push cuando están activos y conectados a una red Wi-Fi.

Si su empresa ya trabaja con Exchange ActiveSync mediante Exchange Server 2003 o Exchange Server 2007, entonces ya dispondrá de los servicios necesarios. En Exchange Server 2007, asegúrese de que el servidor de acceso de cliente está instalado. En Exchange Server 2003, compruebe que tiene activado Outlook Mobile Access (OMA).

Si dispone de un servidor Exchange pero su empresa no utiliza Exchange ActiveSync, consulte la información de los siguientes apartados.

Configuración de red

- Asegúrese de que el puerto 443 está abierto en el firewall. Si su empresa utiliza Outlook Web Access, lo más probable es que el puerto 443 ya esté abierto.
- Compruebe que haya un certificado de servidor instalado en el servidor Exchange frontal y, en las propiedades de los métodos de autenticación, active sólo la autenticación básica para solicitar una conexión SSL al directorio Microsoft Server ActiveSync de su IIS (servidor de información de Internet de Microsoft).

- Si está utilizando un servidor Microsoft Internet Security and Acceleration (ISA), compruebe que haya instalado un certificado de servidor y actualice la DNS pública para resolver de forma apropiada las conexiones entrantes.
- Asegúrese de que la DNS de su red devuelve una sola dirección configurable desde el exterior para el servidor Exchange ActiveSync, tanto para la intranet como para los clientes por Internet. De este modo, el dispositivo puede utilizar la misma dirección IP para comunicarse con el servidor cuando ambos tipos de conexión están activos.
- Si está utilizando un servidor ISA de Microsoft, cree un dispositivo de escucha web, así como una regla de publicación de acceso de clientes web a Exchange. Para obtener más información, consulte la documentación de Microsoft.
- Seleccione 30 minutos como tiempo máximo de inactividad de sesión en todos los firewall y dispositivos de red. Para obtener información acerca de los intervalos de latido y tiempo de espera, consulte la documentación de Microsoft Exchange en http://technet.microsoft.com/en-us/library/cc182270.aspx.

Configuración de la cuenta Exchange

- Active Exchange ActiveSync para usuarios o grupos específicos utilizando el servicio Active Directory. En Exchange Server 2003 y Exchange Server 2007 se activan de forma predeterminada para todos los dispositivos móviles de la empresa. Para Exchange Server 2007, consulte "Configuración de destinatarios" en la consola de administración de Exchange.
- Configure funciones móviles, políticas y ajustes de seguridad de dispositivos utilizando el administrador del sistema de Exchange. En Exchange Server 2007, debe realizarlo en la consola de administración de Exchange.
- Descargue e instale la herramienta web de administración móvil de Microsoft Exchange ActiveSync, necesaria para iniciar un barrido remoto. En Exchange Server 2007, el barrido remoto también puede iniciarse mediante Outlook Web Access o la consola de administración de Exchange.

Redes Wi-Fi WPA/WPA2 Empresa

La compatibilidad con WPA Empresa y WPA2 Empresa permite acceder a las redes inalámbricas de la empresa con el iPhone, el iPod touch y el iPad de forma segura. WPA/WPA2 Empresa utiliza encriptación AES de 128 bits, un método de encriptación muy fiable basado en bloques que proporciona un alto nivel de seguridad a los datos de la empresa.

Gracias a la compatibilidad con la autenticación 802.1X, los dispositivos iPhone OS se pueden integrar en un amplio abanico de entornos de servidor RADIUS. Son compatibles los métodos de autenticación inalámbrica 802.1X como, por ejemplo, EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 y LEAP.

Configuración de red WPA/WPA2 Empresa

- Compruebe la compatibilidad de los dispositivos de red y seleccione un tipo de autenticación (tipo EAP) compatible con el iPhone, el iPod touch y el iPad. Asegúrese de que 802.1X está activado en el servidor de autenticación y, si es necesario, instale un certificado de servidor y asigne permisos de acceso a la red a usuarios y grupos.
- Configure los puntos de acceso inalámbrico para la autenticación 802.1X e introduzca la información de servidor RADIUS correspondiente.
- Pruebe su distribución 802.1X con un Mac o un PC para asegurarse de que la autenticación RADIUS está correctamente configurada.
- Si piensa utilizar una autenticación basada en certificados, compruebe mediante el correspondiente proceso de distribución de claves de que su infraestructura de clave pública esté configurada para admitir certificados de dispositivos y usuarios.
- Verifique la compatibilidad de los formatos de sus certificados con el dispositivo y su servidor de autenticación. Para obtener información acerca de los certificados, consulte "Certificados e identidades" en la página 13.

Redes privadas virtuales

El acceso seguro a redes privadas es posible en el iPhone, el iPod touch y el iPad mediante los protocolos de red virtual privada Cisco IPsec, L2TP sobre IPsec y PPTP. Si su empresa utiliza uno de estos protocolos, para usar los dispositivos con su infraestructura VPN no necesitará una configuración adicional de red ni aplicaciones de terceros.

Las distribuciones con Cisco IPsec pueden aprovechar la autenticación con certificado mediante los certificados estándar x.509. Además, la autenticación con certificado le permite aprovechar la modalidad VPN por petición, que proporciona acceso inalámbrico fácil y seguro a la red de su empresa.

En el caso de la autenticación mediante tokens de dos factores, el sistema iPhone OS admite RSA SecurID y CryptoCard. Al establecer una conexión VPN, el usuario introduce directamente en el dispositivo su PIN y una contraseña única generada por token. En el Apéndice A puede consultar los servidores Cisco VPN compatibles y las recomendaciones para su configuración.

El iPhone, el iPod touch y el iPad también son compatibles con la autenticación mediante secreto compartido para distribuciones Cisco IPsec y L2TP/IPsec, así como con la autenticación básica MS-CHAPv2 mediante nombre de usuario y contraseña.

También son compatibles con la configuración automática de proxy VPN (PAC y WPAD), que le permite especificar los ajustes del servidor proxy para acceder a direcciones URL concretas.

Pautas de configuración VPN

- El sistema iPhone OS se integra con la mayoría de las redes VPN existentes, de modo que basta con una configuración mínima para permitir el acceso de los dispositivos a su red. El mejor modo de preparar la distribución es comprobar si los protocolos VPN existentes y los métodos de autenticación de su empresa son compatibles con el iPhone.
- Asegúrese que los concentradores VPN cumplen con los estándares. También es recomendable revisar la ruta de autenticación hacia su servidor RADIUS o de autenticación para comprobar que los estándares compatibles con el sistema iPhone OS están activados en su versión.
- Consulte con sus proveedores de soluciones para confirmar que su software y su equipo están actualizados con los parches de seguridad y el firmware más recientes.
- Si desea configurar ajustes del proxy para determinadas URL, coloque un archivo PAC en un servidor web que sea accesible con los ajustes de VPN básicos, y asegúrese de que se proporcione con el tipo MIME "application/x-ns-proxy-autoconfig". Otra posibilidad es configurar su DNS o DHCP para que proporcione la ubicación del archivo WPAD en un servidor que sea igualmente accesible.

Correo electrónico IMAP

Aunque no utilice Microsoft Exchange, puede instalar una solución de correo electrónico segura y estandarizada mediante cualquier servidor de correo electrónico compatible con IMAP y configurado para solicitar autenticación de usuario y SSL. Por ejemplo, puede acceder al correo electrónico en Lotus Notes/Domino o Novell Groupwise utilizando esta técnica. Los servidores de correo se pueden encontrar dentro de una subred DMZ, tras un firewall de la empresa o en ambas situaciones a la vez.

Con SSL, el sistema iPhone OS admite la encriptación de 128 bits y los certificados X.509 emitidos por las principales autoridades de certificación. También admite métodos de autenticación estrictos, como los estándares MD5 Challenge-Response y NTLMv2.

Pautas de configuración de redes IMAP

- Para lograr una mayor protección, instale en el servidor un certificado digital emitido por una autoridad de certificación de confianza. La instalación a partir de una autoridad de certificación es un paso importante para asegurar que su servidor proxy pueda considerarse una entidad de confianza en la infraestructura de su empresa. Consulte el apartado "Ajustes de credenciales" en la página 42 para obtener información sobre la instalación de certificados en el iPhone.
- Para permitir que los dispositivos iPhone OS reciban correo electrónico desde su servidor, abra el puerto 993 en el firewall y asegúrese de que el servidor proxy está configurado en IMAP sobre SSL.

- Para permitir el envío de correo electrónico desde los dispositivos, debe tener abiertos los puertos 587, 465 o 25. El primer puerto utilizado es el 587, la mejor opción de las tres.

Directorios LDAP

El sistema iPhone OS le permite acceder a servidores de directorio LDAP estandarizados y proporciona un directorio global de direcciones u otra información similar a la Lista global de direcciones de Microsoft Exchange.

Cuando se configura una cuenta LDAP en el dispositivo, éste busca el atributo `namingContexts` en el directorio raíz del servidor para identificar la base de búsqueda predeterminada. Por omisión, el alcance de la búsqueda es el subdirectorio.

Calendarios CalDAV

Gracias a la compatibilidad de iPhone OS con CalDAV, se pueden proporcionar calendarios y agendas globales para empresas que no utilizan Microsoft Exchange. El sistema iPhone OS funciona con servidores de calendario compatibles con el estándar CalDAV.

Calendarios suscritos

Si desea publicar calendarios de solo lectura para los eventos de la empresa (vacaciones, acontecimientos especiales, etc.), los dispositivos iPhone OS pueden suscribirse a estos calendarios y mostrar la información junto a los calendarios de Microsoft Exchange y CalDAV. iPhone OS admite archivos de calendario en el formato estándar iCalendar (.ics).

Una forma sencilla de distribuir calendarios de suscripción a sus usuarios es enviarles la dirección URL completa mediante SMS o correo electrónico. Cuando el usuario pulse el enlace, el dispositivo le ofrecerá suscribirse al calendario especificado.

Aplicaciones de empresa

Para distribuir aplicaciones para iPhone OS en la empresa, instale las aplicaciones en sus dispositivos mediante la Utilidad Configuración iPhone o iTunes. Una vez distribuida una aplicación en los dispositivos de los usuarios, las actualizaciones serán más sencillas si cada usuario dispone de iTunes instalado en su Mac o PC.

Protocolo OCSP (Online Certificate Status Protocol)

Cuando proporcione certificados digitales para los dispositivos iPhone OS, puede emitirlos de forma que estén preparados para el protocolo OCSP (iniciales en inglés de "protocolo de estado del certificado en línea"). De este modo, el dispositivo preguntará a su servidor OCSP si el certificado ha sido revocado antes de utilizarlo.

Establecimiento de las políticas de código de dispositivo

Una vez decididos el servidor de red y los datos a los que accederán los usuarios, debería determinar qué políticas de código de dispositivo desea implantar.

En las empresas cuyas redes, sistemas o aplicaciones no requieran un código o un token de autenticación se recomienda configurar los dispositivos de modo que soliciten código. Si utiliza autenticación basada en certificado para una red 802.1X o una VPN Cisco IPsec, o si su aplicación de empresa guarda sus datos de inicio de sesión, debería solicitar a los usuarios que configuren un código de dispositivo con un periodo corto, para evitar que se utilice un dispositivo perdido o robado sin conocer su código.

Estas políticas se pueden configurar en el iPhone, el iPod touch y el iPad de dos maneras. Si el dispositivo está configurado para acceder a una cuenta Microsoft Exchange, las políticas Exchange ActiveSync se transmitirán al dispositivo de forma inalámbrica. De este modo, podrá implantar y actualizar las políticas sin que el usuario intervenga. Para obtener información acerca de las políticas EAS, consulte "Políticas de Exchange ActiveSync compatibles" en la página 9.

Si no utiliza Microsoft Exchange puede configurar políticas similares en sus dispositivos creando perfiles de configuración. Si desea cambiar una política, debe publicar o enviar un perfil actualizado a los usuarios o instalarlo mediante la Utilidad Configuración iPhone. Para obtener información acerca de las políticas de código de dispositivo, consulte "Ajustes de código" en la página 36.

Si utiliza Microsoft Exchange, también puede complementar sus políticas EAS mediante políticas de configuración. De este modo se proporciona acceso a políticas que no están disponibles en Microsoft Exchange 2003, por ejemplo, o se le permite definir políticas específicas para los dispositivos iPhone OS.

Configuración de dispositivos

Debe decidir cómo configurará cada iPhone, iPod touch o iPad. Esta decisión depende en parte del número de dispositivos que vaya a distribuir y gestionar a largo plazo. Si el número es pequeño, puede resultar más sencillo que usted o los usuarios los configuren de forma manual. A estos efectos, deberán utilizar el dispositivo para configurar cada cuenta de correo electrónico, los ajustes Wi-Fi y la información de configuración VPN. Para obtener más información sobre la configuración manual, consulte capítulo 3.

Si va a distribuir una gran cantidad de dispositivos o dispone de un gran número de ajustes de red, ajustes de correo electrónico y certificados para instalar, puede resultar más práctico configurar los dispositivos mediante la creación y distribución de perfiles de configuración. Estos perfiles cargan rápidamente en un dispositivo ajustes e información de autorización. Algunos ajustes VPN y Wi-Fi solo se pueden cambiar mediante un perfil de configuración. Si no utiliza Microsoft Exchange, también deberá utilizar un perfil de configuración para configurar las políticas de código de dispositivo.

Los perfiles de configuración se pueden encriptar y firmar, lo que le permite limitar su uso a un determinado dispositivo e impide la modificación de los ajustes del perfil. También puede marcar un perfil como bloqueado con el dispositivo, de modo que una vez instalado no se pueda eliminar sin borrar todos los datos del dispositivo, u opcionalmente, con un código de administrador.

Tanto si configura los dispositivos de forma manual como utilizando perfiles de configuración, también debe decidir si configurará los dispositivos o si delegará esta tarea en los usuarios. La elección depende de dónde estén situados los usuarios, de la política de la empresa acerca de la posibilidad de que los usuarios gestionen su propio equipo informático y de la complejidad de la configuración. Los perfiles de configuración resultan adecuados para grandes empresas, para trabajadores a distancia o para usuarios que no pueden configurar sus propios dispositivos.

Si desea que los usuarios activen el dispositivo o instalen y actualicen las aplicaciones de empresa por su cuenta, todos deben tener instalado iTunes en su Mac o PC. iTunes también es necesario para actualizar el software iPhone OS, por lo que deberá tenerlo en cuenta si decide no distribuir iTunes a sus usuarios. Para obtener información acerca de la distribución de iTunes, consulte el capítulo 4.

Registro y configuración remotos

El *registro* es el proceso de autenticación de un dispositivo y un usuario que le permite automatizar el proceso de distribución de certificados. Los certificados digitales tienen muchas ventajas para los usuarios. Sirven para autenticar el acceso a los principales servicios de la empresa, como Microsoft Exchange ActiveSync, redes inalámbricas WPA2 Empresa y conexiones VPN corporativas. La autenticación mediante certificado también permite el uso de VPN por petición, que ofrece un perfecto método de acceso a redes corporativas.

Además de utilizar las funciones de registro remoto para emitir certificados para la infraestructura de clave pública de su empresa (PKI), también puede distribuir perfiles de configuración de dispositivo, lo que garantiza el acceso únicamente de los usuarios de confianza a los servicios corporativos y la configuración de sus dispositivos de acuerdo con sus políticas informáticas. Puesto que los perfiles de configuración pueden encriptarse y bloquearse, sus ajustes no se pueden eliminar, modificar ni compartir. Estas funciones están disponibles en el proceso remoto que se describe a continuación, así como en la Utilidad Configuración iPhone al configurar dispositivos que están conectados físicamente al ordenador administrador. Consulte el capítulo 2 para obtener más información acerca del uso de la Utilidad Configuración iPhone.

La implementación de los procesos de registro y configuración remotos requiere el desarrollo y la integración de los servicios de autenticación, directorio y certificados. El proceso se puede distribuir mediante servicios web estándar, y una vez instaurado, permite a los usuarios configurar sus dispositivos con total seguridad mediante autenticación.

Información general sobre el proceso de registro y configuración mediante autenticación

Para implementar este proceso, es necesario que cree su propio *servicio de distribución de perfiles* que acepte conexiones HTTP, autentique usuarios, cree perfiles mobileconfig y gestione todo el proceso descrito en este apartado.

También necesita una autoridad de certificación (o CA, por sus iniciales en inglés) que emita las credenciales de los dispositivos mediante el protocolo SCEP (Simple Certificate Enrollment Protocol). Para encontrar enlaces a información sobre PKI, SCEP y otros temas relacionados, consulte “Otros recursos” en la página 30.

El siguiente diagrama muestra el proceso de registro y configuración que admite el iPhone.

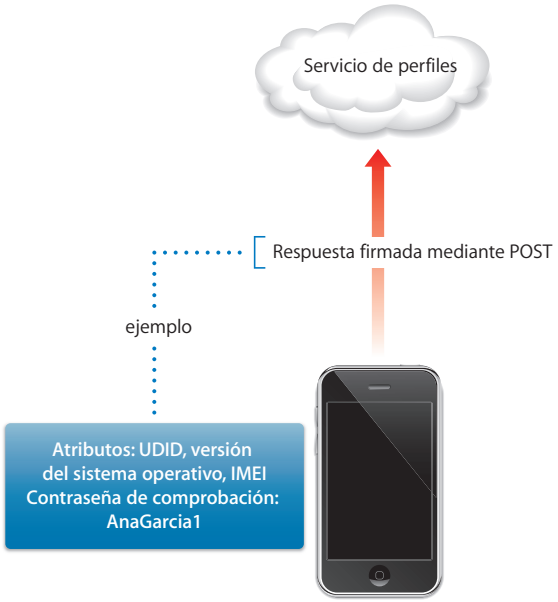
Fase 1: Inicio del registro

Fase 1 – Inicio del registro: el proceso de registro comienza cuando el usuario accede mediante Safari a la URL del servicio de distribución de perfiles que usted ha creado. Puede distribuir esta URL mediante SMS o correo electrónico. La petición de registro (representada como el paso 1 en el diagrama) deberá autenticar la identidad del usuario. La autenticación puede realizarse mediante una autenticación básica o puede estar vinculada a sus servicios de directorio.

En el paso 2, su servicio envía como respuesta un perfil de configuración (.mobileconfig). Esta respuesta especifica una lista de atributos que el dispositivo debe proporcionar en la siguiente respuesta y una clave precompartida (contraseña de comprobación) que puede contener la identidad del usuario durante este proceso para que usted pueda personalizar el proceso de configuración de cada usuario. Los atributos del dispositivo que el servicio puede solicitar son: versión de iPhone OS, ID del dispositivo (dirección MAC), tipo de producto (el iPhone 3GS se identifica como iPhone2,1), ID del teléfono (IMEI) e información de la SIM (ICCID).

Puede consultar un perfil de configuración de ejemplo de esta fase en “Ejemplo de respuesta del servidor (fase 1)” en la página 91.

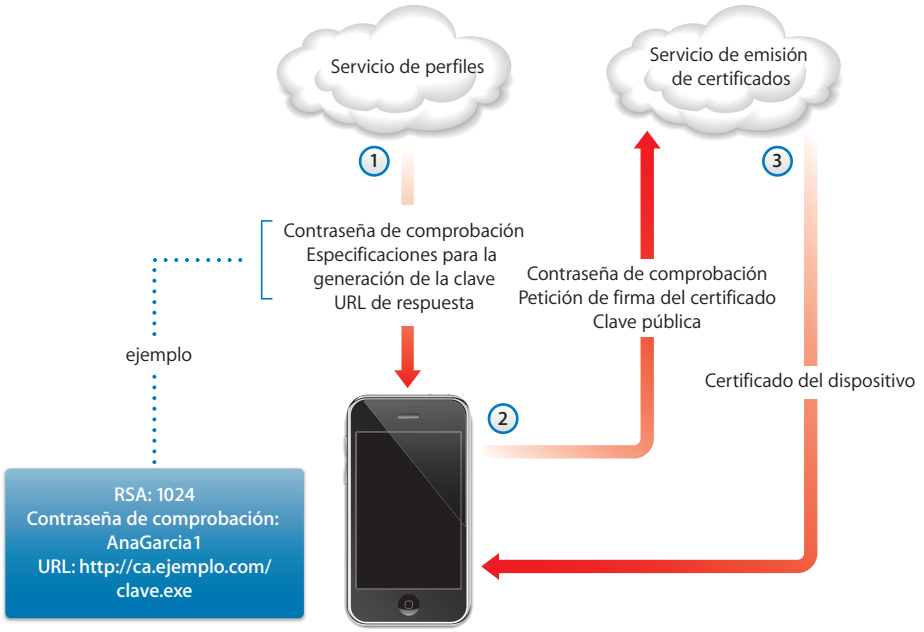
Fase 2: Autenticación del dispositivo



Fase 2 – Autenticación del dispositivo: una vez que el usuario acepta la instalación del perfil recibido en la fase 1, el dispositivo busca los atributos solicitados, añade la respuesta de comprobación (si se proporciona), firma la respuesta mediante la identidad integrada en el dispositivo (certificado emitido por Apple) y la devuelve al servicio de distribución de perfiles mediante HTTP Post.

Puede consultar un perfil de configuración de ejemplo de esta fase en "Ejemplo de respuesta del dispositivo (fase 2)" en la página 92.

Fase 3: Instalación del certificado del dispositivo



Fase 3 – Instalación del certificado: en el paso 1, el servicio de distribución de perfiles responde con especificaciones que el dispositivo utiliza para generar una clave (RSA 1024) y con la ubicación a la que devolverla para la certificación mediante SCEP (Simple Certificate Enrollment Protocol).

En el paso 2, la petición SCEP debe gestionarse de modo automático utilizando la contraseña de comprobación del paquete SCEP para autenticar la petición.

En el paso 3, la CA responde con un certificado de encriptación para el dispositivo.

Puede consultar un perfil de configuración de ejemplo de esta fase en “Ejemplo de respuesta del servidor con especificaciones SCEP (fase 3)” en la página 93.

Fase 4: Configuración del dispositivo

Fase 4 – Configuración del dispositivo: en el paso 1, el dispositivo responde con la lista de atributos, firmados mediante el certificado de encriptación proporcionado por la CA en la fase anterior.

En el paso 2, el servicio de perfiles responde con un archivo .mobileconfig encriptado que se instala automáticamente. El servicio de perfiles debe firmar el archivo .mobileconfig. Su certificado SSL puede utilizarse con este fin, por ejemplo.

Además de los ajustes generales, este perfil de configuración deberá definir también las políticas empresariales que desee aplicar y deberá estar bloqueado para que el usuario no lo pueda eliminar del dispositivo. El perfil de configuración puede contener otras peticiones de registro de identidades mediante SCEP, que se ejecutarán durante la instalación del perfil.

De forma similar, cuando un certificado instalado utilizando SCEP caduca o queda invalidado por alguna otra razón, el dispositivo solicita al usuario que actualice el perfil. Cuando el usuario autoriza la petición, el dispositivo repite el proceso anterior para obtener un nuevo certificado y perfil.

Puede consultar un perfil de configuración de ejemplo de esta fase en “Ejemplo de respuesta del dispositivo (fase 4)” en la página 94.

Otros recursos

- Certificados digitales PKI para redes VPN IPsec en https://cisco.hosted.jivesoftware.com/docs/DOC-3592
- Infraestructura de clave pública (PKI) en http://en.wikipedia.org/wiki/Public_key_infrastructure
- Especificación del protocolo SCEP del IETF http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt

Encontrará información y recursos adicionales para el iPhone, el iPod touch y el iPad para empresas en los sitios www.apple.com/es/iphone/enterprise/ y www.apple.com/es/ipad/business/.

Creación y distribución de perfiles de configuración

2

Los perfiles de configuración definen cómo funcionan el iPhone, el iPod touch y el iPad con los sistemas de su empresa.

Los perfiles de configuración son archivos XML que contienen políticas de seguridad y restricciones para los dispositivos, información de configuración de redes VPN, ajustes Wi-Fi, cuentas de correo electrónico y calendario, y credenciales de autenticación que permiten la integración del iPhone, el iPod touch y el iPad en sus sistemas de empresa.

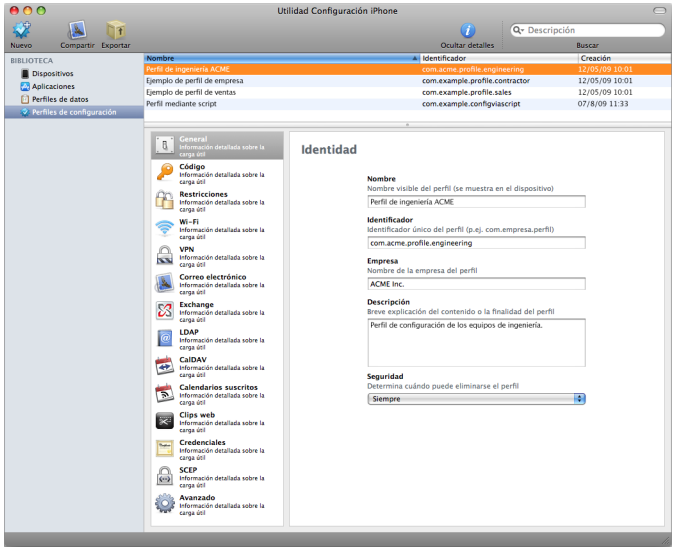
Puede instalar perfiles de configuración en los dispositivos conectados a un ordenador por USB con la Utilidad Configuración iPhone o distribuir perfiles de configuración por correo electrónico o mediante una página web. Cuando un usuario abra el archivo adjunto de correo electrónico o utilice Safari para descargar el perfil en su dispositivo, se le solicitará que inicie el proceso de instalación.

Si no quiere crear y distribuir perfiles de configuración, puede configurar los dispositivos de forma manual. En el capítulo 3 encontrará más información al respecto.

Acerca de Utilidad Configuración iPhone

La Utilidad Configuración iPhone le permite crear, encriptar e instalar fácilmente perfiles de configuración, rastrear e instalar perfiles de datos y aplicaciones autorizadas, y obtener información de los dispositivos (incluidos los registros de consola). Al ejecutar el programa de instalación de la Utilidad Configuración iPhone, esta aplicación se instala en /Aplicaciones/Utilidades en Mac OS X, o en Programas\iPhone Configuration Utility\ en Windows.

Cuando se abre la Utilidad Configuración iPhone, aparece una ventana similar a la que se muestra a continuación.



El contenido de la sección principal de la ventana cambia al seleccionar distintos ítems en la barra lateral.

La barra lateral muestra la Biblioteca, que contiene las siguientes categorías:

- *Dispositivos* muestra una lista de los iPhone e iPod touch que se han conectado al ordenador.
- *Aplicaciones* contiene las aplicaciones que se pueden instalar en los dispositivos conectados al ordenador. Es posible que para poder ejecutar una aplicación en un dispositivo se necesite un perfil de datos.
- *Perfiles de datos* incluye los perfiles que permiten utilizar el dispositivo para el desarrollo de iPhone OS, según autorización de Apple Developer Connection. Para obtener información, consulte el capítulo 5. Los perfiles de datos también permiten la ejecución en los dispositivos de aplicaciones corporativas no distribuidas por la tienda iTunes Store.

- *Perfiles de configuración* incluye los perfiles de configuración que haya creado anteriormente y le permite editar la información que haya introducido o bien crear una nueva configuración que puede enviar a un usuario o instalarla en un dispositivo conectado.

La barra lateral también muestra *Dispositivos conectados*, que contiene información acerca de los dispositivos iPhone OS que actualmente están conectados al puerto USB del ordenador. La información sobre un dispositivo conectado se añade automáticamente a la lista Dispositivos, de modo que pueda verla más adelante sin tener que volver a conectar el dispositivo. Tras conectar un dispositivo, también puede encriptar perfiles para usarlos únicamente en ese dispositivo.

Si tiene un dispositivo conectado, puede usar la Utilidad Configuración iPhone para instalar perfiles de configuración y aplicaciones en el dispositivo. Consulte "Instalación de perfiles de configuración con la Utilidad Configuración iPhone" en la página 45,"Instalación de aplicaciones con la Utilidad Configuración iPhone" en la página 72 y "Instalación de perfiles de datos con la Utilidad Configuración iPhone" en la página 71 para obtener más información al respecto.

Cuando un dispositivo está conectado, también puede ver sus registros de consola y cualquier informe de errores. Se trata de los mismos registros de dispositivo disponibles para su visualización dentro del entorno de desarrollo Xcode en Mac OS X.

Creación de perfiles de configuración

Este documento emplea los términos *perfil de configuración* y *contenido* ("payload"). Un perfil de configuración es el archivo que configura ciertos ajustes (únicos o múltiples) del iPhone, el iPod touch o el iPad. Un contenido es una colección de determinados tipos de ajustes, como por ejemplo los ajustes VPN, dentro del perfil de configuración.

Aunque puede crear un único perfil de configuración que contenga todos los contenidos que necesita para su empresa, contemple la posibilidad de crear un perfil para los certificados y otro para los ajustes, de modo que pueda actualizar y distribuir de forma separada cada tipo de información. Esto permite a los usuarios conservar los certificados ya instalados cuando instalan un nuevo perfil con ajustes VPN o de cuenta.

Muchos de los contenidos le permiten especificar nombres de usuario y contraseñas. Si omite esta información, el perfil podrá ser usado por varios usuarios, pero al instalarlo se les solicitará que introduzcan la información que falta. Si personaliza el perfil para cada usuario e incluye contraseñas, deberá distribuir el perfil en formato encuitado para proteger su contenido. Para más información, consulte "Instalación de perfiles de configuración" en la página 44.

Para crear un nuevo perfil de configuración, haga clic en el botón Nuevo de la barra de herramientas de la Utilidad Configuración iPhone. Se añaden contenidos al perfil mediante la lista de contenidos. Estos contenidos pueden editarse introduciendo y seleccionando las opciones que aparecen en el panel de edición. Los campos requeridos están marcados con una flecha roja. Para algunos ajustes, como los de Wi-Fi, puede hacer clic en el botón Añadir (+) para añadir configuraciones. Para eliminar una configuración, haga clic en el botón Eliminar (–) del panel de edición.

Para editar un contenido, seleccione el elemento adecuado en la lista de contenidos, haga clic en el botón Configurar y rellene la información, tal como se describe a continuación.

Cómo automatizar la creación de perfiles de configuración

También puede automatizar la creación de archivos de configuración mediante scripts de AppleScript en un Mac, o mediante scripts C# en Windows. Para ver los métodos admitidos y su sintaxis, haga lo siguiente:

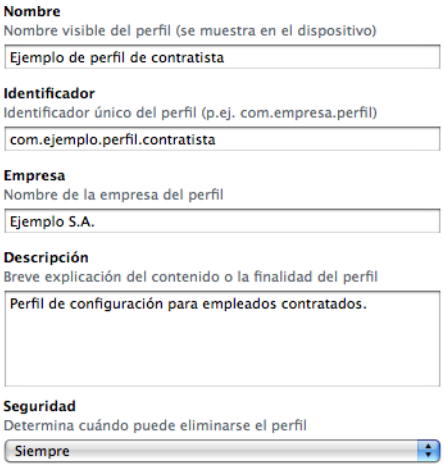
- *Mac OS X:* utilice el Editor de Scripts para abrir el diccionario AppleScript de la Utilidad Configuración iPhone.
- *Windows*: utilice Visual Studio para ver las llamadas a métodos proporcionadas por iPCUScripting.dll.

Para ejecutar un script: en Mac, use el comando Tell de AppleScript; en Windows, pase el nombre del script a la Utilidad Configuración iPhone como un parámetro de línea de comandos.

Para ver ejemplos, consulte apéndice C, "Scripts de ejemplo".

Ajustes generales

Aquí es donde se proporciona el nombre y el identificador del perfil, y se especifica si los usuarios están autorizados a eliminar el perfil una vez instalado.



El nombre especificado aparece en la lista de perfiles y se muestra en el dispositivo tras la instalación del perfil de configuración. Aunque el nombre no tiene por qué ser único, es recomendable elegir uno descriptivo que identifique el perfil.

El identificador del perfil debe designar de forma única este perfil y utilizar el formato com.*nombredelaempresa.identificador*, donde *identificador* describe el perfil. (Por ejemplo, com.miempresa.sedecentral.)

El identificador es importante porque, al instalar un perfil, este valor se compara con los perfiles ya presentes en el dispositivo. Si el identificador es único, la información del perfil se añade al dispositivo. Si el identificador coincide con un perfil ya instalado, la información del perfil reemplaza los ajustes ya presentes en el dispositivo, excepto en el caso de los ajustes de Exchange. Para modificar una cuenta Exchange, primero hay que eliminar el perfil manualmente para que los datos asociados con dicha cuenta también puedan suprimirse.

Para impedir que un usuario pueda eliminar un perfil instalado en un dispositivo, seleccione una opción en el menú local Seguridad. La opción "Con autorización" le permite especificar una contraseña de autorización que permite la eliminación del perfil en el dispositivo. Si selecciona la opción Nunca, el perfil podrá actualizarse con una nueva versión, pero no podrá eliminarse.

Ajustes de código

Utilice este contenido para ajustar políticas de dispositivo si no emplea políticas de código Exchange. Puede especificar si se necesitará un código para utilizar el dispositivo, así como determinar las características del código y la frecuencia con que debe cambiarse. Cuando se carga el perfil de configuración, se solicita de inmediato al usuario que introduzca un código que cumpla las políticas seleccionadas, pues sin este código el perfil no se puede instalar.

Si utiliza políticas de dispositivo y políticas de código Exchange, ambos grupos de políticas se fusionan y se aplican los ajustes más estrictos. Para obtener información acerca de las políticas de Exchange ActiveSync compatibles, consulte "Microsoft Exchange ActiveSync" en la página 9.

Están disponibles las siguientes políticas:

- *Solicitar código en el dispositivo:* requiere que el usuario introduzca un código antes de utilizar el dispositivo. Sin este código, cualquier persona que tenga en su poder el dispositivo podrá acceder a todas sus funciones y datos.
- *Permitir valor simple:* permite al usuario utilizar caracteres secuenciales o repetitivos en sus códigos. Por ejemplo, permitiría los códigos "3333" o "DEFG".
- *Requerir valor alfanumérico:* requiere que el código contenga por lo menos un carácter alfanumérico.
- *Longitud mínima del código:* especifica el número mínimo de caracteres que puede contener un código.
- *Numero mínimo de caracteres complejos:* el número de caracteres no alfanuméricos (como $, & y !) que el código debe contener.
- *Periodo máximo de validez del código (en días):* requiere que el usuario cambie su código cuando transcurre el tiempo especificado.
- *Bloqueo automático (en minutos):* si no se utiliza durante este periodo, el dispositivo se bloquea automáticamente. Se desbloquea introduciendo el código.
- *Historial de códigos:* no se aceptará ningún código nuevo que se haya usado anteriormente. Puede establecer el número de códigos anteriores que se guardan en este historial.
- *Periodo de gracia para el bloqueo del dispositivo:* determina el tiempo durante el cual el dispositivo puede desbloquearse de nuevo tras su uso sin volver a solicitar la introducción del código.

- *Número máximo de intentos fallidos:* determina cuántos intentos fallidos de introducción del código puede haber antes de que el dispositivo se borre. Si no modifica este ajuste, después de seis intentos fallidos, el dispositivo impone un periodo de tiempo antes de poder volver a intentarlo. Este periodo aumenta con cada intento fallido. Tras el undécimo fallo, todos los datos y ajustes del dispositivo se borran de forma segura. El tiempo de retardo del código siempre comienza después del sexto intento; si ajusta este valor a 6 o menos, no habrá retardo y el dispositivo se borrará cuando se exceda el número de intentos.

Ajustes de restricciones

Utilice este contenido para especificar qué funciones del dispositivo el usuario está autorizado a utilizar.

- *Permitir contenido explícito:* cuando esta opción está desactivada, las canciones o vídeos con contenidos para adultos que se hayan comprado en la tienda iTunes Store permanecerán ocultos. Son los propios proveedores de los contenidos (por ejemplo, los propios sellos discográficos) los que los marcan como explícitos cuando los ponen a la venta a través de la iTunes Store.
- *Permitir el uso de Safari:* cuando esta opción está desactivada, el navegador web Safari está desactivado y su icono desaparece de la pantalla de inicio. Además, los usuarios no pueden abrir clips web.
- *Permitir el uso de YouTube:* cuando esta opción está desactivada, la aplicación YouTube está desactivada y su icono desaparece de la pantalla de inicio.
- *Permitir el uso de iTunes Music Store:* cuando esta opción está desactivada, la tienda iTunes Music Store está desactivada y su icono desaparece de la pantalla de inicio. Los usuarios no pueden comprar, descargar ni escuchar fragmentos de los contenidos de la tienda.
- *Permitir instalar aplicaciones:* cuando esta opción está desactivada, la tienda App Store está desactivada y su icono desaparece de la pantalla de inicio. Los usuarios tampoco pueden instalar o actualizar sus aplicaciones.
- *Permitir usar la cámara:* cuando esta opción está desactivada, la cámara está completamente desactivada y su icono desaparece de la pantalla de inicio. Los usuarios no pueden hacer fotos.
- *Permitir captura de pantalla:* cuando esta opción está desactivada, los usuarios no pueden guardar capturas de pantalla.

Ajustes Wi-Fi

Utilice este contenido para configurar el modo en que el dispositivo se conecta a su red inalámbrica. Puede añadir varias configuraciones de red haciendo clic en el botón Añadir (+) del panel de edición.

Estos ajustes deben especificarse y deben coincidir con los requisitos de la red para poder iniciar una conexión.

- *Identificador del conjunto de servicios:* introduzca el SSID de la red inalámbrica a la que desea conectarse.
- *Red oculta:* especifica si la red transmite su identidad.
- *Tipo de seguridad:* seleccione un método de autenticación para la red. Las siguientes opciones están disponibles para redes personales y de empresa.
  - *Ninguna:* la red no utiliza autenticación.
  - *WEP:* la red solo utiliza autenticación WEP.
  - *WPA/WPA 2:* la red solo utiliza autenticación WPA.
  - *Cualquiera:* el dispositivo utiliza autenticación WEP o WPA al conectarse a la red, pero no se conecta a redes no autenticadas.
- *Contraseña:* introduzca la contraseña para acceder a la red inalámbrica. Si deja este campo en blanco, se le solicitará al usuario que la introduzca.

Ajustes para redes corporativas

En esta sección se especifican los ajustes para conectarse a redes corporativas. Estos ajustes solo aparecen si selecciona un ajuste Empresa en el menú local "Tipo de seguridad".

En la pestaña Protocolos se especifican los métodos EAP que se utilizan para la autenticación y se configuran los ajustes EAP-FAST de credencial de acceso protegido.

En la pestaña Autenticación se especifican los ajustes de inicio de sesión, como el nombre de usuario y los protocolos de autenticación. Si ha instalado una identidad en la sección Credenciales, puede seleccionarla con el menú local "Certificado de identidad".

En la pestaña Confianza se especifica qué certificados deberían considerarse de confianza con el propósito de validar el servidor de autenticación para la conexión Wi-Fi. La lista "Certificados de confianza" muestra los certificados añadidos mediante la pestaña Credenciales y permite seleccionar cuáles son considerados de confianza. Añada el nombre de los servidores de autenticación de confianza a la lista "Nombres de certificados de servidor de confianza". Puede especificar un servidor particular, como *servidor.miempresa.com*, o un nombre parcial como **.miempresa.com*.

La opción "Permitir excepciones de confianza" permite a los usuarios confiar en un servidor cuando no es posible establecer la cadena de confianza. Para evitar estos avisos y permitir la conexión solo a los servicios de confianza, desactive esta opción e incluya todos los certificados necesarios en un perfil.

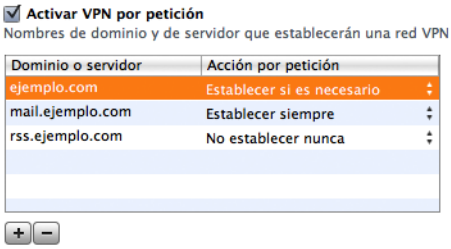
Ajustes VPN

Utilice este contenido para introducir los ajustes VPN para conectarse a su red. Puede añadir múltiples conjuntos de conexiones VPN haciendo clic en el botón Añadir (+).

Para obtener información sobre los protocolos VPN y los métodos de autenticación compatibles, consulte "VPN" en la página 12. Las opciones disponibles varían dependiendo del protocolo y el método de autenticación que seleccione.

VPN por petición

En configuraciones IPsec con certificado, puede activar la función VPN por petición para que se establezca automáticamente una conexión VPN al acceder a ciertos dominios.



VPN por petición ofrece las siguientes opciones:

Ajuste	Descripción
Siempre	Inicia una conexión VPN para cualquier dirección que coincida con el dominio especificado.
Nunca	No inicia una conexión VPN con las direcciones que pertenezcan al dominio especificado, pero si ya hay una VPN activa, es posible que se utilice.
Establecer si es necesario	Inicia una conexión VPN con las direcciones que pertenecen al dominio especificado solamente tras una búsqueda de DNS fallida.

La acción se aplica a todas las direcciones coincidentes. Las direcciones se comparan por coincidencia de cadenas de caracteres simple, comenzando por el final y yendo hacia atrás. La dirección ".ejemplo.org" coincide con "soporte.ejemplo.org" y con "ventas.ejemplo.org" pero no con "www.primer-ejemplo.org". Sin embargo, si especifica el dominio de coincidencia como "ejemplo.org" (fíjese en que no hay un punto al principio), coincidirá con "www.primer-ejemplo.org" y con todas las demás.

Tenga en cuenta que las conexiones LDAP no iniciarán ninguna conexión VPN; si otra aplicación (por ejemplo, Safari) no ha establecido la conexión VPN, la búsqueda LDAP dará un error.

Proxy VPN

El iPhone admite configuraciones de proxy VPN manuales así como configuraciones de proxy automáticas mediante PAC o WPAD. Para especificar un proxy VPN, seleccione una opción en el menú local "Configuración de proxy".

Para configuraciones de proxy automáticas mediante PAC, seleccione Automático en el menú local e introduzca la URL del archivo PAC. Para obtener información acerca de las funciones PAC y el formato de archivo, consulte "Otros recursos" en la página 61.

Para configuraciones WPAD (Web Proxy Autodiscovery), seleccione Automático en el menú local. Deje en blanco el campo "URL del servidor proxy"; el iPhone solicitará el archivo WPAD mediante DHCP y DNS. Para obtener información acerca de WPAD, consulte "Otros recursos" en la página 61

Ajustes de correo electrónico

Utilice este contenido para configurar cuentas de correo electrónico POP o IMAP del usuario. Si va a añadir una cuenta de Exchange, consulte el apartado "Ajustes de Exchange", a continuación.

El usuario puede modificar algunos de los ajustes proporcionados con el perfil, como el nombre de cuenta, la contraseña y los servidores SMTP alternativos. Si se omite cualquiera de estos datos en el perfil, se solicitará a los usuarios que los introduzcan cuando accedan a la cuenta.

Puede añadir múltiples cuentas de correo electrónico haciendo clic en el botón Añadir (+).

Ajustes de Exchange

Utilice este contenido para introducir los ajustes del usuario para su servidor Exchange. Puede crear un perfil para un usuario concreto especificando el nombre de usuario, el nombre del servidor y la dirección de correo electrónico, o puede proporcionar solo el nombre del servidor (en ese caso, se solicitará al usuario que rellene los demás valores al instalar el perfil).

Si especifica en el perfil el nombre de usuario, el nombre de servidor y el ajuste SSL, el usuario no podrá cambiar estos ajustes en el dispositivo.

Solo es posible configurar una cuenta Exchange por dispositivo. Las demás cuentas de correo electrónico, incluidas las cuentas Exchange por IMAP, no se ven afectadas al añadir una cuenta Exchange. Las cuentas Exchange que se añaden mediante un perfil se eliminan cuando se borra el perfil (no pueden eliminarse de otro modo).

Por omisión, Exchange sincroniza contactos, calendarios y correo electrónico. El usuario puede cambiar estos ajustes en el dispositivo (incluido el número de días que abarcan los datos que se sincronizarán), en Ajustes > Cuentas.

Si selecciona la opción "Usar SSL", debe asegurarse de añadir mediante el panel Credenciales los certificados necesarios para autenticar la conexión.

Para proporcionar un certificado que identifique al usuario en el servidor Exchange ActiveSync, haga clic en el botón Añadir (+) y, a continuación, seleccione un certificado de identidad del llavero de Mac OS X o del almacén de certificados de Windows. Después de añadir un certificado, puede especificar el nombre de credencial de autenticación, si es necesario para su configuración de ActiveSync. También puede incluir la contraseña del certificado en el perfil de configuración. Si no proporciona la contraseña, se le pedirá al usuario que la introduzca cuando se instale el perfil.

Ajustes LDAP

Utilice este contenido para introducir los ajustes para conectarse a un directorio LDAPv3. Puede especificar varias bases de búsqueda para cada directorio y puede configurar varias conexiones de directorio haciendo clic en el botón Añadir (+).

Si selecciona la opción "Usar SSL", debe asegurarse de añadir mediante el panel Credenciales los certificados necesarios para autenticar la conexión.

Ajustes CalDAV

Utilice este contenido para proporcionar los ajustes de las cuentas para conectarse a un servidor de calendarios compatible con CalDAV. Estas cuentas se añadirán al dispositivo; como sucede con las cuentas Exchange, al instalar el perfil el usuario debe introducir de forma manual la información omitida (como la contraseña).

Si selecciona la opción "Usar SSL", debe asegurarse de añadir mediante el panel Credenciales los certificados necesarios para autenticar la conexión.

Puede configurar varias cuentas haciendo clic en el botón Añadir (+).

Ajustes de calendarios suscritos

Use este contenido para añadir suscripciones a calendarios de solo lectura a la aplicación Calendario del dispositivo. Puede configurar varias suscripciones haciendo clic en el botón Añadir (+).

En www.apple.com/es/downloads/macosx/calendars/ hay una lista de calendarios públicos a los que puede suscribirse.

Si selecciona la opción "Usar SSL", debe asegurarse de añadir mediante el panel Credenciales los certificados necesarios para autenticar la conexión.

Ajustes de clips web

Utilice este contenido para añadir clips web a la pantalla de inicio del dispositivo del usuario. Los clips web proporcionan un rápido acceso a páginas web favoritas.

Asegúrese de que la URL que introduzca incluye el prefijo http:// o https://, ya que es necesario para que el clip web funcione correctamente. Por ejemplo, para añadir la versión en línea del *Manual del usuario del iPhone* a la pantalla de inicio, especifique la URL del clip web: http://help.apple.com/iphone/

Para añadir un icono personalizado, seleccione un archivo gráfico en formato gif, jpeg o png y con un tamaño de 59 x 60 píxeles. El tamaño de la imagen se ajustará automáticamente, recortándola y convirtiéndola a formato png si es necesario.

Ajustes de credenciales

Utilice este contenido para añadir certificados e identidades al dispositivo. Para obtener información sobre los formatos admitidos, consulte "Certificados e identidades" en la página 13.

Cuando instale credenciales, instale también los certificados intermedios que son necesarios para establecer una cadena a un certificado de confianza que esté en el dispositivo. Para ver una lista de los sistemas preinstalados, consulte el siguiente artículo de soporte técnico de Apple: http://support.apple.com/kb/HT2185.

Si va a añadir una identificación para usarla con Microsoft Exchange, utilice en su lugar el contenido Exchange. Consulte "Ajustes de Exchange" en la página 40.

Para añadir credenciales en Mac OS X:

1. Haga clic en el botón Añadir (+).
2. En el cuadro de diálogo de selección de archivos que aparecerá, seleccione un archivo PKCS1 o PKSC12 y haga clic en Abrir.

   Si el certificado o la identidad que desea instalar está en su llavero, utilice Acceso a Llaveros para exportarlo/a en formato .p12. La aplicación Acceso a Llaveros está instalada en /Aplicaciones/Utilidades. Para más información, puede consultar la Ayuda Acceso a Llaveros, disponible en el menú Ayuda de Acceso a Llaveros.

   Para añadir varias credenciales al perfil de configuración, haga clic de nuevo en el botón Añadir (+).

Para añadir credenciales en Windows:

1. Haga clic en el botón Añadir (+).
2. Seleccione en el almacén de certificados de Windows la credencial que desee instalar.

   Si la credencial no está disponible en su almacén de certificados personal, deberá añadirla y la clave privada deberá estar marcada como exportable (este es uno de los pasos que ofrece el asistente de importación de certificados). Para añadir certificados raíz se requiere acceso de administrador al ordenador, y el certificado debe añadirse al almacén personal.

Si está utilizando varios perfiles de configuración, asegúrese de que no estén duplicados. No se pueden instalar distintas copias del mismo certificado.

En vez de instalar certificados empleando un perfil de configuración, puede permitir al usuario utilizar Safari para descargar los certificados directamente en su dispositivo desde una página web. También es posible enviar los certificados a los usuarios mediante correo electrónico. Consulte "Instalación de identidades y certificados raíz" en la página 60 para obtener más información. También puede utilizar los ajustes SCEP, a continuación, para determinar cómo obtiene el dispositivo los certificados de forma remota cuando el perfil está instalado.

Ajustes SCEP

Con el contenido SCEP puede especificar los ajustes que permiten al dispositivo obtener los certificados de una CA mediante el protocolo SCEP (Simple Certificate Enrollment Protocol).

Ajuste	Descripción
URL	La dirección del servidor SCEP.
Nombre	Cualquier secuencia de caracteres reconocible por parte de la autoridad de certificación (se puede utilizar para distinguir distintas versiones, por ejemplo).
Asunto	La representación de un nombre X.500 expresado como una matriz de OID y valor. Por ejemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se traduciría de la siguiente manera: [[["C","US"]], [["O","Apple Inc."]], ..., [["1.2.5.3","bar"]]]
Contraseña de comprobación	Secreto precompartido que el servidor SCEP puede utilizar para identificar la solicitud o el usuario.
Tamaño de la clave y Uso	Seleccione un tamaño de clave y, mediante las opciones situadas bajo este campo, el uso aceptable de dicha clave.
Huella digital	Si su autoridad de certificación (CA) utiliza HTTP, use este campo para proporcionar la huella digital del certificado de la CA que el dispositivo utilizará para confirmar la autenticidad de la respuesta de la CA durante el proceso de registro. Puede introducir una huella digital SHA1 o MD5, o seleccionar un certificado para importar su firma.

Para obtener más información acerca de cómo obtiene el iPhone los certificados de forma inalámbrica, consulte "Registro y configuración remotos" en la página 25

Ajustes avanzados

El contenido Avanzado permite cambiar los ajustes de nombre de punto de acceso (APN) y de proxy de la red de telefonía móvil. Estos ajustes definen el modo en que el dispositivo se conecta a la red del operador. Solo debe cambiar estos ajustes si se lo indica de forma expresa un experto en la red del operador. Si estos ajustes son incorrectos, el dispositivo no podrá acceder a datos mediante la red de telefonía móvil. Para deshacer un cambio involuntario en estos ajustes, elimine el perfil del dispositivo. Apple le recomienda que defina los ajustes APN en un perfil de configuración aparte de los otros ajustes de empresa, ya que los perfiles que especifican la información APN deben estar firmados por el proveedor del servicio de telefonía móvil.

El sistema iPhone OS admite nombres de usuario APN de hasta 20 caracteres y contraseñas de hasta 32 caracteres.

Edición de perfiles de configuración

En la Utilidad Configuración iPhone, seleccione un perfil en la lista de perfiles de configuración y, a continuación, emplee la lista de contenidos y los paneles de edición para realizar los cambios. También puede importar un perfil seleccionando Archivo > "Añadir a la Biblioteca" y eligiendo después un archivo .mobileconfig. Si los paneles de ajustes no están visibles, seleccione Visualización > Mostrar detalles.

El dispositivo utiliza el campo Identificador del contenido General para determinar si un perfil es nuevo o si se trata de una actualización de otro existente. Si quiere que el perfil actualizado reemplace a uno que los usuarios ya hayan instalado, no cambie el identificador.

Instalación de perfiles de datos y aplicaciones

La Utilidad Configuración iPhone puede instalar aplicaciones y perfiles de datos de distribución en los dispositivos que estén conectados al ordenador. Para más información, consulte el capítulo 5, "Distribución de aplicaciones", en la página 69.

Instalación de perfiles de configuración

Después de crear un perfil, puede conectar un dispositivo e instalarlo mediante la Utilidad Configuración iPhone.

También puede distribuirlo a los usuarios por correo electrónico o colgándolo en un sitio web. Cuando los usuarios empleen su dispositivo para abrir un mensaje de correo electrónico o descargar el perfil de la página web, se les solicitará que comiencen el proceso de instalación.

Instalación de perfiles de configuración con la Utilidad Configuración iPhone

Puede instalar perfiles de configuración directamente en un dispositivo que se haya actualizado a la versión 3.0 o posterior de iPhone OS y que esté conectado físicamente a su ordenador. También puede emplear la Utilidad Configuración iPhone para eliminar los perfiles ya instalados.

Para instalar un perfil de configuración:

1. Conecte el dispositivo al ordenador mediante un cable USB.

   Tras unos instantes, el dispositivo aparecerá en la lista Dispositivos de la Utilidad Configuración iPhone.

2. Seleccione el dispositivo y, a continuación, haga clic en la pestaña "Perfiles de configuración".

3. Elija un perfil de configuración de la lista y haga clic en Instalar.

4. En el dispositivo, pulse Instalar para instalar el perfil.

   Al instalar el perfil de configuración directamente en el dispositivo a través de una conexión USB, el perfil se firma y se encripta de forma automática antes de transferirse al dispositivo.

Distribución de perfiles de configuración mediante correo electrónico

Los perfiles de configuración pueden distribuirse por correo electrónico. Para instalar el perfil, los usuarios deben recibir el mensaje en su dispositivo y pulsar en el archivo adjunto.

Para enviar un perfil de configuración por correo electrónico:

1. Haga clic en el botón Compartir de la barra de herramientas de la Utilidad Configuración iPhone.

   En el cuadro de diálogo que aparecerá, seleccione una opción de seguridad:

   a. *Ninguna:* se crea un archivo .mobileconfig sin encriptación, que puede instalarse en cualquier dispositivo. Parte de su contenido se ofusca para impedir la obtención casual de información si se examina el archivo.

   b. *Firmar perfil de configuración:* el archivo .mobileconfig se firma y, si sufre alguna alteración, el dispositivo no lo instalará. Algunos campos se ofuscan para impedir la obtención casual de información si se examina el archivo. Una vez instalado, el perfil solo puede actualizarse con un perfil que tenga el mismo identificador y esté firmado por la misma copia de la Utilidad Configuración iPhone.

c *Firmar y encriptar el perfil:* firma el perfil para que no se pueda modificar y encripta todo su contenido para que no se pueda examinar y solo se pueda instalar en un dispositivo determinado. Se recomienda utilizar esta opción si el perfil contiene contraseñas. Se creará un archivo .mobileconfig distinto por cada uno de los dispositivos que seleccione en la lista de dispositivos. Si un dispositivo no aparece en la lista, puede deberse a que o bien no se ha conectado anteriormente al ordenador para que pueda obtenerse la clave de encriptación o bien no se ha actualizado a la versión 3.0 o posterior de iPhone OS.

2 Haga clic en Compartir y se abrirá un nuevo mensaje de Mail (Mac OS X) o de Outlook (Windows) con los perfiles añadidos como archivos adjuntos sin comprimir. Los archivos no deben estar comprimidos para que el dispositivo reconozca e instale el perfil.

Distribución de perfiles de configuración en Internet

Los perfiles de configuración pueden distribuirse a través de un sitio web. Los usuarios los instalan descargándoselos en su dispositivo con Safari. Para distribuir fácilmente la URL a los usuarios, puede enviarla en un mensaje SMS.

Para exportar un perfil de configuración:

1 Haga clic en el botón Exportar de la barra de herramientas de la Utilidad Configuración iPhone.

En el cuadro de diálogo que aparecerá, seleccione una opción de seguridad:

a *Ninguna:* se crea un archivo .mobileconfig sin encriptación, que puede instalarse en cualquier dispositivo. Parte de su contenido se ofusca para impedir la obtención casual de información si se examina el archivo, pero debe asegurarse de que, al colgar el archivo en el sitio web, solo puedan acceder a él usuarios autorizados.

b *Firmar perfil de configuración:* el archivo .mobileconfig se firma y, si sufre alguna alteración, el dispositivo no lo instalará. Una vez instalado, el perfil solo puede actualizarse con un perfil que tenga el mismo identificador y esté firmado por la misma copia de la Utilidad Configuración iPhone. Parte de la información contenida en el perfil se ofusca para impedir la obtención casual de información si se examina el archivo, pero debe asegurarse de que, al colgar el archivo en el sitio web, solo puedan acceder a él usuarios autorizados.

c *Firmar y encriptar el perfil:* firma el perfil para que no se pueda modificar y encripta todo su contenido para que no se pueda examinar y solo se pueda instalar en un dispositivo determinado. Se creará un archivo .mobileconfig distinto por cada uno de los dispositivos que seleccione en la lista de dispositivos.

2 Haga clic en Exportar y, a continuación, seleccione la ubicación en la que desee guardar los archivos .mobileconfig.

Los archivos están listos para colgarse en un sitio web. No comprima el archivo .mobileconfig ni cambie su extensión, pues de lo contrario el dispositivo no reconocerá ni instalará el perfil.

Instalación de perfiles de configuración descargados

Debe proporcionar a los usuarios la dirección desde la que descargar los perfiles en sus dispositivos, o enviar los perfiles a una cuenta de correo electrónico a la que los usuarios puedan acceder desde los dispositivos, antes de configurar estos con la información concreta de la empresa.

Cuando un usuario descarga el perfil de la página web en cuestión, o abre con Mail el archivo adjunto que lo contiene, el dispositivo reconoce la extensión .mobileconfig como un perfil y, cuando el usuario pulsa Instalar, inicia la instalación.

Durante la instalación, se solicita al usuario que introduzca cualquier información necesaria, como las contraseñas que no estaban especificadas en el perfil, y otros datos requeridos por los ajustes especificados.

El dispositivo también recupera las políticas Exchange ActiveSync del servidor, y en cada conexión posterior actualizará las políticas en caso de que hayan variado. Si el dispositivo o las políticas de Exchange ActiveSync exigen un ajuste de código, el usuario debe introducir un código conforme a estas políticas para completar la instalación.

Además, se solicitará al usuario que introduzca cualquier contraseña necesaria para utilizar los certificados incluidos en el perfil.

Si la instalación no se completa con éxito, quizá debido a que no se pudo conectar con el servidor Exchange o a que el usuario canceló el proceso, no se conservará ninguna información introducida por el usuario.

El usuario puede indicar cuántos días de mensajes se sincronizarán con el dispositivo y qué buzones de correo además del buzón de entrada se sincronizarán. Por omisión, se sincronizan los mensajes de los últimos tres días y todos los buzones. El usuario puede cambiar estos ajustes en Ajustes > Mail, contactos, calendarios > *Nombre de cuenta Exchange*.

Eliminación y actualización de perfiles de configuración

Las actualizaciones de perfiles de configuración no se transmiten de forma automática a los usuarios. Debe distribuirlas a los usuarios para que ellos se las instalen en sus dispositivos. Mientras el identificador del perfil coincida y, si el perfil esté firmado, lo haya firmado la misma copia de la Utilidad Configuración iPhone, el nuevo perfil reemplazará al del dispositivo.

Los ajustes impuestos por un perfil de configuración no pueden cambiarse en el dispositivo. Para cambiar un ajuste se debe instalar un perfil actualizado. Si el perfil está firmado, solo podrá ser reemplazado por uno que haya sido firmado por la misma copia de la Utilidad Configuración iPhone. Además, el identificador debe coincidir en ambos perfiles para que el perfil actualizado pueda reemplazar el anterior. Para obtener más información acerca del identificador, consulte "Ajustes generales" en la página 35.

Importante: Al eliminar un perfil de configuración, se borran las políticas y todos los datos de la cuenta Exchange almacenados en el dispositivo, así como los ajustes VPN, los certificados y otra información asociada al perfil (incluidos los mensajes de correo electrónico).

Si en los ajustes generales del perfil se especifica que el usuario no lo puede eliminar, el botón Eliminar no aparecerá. Si, en cambio, se permite la eliminación del perfil mediante una contraseña autorizada, se solicitará al usuario que la introduzca después de pulsar Eliminar. Para obtener más información acerca de los ajustes de seguridad del perfil, consulte “Ajustes generales” en la página 35.

Configuración manual de dispositivos

3

En este capítulo se describe cómo configurar el iPhone, el iPod touch y el iPad de forma manual.

Si no se proporcionan perfiles de configuración automáticos, los usuarios podrán configurar sus dispositivos de forma manual. Algunos ajustes, como las políticas de código, solo pueden ajustarse mediante un perfil de configuración.

Ajustes VPN

Para cambiar los ajustes VPN, vaya a Ajustes > General > Red > VPN.

Al configurar los ajustes VPN, el dispositivo solicitará que se introduzca información según la respuesta que obtenga del servidor VPN. Por ejemplo, solicitará un token RSA SecurID si el servidor lo requiere.

No se puede configurar una conexión VPN basada en certificado si en el dispositivo no están instalados los certificados apropiados. Consulte "Instalación de identidades y certificados raíz" en la página 60 para obtener más información.

No es posible configurar la función de VPN por petición en el dispositivo. Para hacerlo, debe utilizar un perfil de configuración. consulte el apartado "VPN por petición" en la página 39.

Configuración de proxy VPN

También es posible definir un proxy VPN para todas las configuraciones. Para configurar un único proxy para todas las conexiones, pulse Manual e introduzca, si es necesario, la dirección, el puerto y la autenticación. Para cargar un archivo de configuración automática de proxy en el dispositivo, pulse Automát. y especifique la URL del archivo PACS. Para especificar una configuración de proxy automática mediante WPAD, pulse Automát. El dispositivo consultará a DHCP y DNS los ajustes de WPAD. Consulte el apartado "Otros recursos" al final de este capítulo para ver ejemplos de archivos PACS y otros recursos.

Ajustes de Cisco IPsec

Cuando se configura de forma manual el dispositivo para una VPN con Cisco IPsec, aparecerá una pantalla similar a esta:

Utilice esta tabla para identificar los ajustes y la información a introducir:

Campo	Descripción
Descripción	Un título descriptivo que identifica este grupo de ajustes.
Servidor	El nombre DNS o dirección IP del servidor VPN al que quiere conectarse.
Cuenta	El nombre de usuario de la cuenta de inicio de sesión VPN del usuario. No introduzca el nombre del grupo en este campo.
Contraseña	La contraseña de la cuenta de inicio de sesión VPN del usuario. Déjela en blanco para la autenticación mediante RSA SecurID y CryptoCard, o si desea que el usuario introduzca la contraseña de forma manual en cada intento de conexión.
Usar certificado	Solo estará disponible si hay instalada una identidad .p12 o .pfx que contenga un certificado preparado para el acceso remoto *y* la clave privada del certificado. Cuando la opción "Usar certificado" está activada, los campos "Nombre grupo" y "Secreto compartido" quedan reemplazados por un campo Identificar que permite elegir entre una lista de identidades instaladas compatibles con VPN.
Nombre grupo	El nombre del grupo al que el usuario pertenece, tal y como lo define el servidor VPN.
Secreto	El secreto compartido del grupo. Es el mismo para todos los miembros del grupo asignado al usuario. La contraseña del usuario es *No* y debe especificarse para iniciar una conexión.

Ajustes PPTP

Cuando se configura de forma manual el dispositivo para una VPN PPTP, aparece una pantalla similar a esta:

Utilice esta tabla para identificar los ajustes y la información a introducir:

Campo	Descripción
Descripción	Un título descriptivo que identifica este grupo de ajustes.
Servidor	El nombre DNS o dirección IP del servidor VPN al que quiere conectarse.
Cuenta	El nombre de usuario de la cuenta de inicio de sesión VPN del usuario.
RSA SecurID	Si se utiliza un token RSA SecurID, active esta opción para ocultar el campo Contraseña.
Contraseña	La contraseña de la cuenta de inicio de sesión VPN del usuario.
Nivel de encriptación	El valor por omisión es Auto, que selecciona el máximo nivel de encriptación disponible, en este orden: 128 bits, 40 bits, Ninguna. El máximo es 128 bits. La opción Ninguna desactiva la encriptación.
Enviar todo el tráfico	El valor por omisión es Sí. Con esta opción, se envía todo el tráfico de red por el enlace VPN. Desactívela para permitir el túnel dividido, que dirige al servidor solo el tráfico destinado a servidores dentro de la VPN. El resto se dirige directamente a Internet.

Ajustes L2TP

Cuando se configura el dispositivo de forma manual para una VPN L2TP, aparece una pantalla similar a esta:

Utilice esta tabla para identificar los ajustes y la información a introducir:

Campo	Descripción
Descripción	Un título descriptivo que identifica este grupo de ajustes.
Servidor	El nombre DNS o dirección IP del servidor VPN al que quiere conectarse.
Cuenta	El nombre de usuario de la cuenta de inicio de sesión VPN del usuario.
Contraseña	La contraseña de la cuenta de inicio de sesión VPN del usuario.
Secreto	El secreto compartido (clave precompartida) para la cuenta L2TP. Es el mismo para todos los usuarios de LT2P.
Enviar todo el tráfico	El valor por omisión es Sí. Con esta opción, se envía todo el tráfico de red por el enlace VPN. Desactívela para permitir el túnel dividido, que dirige al servidor solo el tráfico destinado a servidores dentro de la VPN. El resto se dirige directamente a Internet.

Ajustes Wi-Fi

Para cambiar los ajustes Wi-Fi, vaya a Ajustes > General > Red > Wi-Fi. Si la red que está añadiendo se halla dentro del radio de acción, selecciónela en la lista de redes disponibles. Si no es así, pulse Otra.

Asegúrese de que la infraestructura de red utilice una autenticación y una encriptación compatibles con el iPhone y el iPod touch. Para conocer las especificaciones, consulte "Seguridad de red" en la página 12. Para obtener información acerca de la instalación de certificados de autenticación, consulte "Instalación de identidades y certificados raíz" en la página 60.

Ajustes de Exchange

Solo es posible configurar una cuenta Exchange por dispositivo. Para añadir una cuenta Exchange, vaya a Ajustes > "Mail, contactos, calendarios" y, a continuación, pulse "Añadir cuenta". En la pantalla "Añadir cuenta", pulse "Microsoft Exchange".

Al configurar de forma manual el dispositivo para Exchange, utilice esta tabla para identificar los ajustes y la información a introducir:

Campo	Descripción
Correo	La dirección completa de correo electrónico del usuario.
Dominio	El dominio de la cuenta Exchange del usuario.
Nombre de usuario	El nombre de usuario de la cuenta Exchange.
Contraseña	La contraseña de la cuenta Exchange del usuario.
Descripción	Un título descriptivo que identifica a esta cuenta.

El iPhone, el iPod touch y el iPad son compatibles con el servicio Autodiscover de Microsoft, que utiliza su nombre de usuario y contraseña para determinar la dirección del servidor Exchange frontal. Si no es posible determinar la dirección del servidor, se le solicitará que la introduzca.

Si su servidor Exchange escucha conexiones en un puerto diferente del 443, especifique el número de puerto en el campo Servidor utilizando el formato *exchange.ejemplo.com:númerodepuerto*.

Tras configurar correctamente la cuenta Exchange, se implementan las políticas de código del servidor. Si el código actual del usuario no cumple con las políticas Exchange ActiveSync, se solicitará al usuario que cambie o ajuste el código. El dispositivo no se comunicará con el servidor Exchange hasta que el usuario configure un código correcto.

A continuación, el dispositivo ofrece sincronizarse inmediatamente con el servidor Exchange. Si decide no sincronizar en este momento, puede activar más adelante la sincronización de calendarios y contactos en Ajustes > Mail, contactos, calendarios. Por omisión, Exchange ActiveSync transmite los nuevos datos al dispositivo en cuanto llegan al servidor. Si prefiere obtener nuevos datos de forma programada o bien solo de forma manual, utilice Ajustes > Mail, contactos, calendarios > "Obtener datos" para cambiar los ajustes.

Para cambiar los días de volumen de mensajes de correo electrónico que se sincronizarán con el dispositivo, vaya a Ajustes > "Mail, contactos, calendarios" y seleccione la cuenta de Exchange. También puede elegir qué carpetas, además del buzón de entrada, deben incluirse en la entrega de correo electrónico push.

Para cambiar los ajustes de los datos de calendario, vaya a Ajustes > Mail, contactos, calendarios > Sincronizar.

Ajustes LDAP

El iPhone, el iPod touch y el iPad pueden buscar información de contacto en los servidores de directorio LDAP. Para añadir un servidor LDAP, vaya a Ajustes > Mail, contactos, calendarios > Añadir cuenta > Otras. A continuación, pulse Añadir cuenta LDAP.

Introduzca la dirección del servidor LDAP y, si es necesario, el nombre de usuario y contraseña. A continuación, pulse Siguiente. Si es posible establecer conexión con el servidor y este proporciona ajustes de búsqueda por omisión al dispositivo, se utilizarán dichos ajustes.

Se admiten los ajustes de Alcance de la búsqueda siguientes:

Ajuste de Alcance de la búsqueda	Descripción
Base	Busca sólo en el objeto base.
Un nivel	Busca objetos un nivel por debajo del objeto base, pero no en el propio objeto base.
Subdirectorio	Busca en el objeto base y en todo el árbol de objetos que provienen de él.

Puede definir diversos conjuntos de ajustes de búsqueda para cada servidor.

Ajustes CalDAV

El iPhone, el iPod touch y el iPad funcionan con servidores de calendario CalDAV que proporcionan calendarios y agendas de grupo. Para añadir un servidor CalDAV, vaya a Ajustes > Mail, contactos, calendarios > Añadir cuenta > Otras. A continuación, pulse Añadir cuenta CalDAV.

Introduzca la dirección del servidor CalDAV y, si es necesario, el nombre de usuario y contraseña. A continuación, pulse Siguiente. Tras establecer contacto con el servidor, aparecerán campos adicionales donde podrá definir otras opciones.

Ajustes de suscripción a calendarios

Puede añadir calendarios de solo lectura, como los de planificaciones de proyecto o de días festivos. Para añadir un calendario, vaya a Ajustes > Mail, contactos, calendarios > Añadir cuenta > Otras y, a continuación, pulse Añadir calendario suscrito.

Introduzca la URL de un archivo iCalendar (.ics) y, si es necesario, el nombre de usuario y contraseña correspondientes. A continuación, pulse Guardar. También puede especificar si las alarmas definidas en el calendario deben eliminarse al añadir el calendario al dispositivo.

Además de añadir suscripciones de calendario de forma manual, también puede enviar a los usuarios una URL webcal:// (o un enlace HTTP:// a un archivo .ics) y, cuando el usuario pulse el enlace, el dispositivo le ofrecerá la posibilidad de añadirlo como calendario suscrito.

Instalación de identidades y certificados raíz

Si no distribuye certificados mediante perfiles, el usuario puede instalarlos de forma manual utilizando el dispositivo para descargarlos desde una página web, o abriendo un archivo adjunto en un mensaje de correo electrónico. El dispositivo reconoce los certificados con los siguientes tipos MIME y extensiones de archivo:

- application/x-pkcs12, .p12, .pfx
- application/x-x509-ca-cert, .cer, .crt, .der

Consulte el apartado "Certificados e identidades" en la página 13 para obtener más información sobre los formatos compatibles y otros requisitos.

Cuando se descarga un certificado o identidad en el dispositivo, aparece la pantalla "Instalar perfil". La descripción indica el tipo de elemento: identidad o autoridad de certificación. Para instalar el certificado, pulse Instalar. Si se trata de un certificado de identidad, se le pedirá que introduzca la contraseña del certificado.

Para ver o eliminar un certificado instalado, vaya a Ajustes > General > Perfil. Si elimina un certificado necesario para acceder a una cuenta o red, el dispositivo no podrá conectarse a esos servicios.

Cuentas adicionales de Mail

Aunque solo es posible configurar una cuenta Exchange, puede añadir múltiples cuentas POP e IMAP. Esto sirve, por ejemplo, para acceder al correo electrónico en un servidor de correo de Lotus Notes o Novell Groupwise. Vaya a Ajustes > Cuentas > Mail, contactos, calendarios > Añadir cuenta > Otras. Para obtener más información acerca de cómo añadir una cuenta IMAP, consulte el *Manual del usuario del iPhone, el Manual del usuario del iPod touch* o *el Manual del usuario del iPad*.

Actualización y eliminación de perfiles de configuración

Para obtener información acerca de cómo puede un usuario actualizar o eliminar perfiles de configuración, consulte "Eliminación y actualización de perfiles de configuración" en la página 48.

Para obtener información acerca de la instalación de perfiles de datos de distribución, consulte "Distribución de aplicaciones" en la página 69.

Otros recursos

Para obtener información acerca del formato y función de los archivos de configuración automática de proxy que se utilizan en los ajustes de proxy de VPN, consulte:

- Proxy auto-config (PAC) (Configuración automática de proxy o PAC) en http://en.wikipedia.org/wiki/Proxy_auto-config
- Web Proxy Autodiscovery Protocol (Protocolo de detección automática de proxy web) en http://en.wikipedia.org/wiki/Wpad
- Microsoft TechNet: "Using Automatic Configuration, Automatic Proxy, and Automatic Detection" (Uso de configuración automática, proxy automático y detección automática) en http://technet.microsoft.com/en-us/library/dd361918.aspx

Apple dispone de lecciones de iniciación en vídeo, compatibles con cualquier navegador web estándar, que enseñan al usuario a configurar y utilizar las funciones del iPhone, el iPod touch y el iPad:

- Presentación del iPhone: www.apple.com/es/iphone/guidedtour/
- Presentación del iPod touch: www.apple.com/es/ipodtouch/guidedtour/
- Presentación del iPad: www.apple.com/ipad/guided-tours/
- Página web de soporte del iPhone: www.apple.com/es/support/iphone/
- Página web de soporte del iPod touch: www.apple.com/es/support/ipodtouch/
- Página web de soporte del iPad: www.apple.com/es/support/ipad/

También existe un manual del usuario (en PDF) para cada dispositivo que proporciona más consejos e información de uso:

- *Manual del usuario del iPhone:* http://manuals.info.apple.com/es_ES/iPhone_Manual_del_usuario.pdf
- *Manual del usuario del iPod touch:* http://manuals.info.apple.com/es_ES/iPod_touch_3.0_Manual_del_usuario.pdf
- *Manual del usuario del iPad*: http://manuals.info.apple.com/en/iPad_User_Guide.pdf

Distribución de iTunes

4

Puede utilizar iTunes para sincronizar música y vídeo, instalar aplicaciones y realizar muchas otras tareas.

Este capítulo describe cómo distribuir iTunes y aplicaciones de empresa, y define los ajustes y restricciones que es posible especificar.

El iPhone, el iPod touch y el iPad pueden sincronizar los diferentes tipos de datos (música, contenidos multimedia, etc.) con solo un ordenador al mismo tiempo. Por ejemplo, puede sincronizar música con un ordenador de escritorio y favoritos con un ordenador portátil. Para hacerlo, solo debe configurar debidamente las opciones de sincronización de iTunes en ambos ordenadores. Para obtener más información acerca de las opciones de sincronización, consulte la Ayuda iTunes, disponible en el menú Ayuda, dentro de iTunes.

Instalación de iTunes

iTunes utiliza instaladores estándar de Macintosh y Windows. Puede descargar la versión más reciente y una lista de los requisitos de sistema en www.itunes.com.

Para obtener información acerca de los requisitos de licencia para la distribución de iTunes, consulte: http://developer.apple.com/softwarelicensing/agreements/itunes.html

Instalación de iTunes en ordenadores Windows

Cuando instala iTunes en ordenadores Windows, por omisión también instala la versión más reciente de QuickTime, Bonjour y Apple Software Update. Puede omitir estos componentes añadiendo parámetros al programa de instalación de iTunes, o transmitiendo a los ordenadores de los usuarios sólo los componentes que desea instalar.

Instalación en Windows mediante iTunesSetup.exe

Si piensa utilizar el proceso normal de instalación de iTunes, pero omitir algunos componentes, puede transmitir instrucciones a iTunesSetup.exe utilizando la línea de comandos.

Propiedad	Significado
NO_AMDS=1	No instalar los servicios Apple Mobile Device. Este componente es necesario para que iTunes sincronice y gestione dispositivos móviles.
NO_ASUW=1	No instalar Apple Software Update para Windows. Esta aplicación avisa al usuario cuando hay nuevas versiones del software Apple.
NO_BONJOUR=1	No instalar Bonjour. Bonjour permite detectar impresoras no configuradas de la red, incluye bibliotecas compartidas de iTunes y ofrece otros servicios.
NO_QUICKTIME=1	No instalar QuickTime. Este componente es necesario para utilizar iTunes. No omita QuickTime a no ser que esté seguro de que el ordenador cliente ya dispone de la versión más reciente instalada.

Instalación silenciosa en Windows

Para instalar iTunes de forma "silenciosa", extraiga los archivos .msi individuales de iTunesSetup.exe y, a continuación, envíe los archivos a los ordenadores cliente.

Para extraer archivos .msi de iTunesSetup.exe:

1. Ejecute iTunesSetup.exe.
2. Abra *%temp%* y busque una carpeta denomina IXP*nnn*.TMP, donde *%temp%* es su directorio temporal y *nnn* es un número aleatorio de 3 dígitos. En Windows XP, el directorio temporal suele ser *unidadarranque*:\Documents and Settings*usuario*\Configuración local\temp\. En Windows Vista, el directorio temporal suele ser \Users*usuario*\AppData\Local\Temp\.
3. Copie los archivos .msi desde la carpeta a otra ubicación.
4. Salga del programa de instalación abierto por iTunesSetup.exe.

A continuación, utilice la política de grupo "Editor de objetos" en Microsoft Management Console para añadir los archivos .msi a la política "Configuración de equipo". Asegúrese de añadir la configuración a la política "Configuración de equipo", no a "Configuración de usuario".

Importante: iTunes requiere QuickTime y Apple Application Support. Apple Application Support debe estar instalado antes de instalar iTunes. Para utilizar un iPhone, un iPad o un iPod touch con iTunes es necesario disponer de Apple Mobile Device Services (AMDS).

Antes de distribuir los archivos .msi, debe seleccionar las versiones localizadas de iTunes que desea instalar. Para hacerlo, abra el .msi con la herramienta ORCA, la cual se instala con el kit de desarrollo de software de Windows como Orca.msi, en bin\. A continuación, edite la transmisión de información de resumen y quite los idiomas que no desee instalar. (La localización con el ID1033 corresponde al inglés.) También puede utilizar la política de grupo "Editor de objetos" para modificar las propiedades de despliegue de los archivos .msi de modo que se ignore el idioma.

Instalación de iTunes en ordenadores Macintosh

Los ordenadores Mac ya tienen iTunes instalado. La última versión de iTunes está disponible en www.itunes.com. Para transmitir iTunes a clientes Mac, puede utilizar Administrador Grupos de Trabajo, una herramienta administrativa incluida con Mac OS X Server.

Activación rápida de dispositivos con iTunes

Para poder utilizar un nuevo iPhone, iPod touch o iPad, es necesario conectarlo a un ordenador que esté ejecutando la aplicación iTunes para activarlo. Normalmente, tras la activación de un dispositivo, iTunes ofrece al usuario la posibilidad de sincronizarlo con el ordenador. Para evitar que aparezca esta opción si está configurando un dispositivo para otra persona, active la modalidad de sólo activación. De este modo, iTunes expulsará automáticamente el dispositivo después de activarlo. El dispositivo estará entonces listo para configurarse, pero no contendrá ningún archivo o dato.

Para activar la modalidad de sólo activación en Mac OS X:

1. Asegúrese de que la aplicación iTunes no está abierta y, a continuación, abra Terminal.
2. En Terminal, introduzca un comando:
   - Para activar la modalidad de sólo activación:

     ```
     defaults write com.apple.iTunes StoreActivationMode -integer 1
     ```
   - Para desactivar la modalidad de sólo activación:

     ```
     defaults delete com.apple.iTunes StoreActivationMode
     ```

Para activar un dispositivo, consulte el apartado "Uso de la modalidad de sólo activación".

Para activar la modalidad de sólo activación en Windows:

1. Asegúrese de que la aplicación iTunes no está abierta y, a continuación, abra una ventana de línea de comandos.
2. Introduzca un comando:
   - Para activar la modalidad de sólo activación:

     ```
     "C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 1
     ```
   - Para desactivar la modalidad de sólo activación:

     ```
     "C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 0
     ```

También puede crear una función rápida o modificar la función rápida de iTunes que ya tenga para incluir estos comandos de modo que pueda activar o desactivar rápidamente la modalidad de sólo activación.

Para verificar que iTunes se encuentra en la modalidad de sólo activación, seleccione iTunes > "Acerca de iTunes" y busque el texto "modalidad de sólo activación" debajo de la versión y del identificador de fase de iTunes.

Uso de la modalidad de sólo activación

Asegúrese de haber activado la modalidad de sólo activación tal como se ha descrito anteriormente y, a continuación, siga estos pasos.

1. Si va a activar un iPhone, inserte una tarjeta SIM activada. Use la herramienta de expulsión de tarjetas SIM o un clip de papel enderezado para extraer la bandeja SIM. Para más información al respecto, consulte el *Manual del usuario del iPhone*.
2. Conecte el iPhone, el iPod touch o el iPad al ordenador. El ordenador debe estar conectado a Internet para activar el dispositivo.

   La aplicación iTunes se abre, si es necesario, y activa el dispositivo. Cuando el proceso de activación se haya completado, aparecerá un mensaje.
3. Desconecte el dispositivo.

   Podrá conectar y activar inmediatamente otros dispositivos. iTunes no se sincronizará con ningún dispositivo mientras la modalidad de sólo activación esté activada, así que no olvide desactivar esta modalidad si desea usar iTunes para sincronizar dispositivos.

Ajuste de restricciones de iTunes

Puede restringir a los usuarios la utilización de determinadas funciones de iTunes. A veces, esta función se denomina "control parental". Se pueden restringir las siguientes funciones:

- Búsqueda automática o iniciada por el usuario de nuevas versiones de iTunes y actualizaciones del software para dispositivos
- Visualización de sugerencias de Genius al explorar o reproducir contenidos
- Sincronización automática al conectar dispositivos
- Descarga de ilustraciones de álbum
- Utilización de módulos de Visualizer
- Introducción de una dirección URL de transmisión de contenido en tiempo real
- Detección automática de sistemas Apple TV
- Registro de nuevos dispositivos en Apple
- Suscripción a podcasts
- Reproducción de radio por Internet
- Acceso a iTunes Store

- Compartir la biblioteca con ordenadores de la red local que también utilicen iTunes
- Reproducción de contenido de iTunes para adultos
- Reproducción de películas
- Reproducción de programas de televisión

Ajuste de las restricciones de iTunes para Mac OS X

En Mac OS X, el acceso a iTunes se controla utilizando claves en un archivo plist. En Mac OS X pueden especificarse los valores de clave anteriores para cada usuario editando ~/Librería/Preferencias/com.apple.iTunes.plist mediante Administrador Grupos de Trabajo, una herramienta administrativa incluida con Mac OS X Server.

Para obtener instrucciones al respecto, consulte el siguiente artículo de soporte técnico de Apple: http://docs.info.apple.com/article.html?artnum=303099-es.

Ajuste de las restricciones de iTunes para Windows

En Windows, el acceso a iTunes se controla especificando valores de registro dentro de una de las siguientes claves del registro:

En Windows XP y Windows Vista de 32 bits:

- HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Apple Computer, Inc.\iTunes\Parental Controls

En Windows Vista de 64 bits:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Wow6432Node\Apple Computer, Inc.\iTunes\Parental Controls

Para obtener información sobre los valores de registro de iTunes, consulte el siguiente artículo de soporte técnico de Apple: http://support.apple.com/kb/HT2102?viewlocale=es_ES.

Para obtener información general sobre la modificación del registro de Windows, consulte el siguiente artículo de ayuda y soporte técnico de Microsoft: http://support.microsoft.com/kb/136393.

Actualización manual de iTunes y iPhone OS

Si desactiva en iTunes la búsqueda de actualizaciones de software automatizada e iniciada por el usuario, deberá distribuir a los usuarios las actualizaciones de software para su instalación manual.

Para actualizar iTunes, consulte las instrucciones de instalación y distribución indicadas más arriba en este manual. Se trata de realizar el mismo proceso que se ha seguido para distribuir iTunes a los usuarios.

Para actualizar el sistema iPhone OS, siga estos pasos:

1. En un ordenador que no tenga desactivada la actualización de software de iTunes, utilice iTunes para descargar la actualización de software. Para ello, seleccione un dispositivo conectado en iTunes, haga clic en la pestaña Resumen y, a continuación, haga clic en el botón "Buscar actualizaciones".
2. Tras la descarga, copie el archivo de actualización (.ipsw) que se encuentra en la siguiente ubicación:
   - *En Mac OS X:* ~/Librería/iTunes/iPhone Software Updates/
   - *En Windows XP: disco de arranque*:\Documents and Settings*usuario*\Application Data\Apple Computer\iTunes\iPhone Software Updates\
3. Distribuya el archivo .ipsw a los usuarios, o colóquelo en un disco de red donde sea accesible.
4. Indique a los usuarios que realicen una copia de seguridad de su dispositivo con iTunes antes de aplicar la actualización. Durante las actualizaciones manuales, iTunes no realiza una copia de seguridad automática del dispositivo antes de la instalación. Para crear una nueva copia de seguridad, haga clic con el botón derecho del ratón (Windows) o pulse Control y haga clic (Mac) en el dispositivo, en la barra lateral de iTunes. A continuación, seleccione "Copia de seguridad" en el menú local que aparecerá.
5. Los usuarios instalan la actualización conectando el dispositivo a iTunes y seleccionando la pestaña Resumen de su dispositivo. A continuación, mantienen pulsada la tecla Opción (Mac) o Mayúsculas (Windows) y hacen clic en el botón "Buscar actualizaciones".
6. Aparecerá un cuadro de diálogo de selección de archivos. Los usuarios deben seleccionar el archivo .ipsw y hacer clic en Abrir para comenzar el proceso de actualización.

Copia de seguridad de un dispositivo con iTunes

Cuando se sincronizan el iPhone, el iPod touch o el iPad con iTunes, se crea una copia de seguridad automática de los ajustes del dispositivo en el ordenador. Las aplicaciones adquiridas en la tienda App Store se copian en la biblioteca de iTunes.

Las aplicaciones desarrolladas por usted mismo y distribuidas a sus usuarios mediante perfiles de distribución de empresa no se copiarán ni transferirán al ordenador del usuario. Sin embargo, la copia de seguridad del dispositivo incluirá todos los archivos de datos que haya creado su aplicación.

Las copias de seguridad de dispositivos se pueden almacenar con un formato encriptado. Para hacerlo, seleccione la opción "Encriptar copia de seguridad" del dispositivo en el panel de resumen de iTunes. Los archivos están encriptados mediante AES256. La clave se almacena de forma segura en el llavero de iPhone OS.

Importante: Si el dispositivo del que se está creando la copia de seguridad tiene instalado algún perfil encuitado, iTunes solicitará al usuario que active la encriptación de la copia de seguridad.

Distribución de aplicaciones 5

Puede distribuir aplicaciones del iPhone, el iPod touch y el iPad a los usuarios.

Si desea instalar aplicaciones para iPhone OS que haya desarrollado, distribúyalas a los usuarios para que las instalen mediante iTunes.

Las aplicaciones de la tienda App Store en Internet funcionan en el iPhone, el iPod touch y el iPad sin necesidad de realizar pasos adicionales. Si desarrolla una aplicación y quiere distribuirla por su cuenta, deberá firmarla digitalmente con un certificado emitido por Apple. También deberá proporcionar a los usuarios un perfil de datos de distribución que permita al dispositivo utilizar la aplicación.

El proceso para distribuir sus propias aplicaciones es el siguiente:

- Regístrese en Apple como desarrollador de productos para empresa.
- Firme sus aplicaciones utilizando su certificado.
- Cree un perfil de datos de distribución corporativa que autorice a los dispositivos a utilizar las aplicaciones firmadas por usted.
- Distribuya la aplicación y el perfil de datos de distribución corporativa a los ordenadores de los usuarios.
- Indique a los usuarios que instalen la aplicación y el perfil mediante iTunes.

A continuación tiene más información acerca de cada uno de estos pasos.

Registro como desarrollador de aplicaciones

Para desarrollar y distribuir aplicaciones personalizadas para iPhone OS, antes debe registrarse en el programa iPhone Enterprise Developer Program, en el sitio http://developer.apple.com/.

Una vez complete el proceso de registro, recibirá instrucciones para que sus aplicaciones funcionen en los dispositivos.

Firma de aplicaciones

Las aplicaciones que distribuya a los usuarios deben estar firmadas con su certificado de distribución. Para obtener instrucciones sobre la obtención y utilización de un certificado, consulte el iPhone Developer Center en http://developer.apple.com/iphone (en inglés).

Creación de un perfil de datos de distribución

Los perfiles de datos de distribución le permiten crear aplicaciones que los usuarios pueden utilizar en su dispositivo. Para crear un perfil de datos de distribución de empresa para una aplicación específica, o para múltiples aplicaciones, especifique el AppID autorizado por el perfil. Si un usuario tiene una aplicación pero carece de un perfil que autorice su uso, no podrá utilizarla.

El Team Agent designado para su empresa puede crear perfiles de datos de distribución en el portal Enterprise Program, en http://developer.apple.com/iphone (en inglés). Consulte este sitio web para obtener instrucciones.

Una vez creado el perfil de datos de distribución de empresa, descargue el archivo .mobileprovision y distribuya de forma segura su aplicación.

Instalación de perfiles de datos mediante iTunes

La copia de iTunes del usuario instala los perfiles de datos ubicados en las siguientes carpetas, definidas en esta sección. Si las carpetas no existen, créelas usando los nombres mostrados.

Mac OS X

- ~/Librería/MobileDevice/Provisioning Profiles
- /Librería/MobileDevice/Provisioning Profiles
- La ruta especificada por la clave ProvisioningProfilesPath en ~/Librería/Preferencias/com.apple.itunes

Windows XP

- *Unidad de arranque*:\Documents and Settings*usuario*\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- *Unidad de arranque*:\Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- La ruta especificada en HKCU o HKLM por la clave de registro ProvisioningProfilesPath SOFTWARE\Apple Computer, Inc\iTunes

Windows Vista

- *Unidad de arranque*:\Users*nombre de usuario*\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- *Unidad de arranque*:\ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- La ruta especificada en HKCU o HKLM por la clave de registro ProvisioningProfiles-Path SOFTWARE\Apple Computer, Inc\iTunes

iTunes instala automáticamente los perfiles de datos que encuentre en las ubicaciones anteriores en los dispositivos con los que se sincroniza. Una vez instalados, los perfiles de datos pueden verse en el dispositivo seleccionando Ajustes > General > Perfiles.

También puede distribuir el archivo .mobileprovision a los usuarios e indicarles que lo arrastren al icono de la aplicación iTunes, que copiará el archivo en la ubicación correcta definida anteriormente.

Instalación de perfiles de datos con la Utilidad Configuración iPhone

Puede emplear la Utilidad Configuración iPhone para instalar perfiles de datos en los dispositivos conectados. Siga estos pasos:

1. En la Utilidad Configuración iPhone, seleccione Archivo > "Añadir a la biblioteca" y, a continuación, seleccione el perfil de datos que desee instalar.

   El perfil se añade a la Utilidad Configuración iPhone y puede visualizarse seleccionando la categoría "Perfiles de datos" en la Biblioteca.
2. Elija un dispositivo en la lista "Dispositivos conectados".
3. Haga clic en la pestaña Perfiles de datos.
4. Seleccione el perfil de datos en la lista y haga clic en el botón Instalar.

Instalación de aplicaciones mediante iTunes

Los usuarios emplean iTunes para instalar aplicaciones en sus dispositivos. Distribuya de forma segura la aplicación a los usuarios e indíqueles que sigan estos pasos:

1. En iTunes, seleccione Archivo > "Añadir a Biblioteca" y, a continuación, seleccione la aplicación (.app) proporcionada.

   También puede arrastrar el archivo .app al icono de aplicación de iTunes.
2. Conecte un dispositivo al ordenador y selecciónelo en la lista Dispositivos de iTunes.
3. Haga clic en la pestaña Aplicaciones y seleccione la aplicación en la lista.

4 Haga clic en Aplicar para instalar la aplicación y todos los perfiles de datos de distribución ubicados en las carpetas indicadas en "Instalación de perfiles de datos mediante iTunes" en la página 70.

Instalación de aplicaciones con la Utilidad Configuración iPhone

Puede emplear la Utilidad Configuración iPhone para instalar aplicaciones en los dispositivos conectados. Siga estos pasos:

1 En la Utilidad Configuración iPhone, seleccione Archivo > "Añadir a la biblioteca" y, a continuación, seleccione la aplicación que desee instalar.

La aplicación se añade a la Utilidad Configuración iPhone y puede visualizarse seleccionando la categoría Aplicaciones en la Biblioteca.

2 Elija un dispositivo en la lista "Dispositivos conectados".

3 Haga clic en la pestaña Aplicaciones.

4 Elija la aplicación en la lista y haga clic en el botón Instalar.

Utilización de aplicaciones para empresa

Cuando un usuario ejecuta una aplicación no firmada por Apple, el dispositivo busca un perfil de datos de distribución que autorice su uso. Si no se encuentra un perfil, la aplicación no se abrirá.

Cómo desactivar una aplicación de empresa

Si necesita desactivar una aplicación interna, puede hacerlo revocando la identidad empleada para firmar el perfil de datos de distribución. De ese modo, la aplicación ya no podrá instalarse y, si está ya instalada, no podrá volver a abrirse.

Otros recursos

Para obtener más información acerca de la creación de aplicaciones y perfiles de datos, consulte:

- iPhone Devolver Center en http://developer.apple.com/iphone/ (en inglés)

Configuración del servidor Cisco VPN

Utilice estas directrices para configurar un servidor Cisco VPN y utilizarlo con el iPhone, el iPod touch y el iPad.

Plataformas Cisco compatibles

El sistema iPhone OS es compatible con los dispositivos de seguridad ASA 5500 y los firewalls PIX de Cisco configurados con la versión 7.2.x o posterior del software. Se recomienda utilizar la versión del software 8.0.x (o posterior) más reciente disponible. iPhone OS también es compatible con los routers VPN IOS de Cisco con la versión 12.4(15)T o posterior de IOS. En cambio, los concentradores de la serie VPN 3000 no son compatibles con las funciones de VPN del iPhone.

Métodos de autenticación

El sistema iPhone OS es compatible con los siguientes métodos de autenticación:

- Autenticación IPsec de clave precompartida con autenticación de usuario mediante xauth
- Certificados de cliente y servidor para autenticación IPsec con autenticación opcional de usuario mediante xauth
- Autenticación híbrida, en la que el servidor proporciona un certificado y el cliente proporciona una clave precompartida para la autenticación IPsec; se requiere la autenticación de usuario mediante xauth.
- La autenticación de usuario se proporciona mediante xauth e incluye los siguientes métodos:
  - Nombre de usuario con contraseña
  - RSA SecurID
  - CryptoCard

Grupos de autenticación

El protocolo Cisco Unity utiliza grupos de autenticación para agrupar a los usuarios según conjuntos comunes de autenticación y otros parámetros. Es conveniente crear un grupo de autenticación para los usuarios de dispositivos iPhone OS. Para la autenticación por clave precompartida e híbrida, el nombre del grupo debe configurarse en el dispositivo, siendo la contraseña el secreto compartido (la clave precompartida).

Al utilizar autenticación por certificado, no se emplea secreto compartido y el grupo de los usuarios se determina según los campos del certificado. Se pueden utilizar los ajustes del servidor Cisco para vincular campos de un certificado a grupos de usuarios.

Certificados

Al configurar e instalar certificados, asegúrese de lo siguiente:

- El certificado de identidad del servidor debe contener el nombre DNS y/o la dirección IP del servidor en el campo de nombre alternativo (SubjectAltName). El dispositivo emplea esta información para verificar que el certificado pertenece al servidor. Puede especificar el SubjectAltName empleando caracteres comodín en algunos segmentos, como por ejemplo "vpn.*.miempresa.com", y así disfrutar de mayor flexibilidad. El nombre DNS puede introducirse en el campo del nombre común si no se ha especificado un SubjectAltName.
- Debería instalarse en el dispositivo el certificado de la autoridad de certificación que firmó el certificado del servidor. Si no se trata de un certificado raíz, instale el resto de la cadena de confianza para que el certificado sea aprobado.
- Si se emplean certificados cliente, asegúrese de que el certificado fiable de la autoridad de certificación que firmó el del cliente esté instalado en el servidor VPN.
- Los certificados y autoridades de certificación deben ser válidos (no pueden haber caducado, por ejemplo).
- No es posible enviar cadenas de certificados por parte del servidor, por lo que esta opción debe desactivarse.
- Al utilizar la autenticación mediante certificados, asegúrese de que el servidor esté configurado para identificar el grupo del usuario según los campos del certificado cliente. Consulte "Grupos de autenticación" en la página 74.

Ajustes IPsec

Utilice los siguientes ajustes de IPsec:

- *Modo:* modo Túnel
- *Modos de intercambio IKE:* modo agresivo de autenticación con clave precompartida e híbrida, modo principal para la autenticación mediante certificado.
- *Algoritmos de encriptación:* 3DES, AES-128, AES-256
- *Algoritmos de autenticación:* HMAC-MD5, HMAC-SHA1
- *Grupos Diffie Hellman:* para la autenticación por clave precompartida e híbrida se requiere el grupo 2. Para la autenticación mediante certificado, utilice el grupo 2 con 3DES y AES-128. Utilice los grupos 2 o 5 con AES-256.
- *PFS (Perfect Forward Secrecy):* en IKE fase 2, si se utiliza PFS, el grupo Diffie-Hellman debe ser el mismo que para IKE fase 1.
- *Configuración de modo:* debe estar activado.
- *Detección de Dead Peer:* recomendada.
- *NAT transversal estándar:* es compatible y puede activarse si se desea. (No puede utilizarse IPsec por TCP).
- *Equilibrio de carga:* es compatible y puede activarse si se desea.
- *Re-keying de fase 1:* no es compatible en este momento. Se recomienda ajustar los tiempos de re-keying en el servidor a una hora aproximadamente.
- *Máscara de direcciones ASA:* asegúrese de que ninguna de las máscaras de direcciones del dispositivo esté configurada o bien que todas ellas estén ajustadas a 255.255.255.255. Por ejemplo:

  ```
  asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 mask
     255.255.255.255.
  ```

  Al utilizar la máscara de direcciones recomendada, puede que se ignoren algunas rutas asumidas por la configuración VPN. Para evitarlo, asegúrese de que su tabla de enrutamiento contiene todas las rutas necesarias y compruebe que las direcciones de subred son accesibles antes de la implementación.

Otras características compatibles

El iPhone, el iPod touch y el iPad admiten las funciones siguientes:

- *Versión de aplicación:* la versión del software cliente se envía al servidor, lo que permite a este aceptar o rechazar conexiones según la versión del software del dispositivo.
- *Banner:* el banner, si está configurado en el servidor, se muestra en el dispositivo y el usuario debe aceptarlo o desconectarse.
- *Túnel dividido:* se admite el túnel dividido.
- *DNS dividida:* se admite la DNS dividida.
- *Dominio por omisión:* se admite el dominio por omisión.

Formato del perfil de configuración

B Apéndice

Este apéndice especifica el formato de los archivos mobileconfig para aquellos que deseen crear sus propias herramientas.

Este documento asume que está familiarizado con la DTD XML de Apple y con el formato general "property list". Puede consultar una descripción general del formato plist de Apple en www.apple.com/DTDs/PropertyList-1.0.dtd. Para comenzar, utilice la Utilidad Configuración iPhone para crear un archivo de base que podrá modificar utilizando la información contenida en este apéndice.

Este documento emplea los términos *"contenido" ("payload")* y *"perfil"*. Un perfil es el archivo que configura ciertos ajustes (únicos o múltiples) en el iPhone, el iPod touch o el iPad. Un contenido es un componente individual del archivo perfil.

Nivel raíz

En el nivel raíz, el archivo de configuración es un diccionario con los siguientes pares clave/valor:

Clave	Valor
PayloadVersion	Número, obligatorio. La versión del archivo perfil de configuración. Este número de versión designa el formato de todo el perfil, no el de los contenidos individuales.
PayloadUUID	Secuencia de caracteres, obligatoria. Una secuencia de caracteres identificadora y única, normalmente generada de forma sintética. El contenido exacto de esta secuencia es irrelevante, pero debe ser único en el ámbito global. En Mac OS X, puede generar identificadores UUID con /usr/bin/uuidgen.
PayloadType	Secuencia de caracteres, obligatoria. En este momento, "Configuration" es el único valor válido para esta clave.
PayloadOrganization	Secuencia de caracteres, opcional. Este valor describe la organización emisora del perfil tal y como se muestra al usuario.

Clave	Valor
PayloadIdentifier	Secuencia de caracteres, obligatoria. Este valor es, por convención, una secuencia de caracteres delimitada por puntos que describe de forma única el perfil, como "com.miCorp.iPhone.mailSettings" o "edu.miUniversidad.estudiantes.vpn". Es la secuencia que diferencia los perfiles. Si se instala un perfil que tiene el mismo identificador que otro, dicho perfil no se añade, sino que sustituye al antiguo.
PayloadDisplayName	Secuencia de caracteres, obligatoria. Este valor determina una secuencia de caracteres muy corta que se muestra al usuario y que describe el perfil, como "Ajustes VPN". No tiene por qué ser único.
PayloadDescription	Secuencia de caracteres, opcional. Este valor determina el texto descriptivo y de formato libre que se mostrará al usuario en la pantalla Detalle de todo el perfil. Esta secuencia debería identificar con claridad el perfil, de modo que el usuario pueda decidir si lo instala o no.
PayloadContent	Matriz, opcional. Este valor es la información real del perfil. Si se omite, el perfil carece de significado funcional.
PayloadRemovalDisallowed	Booleano, opcional. Por omisión, "No". Si está definido, el usuario no podrá eliminar el perfil. Un perfil con este parámetro definido puede actualizarse a través de una conexión USB o de Internet/correo electrónico únicamente si el identificador del perfil coincide y está firmado por la misma autoridad. Si se proporciona una contraseña de eliminación, se podrá eliminar el perfil introduciendo dicha contraseña. Con perfiles firmados y encriptados, tener este valor sin cifrar no tiene consecuencias ya que el perfil no se puede alterar y este ajuste también se muestra en el dispositivo.

Contenidos

PayloadContent es una matriz de diccionarios, cada uno de los cuales describe uno de los contenidos del perfil. Todo perfil funcional posee al menos una entrada en esta matriz. Todos los diccionarios de esta matriz tienen algunas propiedades comunes, sea cual sea el tipo de contenido. Otros están especializados y son únicos para cada tipo de contenido.

Clave	Valor
PayloadVersion	Número, obligatorio. La versión del contenido concreto. Todo perfil puede consistir en contenidos con distintos números de versión. Por ejemplo, puede incrementarse el número de versión VPN en cualquier momento, mientras que el de Mail permanece igual.
PayloadUUID	Secuencia de caracteres, obligatoria. Una secuencia de caracteres identificadora y única, normalmente generada de forma sintética. El contenido exacto de esta secuencia es irrelevante, pero debe ser único en el ámbito global.
PayloadType	Secuencia de caracteres, obligatoria. Este par clave/valor determina el tipo de contenido concreto dentro del perfil.
PayloadOrganization	Secuencia de caracteres, opcional. Este valor describe la organización emisora del perfil tal y como se mostrará al usuario. Puede ser el mismo que el del PayloadOrganization del nivel raíz, pero no necesariamente.
PayloadIdentifier	Secuencia de caracteres, obligatoria. Este valor es, por convención, una secuencia de caracteres única y delimitada por puntos que describe el contenido. Suele ser el valor PayloadIdentifier raíz con un subidentificador añadido que describe el contenido concreto.
PayloadDisplayName	Secuencia de caracteres, obligatoria. Este valor es una secuencia de caracteres muy corta que se muestra al usuario y que describe el perfil, como "Ajustes VPN". No tiene por qué ser único.
PayloadDescription	Secuencia de caracteres, opcional. Este valor determina el texto descriptivo y de formato libre que se muestra al usuario en la pantalla Detalle del contenido concreto.

Contenido de contraseña de eliminación del perfil

El contenido de la contraseña de eliminación queda designado por el valor com.apple.profileRemovalPassword de PayloadType. Sirve para codificar la contraseña que permite a los usuarios eliminar un perfil de configuración del dispositivo. Si este contenido está presente y tiene configurado un valor de contraseña, el dispositivo solicitará dicha contraseña cuando el usuario pulse el botón Eliminar de un perfil. Este contenido se encripta junto con el resto del perfil.

Clave	Valor
RemovalPassword	Secuencia de caracteres, opcional. Especifica la contraseña de eliminación del perfil.

Contenido de política de código

El contenido "Política de código" se designa mediante el valor PayloadType de com.apple.mobiledevice.passwordpolicy. La presencia de este tipo de contenido hace que el dispositivo presente al usuario un mecanismo de entrada de código alfanumérico para introducir códigos de longitud y complejidad arbitrarias.

Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
allowSimple	Booleano, opcional. Por omisión, YES. Determina si se permite un código simple. Un código simple es uno que contiene caracteres repetidos o en orden creciente/decreciente (como "123" o "CBA"). Ajustar este valor a NO equivale a ajustar minComplexChars a 1.
forcePIN	Booleano, opcional. Por omisión, NO. Determina si el usuario está obligado a introducir un PIN. Ajustar solo este valor (y no otros) obliga al usuario a introducir un código, sin imponer su longitud o calidad.
maxFailedAttempts	Número, opcional. Por omisión, 11. Intervalo permitido: [2...11]. Especifica el número de fallos de introducción del código que se permiten en la pantalla de bloqueo del dispositivo. Cuando se excede este número, el dispositivo se bloquea y debe conectarse a su iTunes designado para poder desbloquearse.
maxInactivity	Número, opcional. Por omisión, Infinity. Especifica el número de minutos que el dispositivo puede permanecer inactivo (sin ser desbloqueado por el usuario) antes de que el sistema lo bloquee. Una vez alcanzado este límite, el dispositivo se bloquea y es necesario introducir el código.
maxPINAgeInDays	Número, opcional. Por omisión, Infinity. Especifica el número de días que el código puede permanecer sin ser cambiado. Tras este tiempo, el usuario está obligado a cambiar el código para desbloquear el dispositivo.

Clave	Valor
minComplexChars	Número, opcional. Por omisión, 0. Especifica el número mínimo de caracteres complejos que debe contener un código. Un carácter "complejo" es aquel que no es ni un número ni una letra, como &%$#.
minLength	Número, opcional. Por omisión, 0. Especifica la longitud mínima del código. Este parámetro es independiente del argumento también opcional minComplexChars.
requireAlphanumeric	Booleano, opcional. Por omisión, NO. Especifica si el usuario debe introducir caracteres alfabéticos ("abcd"), o si es suficiente con números.
pinHistory	Número, opcional. Cuando el usuario cambia el código, éste debe ser único y diferente en las últimas N entradas del historial. El valor mínimo es 1 y el máximo, 50.
manualFetchingWhenRoaming	Booleano, opcional. Si está definido, todas las operaciones Push se desactivarán en el modo de itinerancia. El usuario deberá obtener manualmente los datos nuevos.
maxGracePeriod	Número, opcional. El periodo de gracia máximo, en minutos, en el que se puede desbloquear el teléfono sin tener que introducir un código. El valor por omisión es 0, es decir, que no hay periodo de gracia y que es necesario introducir el código de inmediato.

Contenido de correo electrónico

El contenido de correo electrónico queda designado por el valor PayloadType de com.apple.mail.managed. Este contenido crea una cuenta de correo electrónico en el dispositivo. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
EmailAccountDescription	Secuencia de caracteres, opcional. Una descripción de la cuenta de correo electrónico que se muestra al usuario en las aplicaciones Mail y Ajustes.
EmailAccountName	Secuencia de caracteres, opcional. El nombre de usuario completo de la cuenta. Este es el nombre de usuario que aparece en los mensajes enviados, etc.
EmailAccountType	Secuencia de caracteres, obligatoria. Los valores permitidos son EmailTypePOP y EmailTypeIMAP. Define el protocolo a emplear para esa cuenta.
EmailAddress	Secuencia de caracteres, obligatoria. Designa la dirección de correo electrónico completa de la cuenta. Si no está presente en el contenido, el dispositivo solicita esta secuencia durante la instalación del perfil.

Clave	Valor
IncomingMailServerAuthentication	Secuencia de caracteres, obligatoria. Designa el esquema de autenticación para el correo entrante. Los valores permitidos son EmailAuthPassword y EmailAuthNone.
IncomingMailServerHostName	Secuencia de caracteres, obligatoria. Designa el nombre (o la dirección IP) del servidor de correo entrante.
IncomingMailServerPortNumber	Número, opcional. Designa el número de puerto del servidor de correo entrante. Si no se especifica un número de puerto, se emplea el puerto por omisión de un protocolo dado.
IncomingMailServerUseSSL	Booleano, opcional. Por omisión, YES. Designa si el servidor de correo entrante utiliza SSL para la autenticación.
IncomingMailServerUsername	Secuencia de caracteres, obligatoria. Designa el nombre de usuario de la cuenta de correo electrónico, que suele ser igual a la dirección de correo electrónico hasta el símbolo @. Si no está presente en el contenido y la cuenta se configura de modo que requiera autenticación para el correo entrante, el dispositivo solicitará esta secuencia de caracteres durante la instalación del perfil.
IncomingPassword	Secuencia de caracteres, opcional. Corresponde a la contraseña del servidor de correo entrante. Solo se puede usar con perfiles encriptados.
OutgoingPassword	Secuencia de caracteres, opcional. Corresponde a la contraseña del servidor de correo saliente. Solo se puede usar con perfiles encriptados.
OutgoingPasswwordSameAsIncomingPassword	Booleano, opcional. Si este parámetro está definido, se solicitará al usuario la contraseña solamente una vez y se utilizará tanto para el correo entrante como para el saliente.
OutgoingMailServerAuthentication	Secuencia de caracteres, obligatoria. Designa el esquema de autenticación para el correo saliente. Los valores permitidos son EmailAuthPassword y EmailAuthNone.
OutgoingMailServerHostName	Secuencia de caracteres, obligatoria. Designa el nombre (o la dirección IP) del servidor de correo saliente.
OutgoingMailServerPortNumber	Número, opcional. Designa el número de puerto del servidor de correo saliente. Si no se especifica un número de puerto, se emplean los puertos 25, 587 y 465 (por este orden).
OutgoingMailServerUseSSL	Booleano, opcional. Por omisión, YES. Designa si el servidor de correo saliente utiliza SSL para la autenticación.
OutgoingMailServerUsername	Secuencia de caracteres, obligatoria. Designa el nombre de usuario de la cuenta de correo electrónico, que suele ser igual a la dirección de correo electrónico hasta el símbolo @. Si no está presente en el contenido y la cuenta se configura de modo que requiera autenticación para el correo saliente, el dispositivo solicita esta secuencia de caracteres durante la instalación del perfil.

Contenido Clip web

El contenido Clip web se designa mediante el valor PayloadType de com.apple.web-Clip.managed. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
URL	Secuencia de caracteres, obligatoria. La URL que el clip web debe abrir cuando se hace clic en él. La URL debe comenzar por HTTP o HTTPS para que funcione.
Etiqueta	Secuencia de caracteres, obligatoria. El nombre del clip web se muestra en la pantalla de inicio.
Icono	Dato, opcional. Icono PNG que se muestra en la pantalla de inicio. El tamaño habitual es 59 x 60 píxeles. Si no se especifica, se mostrará un cuadro en blanco.
IsRemovable	Booleano, opcional. Si se ajusta a "No", el usuario no podrá eliminar el clip web, aunque sí se eliminará si se borra el perfil.

Contenido Restricciones

El contenido Restricciones se designa mediante el valor PayloadType de com.apple.applicationaccess. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
allowAppInstallation	Booleano, opcional. Cuando es falso, la tienda App Store está desactivada y su icono desaparece de la pantalla de inicio. Los usuarios tampoco pueden instalar o actualizar sus aplicaciones.
allowCamera	Booleano, opcional. Cuando es falso, la cámara está completamente desactivada y su icono desaparece de la pantalla de inicio. Los usuarios no pueden hacer fotos.
allowExplicitContent	Booleano, opcional. Cuando es falso, las canciones o vídeos con contenidos para adultos que se hayan comprado en la tienda iTunes Store permanecerán ocultos. Son los propios proveedores de los contenidos (por ejemplo, los propios sellos discográficos) los que los marcan como explícitos cuando los ponen a la venta a través de la iTunes Store.
allowScreenShot	Booleano, opcional. Cuando es falso, los usuarios no pueden guardar capturas de pantalla.
allowYouTube	Booleano, opcional. Cuando es falso, la aplicación YouTube está desactivada y su icono desaparece de la pantalla de inicio.

Clave	Valor
allowiTunes	Booleano, opcional. Cuando es falso, la tienda iTunes Music Store está desactivada y su icono desaparece de la pantalla de inicio. Los usuarios no pueden comprar, descargar ni escuchar fragmentos de los contenidos de la tienda.
allowSafari	Booleano, opcional. Cuando es falso, el navegador web Safari está desactivado y su icono desaparece de la pantalla de inicio. Además, los usuarios no pueden abrir clips web.

Contenido LDAP

El contenido LDAP se designa mediante el valor PayloadType de com.apple.ldap.account. Se establece una relación de uno a muchos entre Cuenta LDAP y LDAPSearchSettings. Si piensa en LDAP como un árbol, cada objeto SearchSettings representa un nodo del árbol en el que empezar la búsqueda y el alcance de dicha búsqueda (nodo, nodo+1 nivel inferior, nodo + todos los niveles inferiores). Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
LDAPAccountDescription	Secuencia de caracteres, opcional. Descripción de la cuenta.
LDAPAccountHostName	Secuencia de caracteres, obligatoria. El servidor.
LDAPAccountUseSSL	Booleano, obligatorio. Si se usa SSL o no.
LDAPAccountUserName	Secuencia de caracteres, opcional. El nombre de usuario.
LDAPAccountPassword	Secuencia de caracteres, opcional. Solo se puede usar con perfiles encriptados.
LDAPSearchSettings	El objeto contenedor del primer nivel. Aunque una cuenta puede tener más de uno, debe tener como mínimo uno para que resulte útil.
LDAPSearchSettingDescription	Secuencia de caracteres, opcional. Descripción de este ajuste de búsqueda.
LDAPSearchSettingSearchBase	Secuencia de caracteres, obligatoria. Conceptualmente, la ruta del nodo para iniciar una búsqueda en "ou=personas,o=empresa ejemplo".
LDAPSearchSettingScope	Secuencia de caracteres, obligatoria. Define la recursividad de la búsqueda. Puede ser uno de los siguientes tres valores: LDAPSearchSettingScopeBase: el nodo inmediato al que señala SearchBase. LDAPSearchSettingScopeOneLevel: el nodo más su nodo hijo inmediato. LDAPSearchSettingScopeSubtree: el nodo más todos sus nodos hijo, independientemente de su profundidad.

Contenido CalDAV

El contenido CalDAV se designa mediante el valor PayloadType de com.apple.caldav.account. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
CalDAVAccountDescription	Secuencia de caracteres, opcional. Descripción de la cuenta.
CalDAVHostName	Secuencia de caracteres, obligatoria. La dirección del servidor.
CalDAVUsername	Secuencia de caracteres, obligatoria. El nombre de inicio de sesión del usuario.
CalDAVPassword	Secuencia de caracteres, opcional. La contraseña del usuario.
CalDAVUseSSL	Booleano, obligatorio. Si se usa SSL o no.
CalDAVPort	Número, opcional. El puerto de conexión del servidor.
CalDAVPrincipalURL	Secuencia de caracteres, opcional. La URL base del calendario del usuario.

Contenido de suscripción a calendario

El contenido CalSub se designa mediante el valor PayloadType de com.apple.subscribedcalendar.account. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
SubCalAccountDescription	Secuencia de caracteres, opcional. Descripción de la cuenta.
SubCalAccountHostName	Secuencia de caracteres, obligatoria. La dirección del servidor.
SubCalAccountUsername	Secuencia de caracteres, opcional. El nombre de inicio de sesión del usuario.
SubCalAccountPassword	Secuencia de caracteres, opcional. La contraseña del usuario.
SubCalAccountUseSSL	Booleano, obligatorio. Si se usa SSL o no.

Contenido SCEP

El contenido SCEP (Simple Certificate Enrollment Protocol) se designa mediante el valor PayloadType de com.apple.encrypted-profile-service. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
URL	Secuencia de caracteres, obligatoria.
Nombre	Secuencia de caracteres, opcional (cualquier secuencia de caracteres reconocida por el servidor SCEP). Podría tratarse, por ejemplo, de un nombre de dominio como "ejemplo.org". Si una autoridad de certificación tiene varios certificados de CA, este campo se puede usar para distinguir cuál de ellos es el necesario.
Asunto	Matriz, opcional. La representación de un nombre X.500 expresado como una matriz de OID y valor. Por ejemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se traduciría de la siguiente manera: [[["C","US"]], [["O","Apple Inc."]], ..., [["1.2.5.3","bar"]]] Los OID (identificadores de objeto) se pueden representar como una serie de números separados por puntos y abreviaciones: C (país), L (localidad), ST (estado), O (organización), OU (unidad organizativa), CN (nombre común).
Contraseña de comprobación	Secuencia de caracteres, opcional. Un secreto precompartido.
Tamaño de la clave	Número, opcional. El tamaño de la clave en bits (1024 o 2048).
Tipo de clave	Secuencia de caracteres, opcional. Actualmente, siempre "RSA".
Uso de la clave	Número, opcional. Una máscara de bits que indica el uso de la clave. 1 es firma, 4 es encriptación y 5 es firma y encriptación. Algunas CA, como la CA de Windows, solo admiten encriptación o firma, pero no ambas al mismo tiempo.

Claves de diccionario SubjectAltName

El contenido SCEP puede especificar un diccionario SubjectAltName opcional que proporciona valores requeridos por la CA para emitir un certificado. Puede especificar una sola cadena de caracteres o una matriz de cadenas para cada clave. Los valores que especifique dependerán de la CA que esté utilizando, pero deberían incluir valores como el nombre DNS, la URL o el correo electrónico. Para ver un ejemplo, consulte "Ejemplo de respuesta del servidor con especificaciones SCEP (fase 3)" en la página 93.

Claves de diccionario GetCACaps

Si añade un diccionario con la clave GetCACaps, el dispositivo utilizará las cadenas de caracteres que le proporcione como fuente autorizada de información sobre las prestaciones de su CA. En caso contrario, el dispositivo solicitará el GetCACaps a la CA y utilizará la respuesta que reciba. Si la CA no responde, el dispositivo usará por omisión peticiones GET 3DES y SHA-1.

Contenido APN

El contenido APN (Nombre de Punto de Acceso) se designa mediante el valor PayloadType de com.apple.apn.managed. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
DefaultsData	Diccionario, obligatorio. Este diccionario contiene dos pares clave/valor.
DefaultsDomainName	Secuencia de caracteres, obligatoria. El único valor permitido es com.apple.managedCarrier.
apns	Matriz, obligatoria. Esta matriz contiene un número arbitrario de diccionarios, cada uno de los cuales describe una configuración APN con los siguientes pares clave/valor.
apn	Secuencia de caracteres, obligatoria. Esta secuencia especifica el Nombre de Punto de Acceso (APN).
username	Secuencia de caracteres, obligatoria. Esta secuencia de caracteres especifica el nombre de usuario de este APN. Si no se indica, el dispositivo lo solicita durante la instalación del perfil.
contraseña	Dato, opcional. Este dato representa la contraseña del usuario para este APN. Está codificado por motivos de seguridad. Si no se indica, el dispositivo lo solicita durante la instalación del perfil.
proxy	Secuencia de caracteres, opcional. La dirección IP o la URL del proxy APN.
proxyPort	Número, opcional. El número de puerto del proxy APN.

Contenido de Exchange

El contenido de Exchange se designa mediante el valor PayloadType de com.apple.eas.account. Este contenido crea una cuenta de Microsoft Exchange en el dispositivo. Además de los ajustes comunes a todos los contenidos, este define lo siguiente:

Clave	Valor
EmailAddress	Secuencia de caracteres, obligatoria. Si no está presente en el contenido, el dispositivo solicita esta secuencia durante la instalación del perfil. Especifica la dirección de correo electrónico completa de la cuenta.
Host	Secuencia de caracteres, obligatoria. Especifica el nombre (o la dirección IP) del servidor Exchange.
SSL	Booleano, opcional. Por omisión, YES. Especifica si el servidor Exchange utiliza SSL para la autenticación.
username	Secuencia de caracteres, obligatoria. Esta secuencia especifica el nombre de usuario de esta cuenta Exchange. Si no está indicada, los dispositivos la solicitan durante la instalación del perfil.

Clave	Valor
Contraseña	Secuencia de caracteres, opcional. La contraseña de la cuenta. Solo se puede usar con perfiles encriptados.
Certificado	Opcional. Para la cuentas que admiten autenticación mediante certificado, un certificado de identidad .p12 en formato blob NSData.
CertificateName	Secuencia de caracteres, opcional. Especifica el nombre o la descripción del certificado.
CertificatePassword	Opcional. La contraseña necesaria para el certificado de identidad p12. Solo se puede usar con perfiles encriptados.

Contenido VPN

El contenido VPN se designa mediante el valor PayloadType de com.apple.vpn.managed. Además de los ajustes comunes a todos los tipos de contenido, este define las siguientes claves.

Clave	Valor
UserDefinedName	Secuencia de caracteres. Descripción de la conexión VPN mostrada en el dispositivo.
OverridePrimary	Booleano. Especifica si se envía todo el tráfico a la interfaz VPN. Si es cierto, todo el tráfico de la red se envía a VPN.
VPNType	Secuencia de caracteres. Determina los ajustes disponibles en el contenido para este tipo de conexión VPN. Puede adoptar tres posibles valores: "L2TP", "PPTP" o "IPsec", que representan a L2TP, PPTP y Cisco IPsec, respectivamente.

Puede haber dos diccionarios en el nivel superior, bajo las claves PPP e IPsec. Las claves contenidas en estos dos diccionarios se describen a continuación, junto al valor VPNType en el que se emplean.

Claves de diccionario PPP

Los siguientes elementos se emplean para los contenidos VPN de tipo PPP.

Clave	Valor
AuthName	Secuencia de caracteres. El nombre de usuario de la cuenta VPN. Se emplea para L2TP y PPTP.
AuthPassword	Secuencia de caracteres, opcional. Visible solo si TokenCard es falso. Se emplea para L2TP y PPTP.
TokenCard	Booleano. Indica si se utiliza un elemento para la conexión, como una tarjeta RSA SecurID. Se emplea para L2TP.
CommRemoteAddress	Secuencia de caracteres. Dirección IP o nombre de usuario del servidor VPN. Se emplea para L2TP y PPTP.

Clave	Valor
AuthEAPPlugins	Matriz. Solo está presente si se utiliza RSA SecurID, en cuyo caso tiene una única entrada, que es una secuencia de caracteres con el valor "EAP-RSA". Se emplea para L2TP y PPTP.
AuthProtocol	Matriz. Solo está presente si se utiliza RSA SecurID, en cuyo caso tiene una única entrada, que es una secuencia de caracteres con el valor "EAP". Se emplea para L2TP y PPTP.
CCPMPPE40Enabled	Booleano. Véanse los comentarios de CCPEnabled. Se emplea para PPTP.
CCPMPPE128Enabled	Booleano. Véanse los comentarios de CCPEnabled. Se emplea para PPTP.
CCPEnabled	Booleano. Activa la encriptación de la conexión. Si esta clave y CCPMPPE40Enabled son verdaderas, el nivel de encriptación es automático; si esta clave y CCPMPPE128Enabled son verdaderas, el nivel de encriptación es máximo. Si no se utiliza encriptación, ninguna de las dos claves CCP es verdadera. Se emplea para PPTP.

Claves de diccionario IPsec

Los siguientes elementos se emplean para los contenidos VPN de tipo IPsec.

Clave	Valor
RemoteAddress	Secuencia de caracteres. Dirección IP o nombre de usuario del servidor VPN. Se emplea para Cisco IPsec.
AuthenticationMethod	Secuencia de caracteres. "SharedSecret" o "Certificate". Se emplea para L2TP y Cisco IPsec.
XAuthName	Secuencia de caracteres. Nombre de usuario de la cuenta VPN. Se emplea para Cisco IPsec.
XAuthEnabled	Entero. 1 si XAUTH está activado, 0 si está desactivado. Se emplea para Cisco IPsec.
LocalIdentifier	Secuencia de caracteres. Solo está presente si AuthenticationMethod = SharedSecret. El nombre del grupo a utilizar. Si se utiliza autenticación híbrida, la secuencia debe terminar con "[hybrid]". Se emplea para Cisco IPsec.
LocalIdentifierType	Secuencia de caracteres. Solo está presente si AuthenticationMethod = SharedSecret. El valor es "KeyID". Se emplea para L2TP y Cisco IPsec.
SharedSecret	Dato. El secreto compartido de esta cuenta VPN. Solo está presente si AuthenticationMethod = SharedSecret. Se emplea para L2TP y Cisco IPsec.
PayloadCertificateUUID	Secuencia de caracteres. El UUID del certificado a utilizar para las credenciales de cuenta. Solo está presente si AuthenticationMethod = Certificate. Se emplea para Cisco IPsec.
PromptForVPNPIN	Booleano. Indica si se solicita un PIN al conectarse. Se emplea para Cisco IPsec.

Contenido Wi-Fi

El contenido Wi-Fi se designa mediante el valor PayloadType de com.apple.wifi.managed. Esto describe la versión 0 del valor PayloadVersion. Además de los ajustes comunes a todos los tipos de contenido, este define las siguientes claves.

Clave	Valor
SSID_STR	Secuencia de caracteres. SSID de la red Wi-Fi que se va a utilizar.
HIDDEN_NETWORK	Booleano. Además de SSID, el dispositivo utiliza información como el tipo de emisión y el tipo de encriptación para diferenciar una red. Por omisión, se considera que todas las redes configuradas son abiertas o emisoras. Para especificar una red oculta, debe incluir un valor booleano para la clave "HIDDEN_NETWORK".
EncryptionType	Secuencia de caracteres. Los posibles valores de EncryptionType son "WEP", "WPA" y "Any". "WPA" corresponde a WPA y WPA2 y se aplica a ambos tipos de encriptación. Asegúrese de que estos valores concuerden exactamente con las características del punto de acceso a la red. Si no está seguro del tipo de encriptación, o si prefiere que se aplique a todos los tipos de encriptación, utilice el valor "Any".
Contraseña	Secuencia de caracteres, opcional. La ausencia de contraseña no impide que la red se añada a la lista de redes conocidas. Al conectarse a esa red, se solicitará al usuario que introduzca la contraseña.

Para las redes 802.1X de empresa debe proporcionarse el diccionario de configuración del cliente EAP.

Diccionario EAPClientConfiguration

Además de los tipos de encriptación estándar, es posible especificar un perfil de empresa para una red dada mediante la clave "EAPClientConfiguration". Si está presente, su valor es un diccionario con las siguientes claves.

Clave	Valor
username	Secuencia de caracteres, opcional. Salvo que conozca el nombre de usuario exacto, esta propiedad no aparecerá en una configuración importada. El usuario puede introducir esta información al autenticar.
AcceptEAPTypes	Matriz de valores enteros. Se aceptan los siguientes tipos EAP: 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST

Clave	Valor
PayloadCertificateAnchorUUID	Matriz de secuencias de caracteres, opcional. Identifica los certificados de confianza para esta autenticación. Todas las entradas deben contener el UUID del contenido de un certificado. Utilice esta clave para evitar que el dispositivo pregunte al usuario si los certificados de la lista son de confianza. La confianza dinámica (el cuadro de diálogo del certificado) se desactiva al especificar esta propiedad, salvo que TLSAllowTrustExceptions también se haya ajustado como verdadero.
TLSTrustedServerNames	Matriz de secuencias de caracteres, opcional. Esta es la lista de nombres comunes de certificado de servidor que se aceptarán. Puede utilizar comodines para especificar el nombre, como en "wpa.*.ejemplo.com". Si un servidor presenta un certificado que no está en esta lista, no se confiará en él. Sola o en combinación con TLSTrustedCertificates, esta propiedad permite determinar cuidadosamente en qué certificados se confiará en una red dada, evitándose la confirmación dinámica de confianza. La confianza dinámica (el cuadro de diálogo del certificado) se desactiva al especificar esta propiedad, salvo que TLSAllowTrustExceptions también se haya ajustado como verdadero.
TLSAllowTrustExceptions	Booleano, opcional. Permite o impide que el usuario decida una solicitud dinámica de confianza. La solicitud dinámica de confianza es el cuadro de diálogo que aparece cuando un certificado no es de confianza. Cuando el valor es falso, la autenticación falla si el certificado no es de confianza. Véanse PayloadCertificateAnchorUUID y TLSTrustedNames más arriba. El valor por omisión de esta propiedad es verdadero salvo que se especifique PayloadCertificateAnchorUUID o TLSTrustedServerNames, en cuyo caso el valor por omisión es falso.
TTLSInnerAuthentication	Secuencia de caracteres, opcional. Esta es la autenticación interna empleada por el módulo TTLS. El valor por omisión es "MSCHAPv2". Los posibles valores son "PAP", "CHAP", "MSCHAP" y "MSCHAPv2".
OuterIdentity	Secuencia de caracteres, opcional. Esta clave solo es relevante para TTLS, PEAP y EAP-FAST. Permite al usuario ocultar su identidad. El nombre real del usuario solo aparecerá dentro del túnel encriptado. Por ejemplo, puede ajustarse a "anónimo" o "anon", o a "anon@miempresa.net". Esto aumenta la seguridad porque un atacante verá cifrado el nombre del usuario que se autentica.

Soporte EAP-Fast

El módulo EAP-FAST utiliza las siguientes propiedades en el diccionario EAPClientConfiguration.

Clave	Valor
EAPFASTUsePAC	Booleano, opcional.
EAPFASTProvisionPAC	Booleano, opcional.
EAPFASTProvisionPACAnonymously	Booleano, opcional.

Estas claves son de naturaleza jerárquica: si EAPFASTUsePAC es falso, no se consultarán las otras dos propiedades. Del mismo modo, si EAPFASTProvisionPAC es falso, no se consultará EAPFASTProvisionPACAnonymously.

Si EAPFASTUsePAC es falso, la autenticación procederá de un modo similar a PEAP o TTLS: el servidor proporciona su identidad en cada ocasión mediante un certificado.

Si EAPFASTUsePAC es verdadero, se utilizará un PAC existente, si está presente. Por ahora, el único modo de introducir un PAC en el dispositivo es permitir el suministro de PAC. Por tanto, debe activar EAPFASTProvisionPAC y, si lo desea, EAPFASTProvisionPACAnonymously. EAPFASTProvisionPACAnonymously tiene un problema de seguridad: no autentica el servidor, por lo que las conexiones son vulnerables a un ataque por intermediación de un tercero (MITM).

Certificados

Como sucede en las configuraciones VPN, es posible asociar una configuración de identidad de certificado a una configuración Wi-Fi. Esto resulta muy útil al definir credenciales para una red corporativa segura. Para asociar una identidad, especifique su contenido UUID mediante la clave PayloadCertificateUUID.

Clave	Valor
PayloadCertificateUUID	Secuencia de caracteres. UUID del contenido del certificado a utilizar para la credencial de identidad.

Perfiles de configuración de ejemplo

En este apartado encontrará ejemplos de perfiles que ilustran las fases de registro y configuración remotas. Se trata tan solo de fragmentos, y sus requisitos serán diferentes de los de los ejemplos. Para obtener ayuda con la sintaxis, consulte la información proporcionada anteriormente en este apéndice. Para ver una descripción de cada fase, consulte “Registro y configuración remotos” en la página 25.

Ejemplo de respuesta del servidor (fase 1)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <dict>
        <key>URL</key>
        <string>https://profileserver.example.com/iphone</string>
        <key>DeviceAttributes</key>
        <array>
               <string>UDID</string>
  <string>IMEI</string>
  <string>ICCID</string>
  <string>VERSION</string>
  <string>PRODUCT</string>
        </array>
    <key>Challenge</key>
     <string>optional challenge</string>
     o bien
     <data>base64-encoded</data>
    </dict>
    <key>PayloadOrganization</key>
    <string>Example Inc.</string>
    <key>PayloadDisplayName</key>
    <string>Profile Service</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>fdb376e5-b5bb-4d8c-829e-e90865f990c9</string>
    <key>PayloadIdentifier</key>
    <string>com.example.mobileconfig.profile-service</string>
    <key>PayloadDescription</key>
    <string>Enter device into the Example Inc encrypted profile service</
     string>
    <key>PayloadType</key>
     <string>Profile Service</string>
</dict>
</plist>
```

Ejemplo de respuesta del dispositivo (fase 2)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
```

```
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
    <key>Challenge</key>
o bien:
    <string>String</string>
o bien:
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

Ejemplo de respuesta del servidor con especificaciones SCEP (fase 3)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>Ignored</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadIdentifier</key>
    <string>Ignored</string>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>PayloadContent</key>
        <dict>
          <key>URL</key>
          <string>https://scep.example.com/scep</string>
          <key>Name</key>
          <string>EnrollmentCAInstance</string>
          <key>Subject</key>
          <array>
            <array>
              <array>
                <string>O</string>
                <string>Example, Inc.</string>
              </array>
            </array>
            <array>
              <array>
                <string>CN</string>
                <string>User Device Cert</string>
              </array>
            </array>
```

```
            </array>
            <key>Challenge</key>
            <string>...</string>
            <key>Keysize</key>
            <integer>1024</integer>
            <key>Key Type</key>
            <string>RSA</string>
            <key>Key Usage</key>
            <integer>5</integer>
          </dict>
          <key>PayloadDescription</key>
          <string>Provides device encryption identity</string>
          <key>PayloadUUID</key>
          <string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
          <key>PayloadType</key>
          <string>com.apple.security.scep</string>
          <key>PayloadDisplayName</key>
          <string>Encryption Identity</string>
          <key>PayloadVersion</key>
          <integer>1</integer>
          <key>PayloadOrganization</key>
          <string>Example, Inc.</string>
          <key>PayloadIdentifier</key>
          <string>com.example.profileservice.scep</string>
        </dict>
      </array>
    </dict>
</plist>
```

Ejemplo de respuesta del dispositivo (fase 4)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
</dict>
</plist>
```

Scripts de ejemplo

En este apéndice se proporcionan scripts de ejemplo para tareas de distribución de iPhone OS.

Los scripts de este apartado deberán modificarse para que se adapten a necesidades y configuraciones específicas.

Script de ejemplo C# para la Utilidad Configuración iPhone

Este script de ejemplo crea archivos de configuración mediante la Utilidad Configuración iPhone para Windows.

```
using System;
using Com.Apple.iPCUScripting;

public class TestScript : IScript
  {
  private IApplication _host;

  public TestScript()
     {
     }

  public void main(IApplication inHost)
     {
     _host = inHost;

     string msg = string.Format("# of config profiles : {0}", _host.Configu-
     rationProfiles.Count);
     Console.WriteLine(msg);

     IConfigurationProfile profile = _host.AddConfigurationProfile();
     profile.Name = "Profile Via Script";
     profile.Identifier = "com.example.configviascript";
     profile.Organization = "Example Org";
     profile.Description = "This is a configuration profile created via the
     new scripting feature in iPCU";

     // passcode
     IPasscodePayload passcodePayload = profile.AddPasscodePayload();
```

```
    passcodePayload.PasscodeRequired = true;
    passcodePayload.AllowSimple = true;

    // restrictions
    IRestrictionsPayload restrictionsPayload = profile.AddRestrictionsPa-
    yload();
    restrictionsPayload.AllowYouTube = false;

    // wi-fi
    IWiFiPayload wifiPayload = profile.AddWiFiPayload();
    wifiPayload.ServiceSetIdentifier = "Example Wi-Fi";
    wifiPayload.EncryptionType = WirelessEncryptionType.WPA;
    wifiPayload.Password = "password";

    wifiPayload = profile.AddWiFiPayload();
    profile.RemoveWiFiPayload(wifiPayload);

    // vpn
    IVPNPayload vpnPayload = profile.AddVPNPayload();
    vpnPayload.ConnectionName = "Example VPN Connection";

    vpnPayload = profile.AddVPNPayload();
    profile.RemoveVPNPayload(vpnPayload);

    // email
    IEmailPayload emailPayload = profile.AddEmailPayload();
    emailPayload.AccountDescription = "Email Account 1 Via Scripting";

    emailPayload = profile.AddEmailPayload();
    emailPayload.AccountDescription = "Email Account 2 Via Scripting";

    // exchange
    IExchangePayload exchangePayload = profile.AddExchangePayload();
    exchangePayload.AccountName = "ExchangePayloadAccount";

    // ldap
    ILDAPPayload ldapPayload = profile.AddLDAPPayload();
    ldapPayload.Description = "LDAP Account 1 Via Scripting";

    ldapPayload = profile.AddLDAPPayload();
    ldapPayload.Description = "LDAP Account 2 Via Scripting";

    // webclip
    IWebClipPayload wcPayload = profile.AddWebClipPayload();
    wcPayload.Label = "Web Clip 1 Via Scripting";

    wcPayload = profile.AddWebClipPayload();
    wcPayload.Label = "Web Clip 2 Via Scripting";

    }
}
```

Script de ejemplo de AppleScript para la Utilidad Configuración iPhone

Este script de ejemplo crea archivos de configuración mediante la Utilidad Configuración iPhone para Mac OS X.

```
tell application "iPhone Configuration Utility"
  log (count of every configuration profile)
  set theProfile to make new configuration profile with properties {displa-
     yed name:"Profile Via Script", profile identifier:"com.example.confi-
     gviascript", organization:"Example Org.", account description:"This is
     a configuration profile created via AppleScript"}
  tell theProfile
     make new passcode payload with properties {passcode required:true, sim-
     ple value allowed:true}
     make new restrictions payload with properties {YouTube allowed:false}
     make new WiFi payload with properties {service set identifier:"Example
     Wi-Fi", security type:WPA, password:"password"}
     set theWiFiPayload to make new WiFi payload
     delete theWiFiPayload
     make new VPN payload with properties {connection name:"Example VPN Con-
     nection"}
     set theVPNPayload to make new VPN payload
     delete theVPNPayload
     make new email payload with properties {account description:"Email
     Account 1 Via Scripting"}
     make new email payload with properties {account description:"Email
     Account 2 Via Scripting"}
     make new Exchange ActiveSync payload with properties {account
     name:"ExchangePayloadAccount"}
     make new LDAP payload with properties {account description:"LDAP
     Account 1 Via Scripting"}
     make new LDAP payload with properties {account description:"LDAP
     Account 2 Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 1
     Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 2
     Via Scripting"}
  end tell
end tell
```