

Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Propuesta de Trabajo Final

Tema:

Seguridad de sistemas operativos Apple

Título:

Aplicación de políticas de seguridad corporativas sobre dispositivos con iOS o Mac OSX en organizaciones financieras

Autor Lic. Rodrigo Manuel Sánchez Rivera

Año 2012

Cohorte 2012

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Resumen

Este trabajo aspira a reunir diversos conocimientos que puedan obrar de guía de buenas prácticas para proteger dispositivos con sistema operativo Apple que son utilizados dentro de las empresas.

Ya sea en equipos portátiles Macbook o bien en los nuevos dispositivos móviles iOS, se crea un nuevo punto de conflicto a resolver por los expertos y responsables de la seguridad.

Siguiendo e implementando los consejos a lo largo del trabajo se logrará mantener un equilibrio que permita un máximo posible de seguridad, de protección de la información y de los recursos de la organización sin castigar de sobremanera las funciones y utilidades que en cada caso brindan los equipos y dispositivos que tanto potencial poseen.

INDICE

Declaración Jurada de origen de los contenidos.....	1
Resumen.....	2
INDICE	3
<i>CAPITULO PRIMERO</i>	5
1- Mac OSX (sistema operativo de equipos MacBook Pro y MacBook Air).....	5
1.1- Ingresando la MacBook al dominio Active Directory utilizando el cliente nativo.....	6
1.2.1- Open Directory.....	9
1.2.2- Centrify for Mac OSX.....	11
1.2.2.1- Instalación.....	14
1.2.3- ADmitMac v7	29
1.2.3.1- Instalación.....	30
1.2.4- Authentication Services	34
1.2.4.1- Instalación.....	35
1.2.5- PowerBroker Identity Services Open for "AD Bridge"	38
1.2.5.1- Instalación.....	39
1.3- Antivirus	43
1.4- Cifrado del disco rígido.....	46
1.4.1- McAfee Endpoint Encryption.....	47
1.4.2- FileVault (Aplicación nativa).....	50
1.4.2.1- Eliminar el almacenamiento de clave en Suspensión del equipo	54
<i>CAPITULO SEGUNDO</i>	56
2- iOS (Sistema Operativo de dispositivos iPhone, iPod Touch y iPad).....	56

2.1- Apple Configurator configuración.....	58
3- Conclusión	71
Bibliografía Inicial	76
Referencias.....	76
Otras referencias y manuales:	78

CAPITULO PRIMERO

1- Mac OSX (sistema operativo de equipos MacBook Pro y MacBook Air)

¿Qué debe tener?

La creciente popularidad de los equipos Apple por su gran desempeño y estabilidad sumado a su diseño ha logrado que muchas organizaciones se decidan a integrar dentro de su parque informático equipos móviles MacBook generalmente para los niveles de máxima jerarquía.

Justamente estos niveles jerárquicos manejan información de suma importancia y gran criticidad para las organizaciones siendo puntos claves para mantener protegidos de la mejor manera posible equilibrando la operatividad con las máximas restricciones y cuidados.

Existen varios aspectos técnicos a tener en cuenta para la integración y protección que se detallarán en las próximas páginas.

Para utilizar un equipo portátil MacBook con SO Mac OSX dentro de una red Microsoft (que es lo que generalmente las organizaciones utilizan como soporte para su infraestructura distribuida de red), es necesario ingresar el equipo dentro del dominio Active Directory para lograr su integración y aprovechar los servicios que brinda como ser la libreta de direcciones, el mail corporativo o utilizar las mismas credenciales que las usadas para acceder a equipos PC por ejemplo.

Al ingresar el equipo al dominio se consigue que el mismo pase a ser un objeto dentro del árbol y ser reconocido por Microsoft Active Directory. Esto último es de importancia para lograr que las políticas de dominio que contienen gran cantidad de las medidas de seguridad que las organizaciones definen para sus equipos, sean plausibles de ser aplicadas en el equipo MacBook.

1.1- Ingresando la MacBook al dominio Active Directory utilizando el cliente nativo

Como primer paso se debe contar en el equipo con una conexión a la red de dominio.

Luego se debe ingresar a las “Preferencias del sistema” y hacer clic en “Usuarios y grupos” [10]:



Imagen 1

Hacer clic en el botón “Acceder...” y a continuación en “Abrir Utilidad de Directorios”

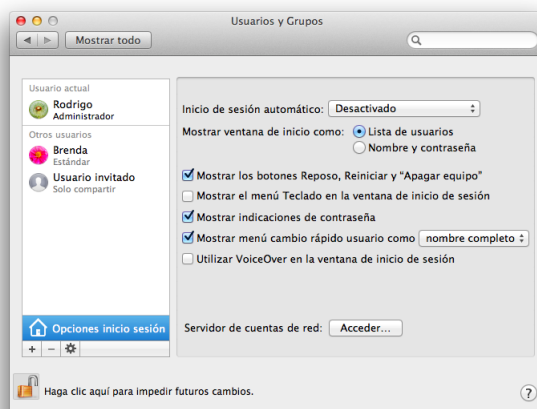


Imagen 2

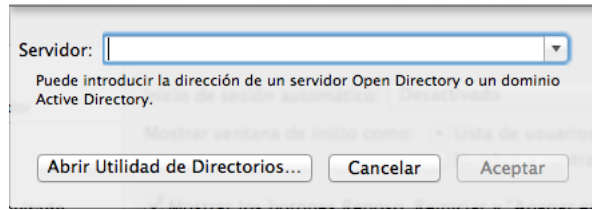


Imagen 3

Seleccionar "Active Directory"

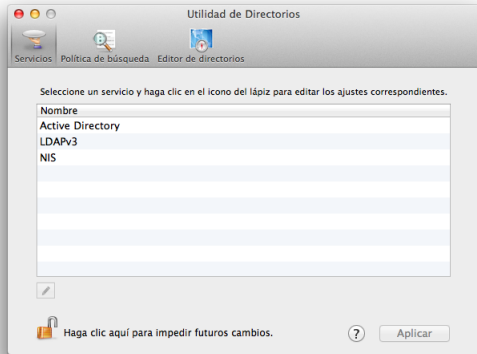


Imagen 4

Ingresar el nombre del dominio en el campo "Dominio de Active Directory" y elegir una denominación adecuada para el equipo MacBook en el campo "ID del ordenador".

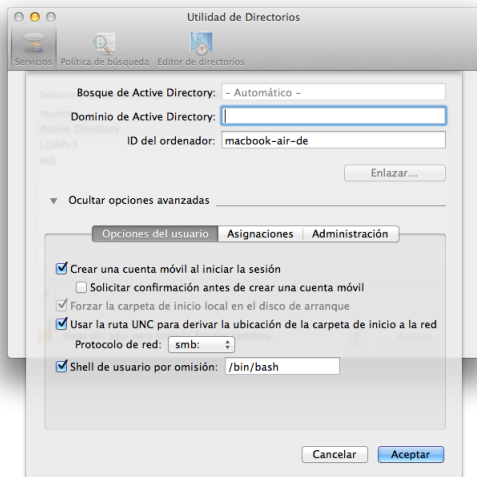


Imagen 5

Es importante seleccionar la casilla de "Crear una cuenta móvil al iniciar la sesión" para que se encuentre disponible la opción de acceso al equipo utilizando las credenciales de dominio aun cuando el equipo no posea conexión a la red.

La principal limitación de este procedimiento es que si bien la MacBook queda vinculada al dominio como un objeto dentro del Active Directory no son aplicadas ninguna de las GPOs (Group Policies Object) con directivas de seguridad definidas.

1.2- Diversas alternativas de integración del equipo MacBook a un Active Directory con la aplicación de políticas

Ya contando con el equipo en dominio el siguiente paso es lograr que las políticas y medidas de seguridad que las organizaciones definen se apliquen de forma automática y centralizada en los equipos MacBook que se encuentren como objetos dentro del dominio.

Existen diversas alternativas entre las cuales se encuentran las que veremos a continuación siendo soluciones recomendadas o bien productos de terceros. De los productos existentes se seleccionaron Open Directory, Centrify, ADmitMac, Authentication Services y Power Broker que se verán a continuación.

1.2.1- Open Directory

De acuerdo a lo recomendado por Apple en su documentación, la alternativa oficial para lograr que las políticas de dominio (conocidas como GPO o Group Policy Object) definidas en el Active Directory (como ser características de fortaleza de clave de acceso u otro tipo de configuraciones que es posible configurar) sea aplicado en los equipos MacBook es utilizando el software Open Directory que genera el “triángulo dorado” [10] [11].

La solución necesita la instalación y configuración de Open Directory software que se comunica con el Active Directory de Microsoft y envía a los clientes MacBook las políticas de dominio.

Las ventajas de realizar la instalación de esta solución es que es gratuita y posee documentación oficial de Apple donde se describe a todo detalle cómo realizar la instalación como así también la configuración necesaria para los diversos servicios de directorios existentes en el mercado.

Como desventajas encontramos que es necesario incorporar hardware que aloje el Open Directory, suma carga administrativa dado que se debe configurar y mantener un nuevo servicio de directorio y la desventaja más importante implica que es necesaria la modificación del esquema del Active Directory, tarea que se debe realizar con permisos específicos y con los riesgos que siempre conlleva el modificar una configuración al dominio.

Exponemos la opción para que sea una posibilidad solamente si el costo beneficio lo amerite y dado que es la alternativa oficial propuesta por Apple. Es de gran complejidad la instalación dado que es necesario instalar otro contenedor de usuarios y relacionarlo con el Active Directory no siendo la alternativa recomendada sobre todo si en la organización se poseen pocos

equipos MacBook dado que la administración sería sumamente costosa al no ser a escala.

Igualmente todos los detalles para la instalación de esta alternativa se encuentran en la documentación de Apple llamada “Best Practices for Integrating OS X with Active Directory” [10]

1.2.2- Centrify for Mac OSX

Una de las alternativas mencionada en la documentación de Apple como solución de terceros es el producto Centrify for Mac OS X de la firma Centrify Corporation.

La solución permite controlar la integración de equipos MacBook al dominio Active Directory destacando los siguientes beneficios [12]:

- Manejar de forma centralizada el Single Sign On de usuarios MacBook al Active Directory sin la necesidad de la creación de usuarios locales.
- Limitar con la herramienta "DirectControl's" los usuarios que necesiten realmente acceder a los equipos MacBook.
- Delegar la administración de sistemas MacBook sin otorgar privilegios a otros sistemas.
- Generar reportes con la herramienta "DirectControl's" para que los entes de control verifiquen los accesos otorgados.
- Forzar la aplicación de políticas de clave definidas en el Active Directory independientemente de que usuarios utilizarán el equipo.
- Manejar un nivel criptográfico de excelente calidad que ha sido galardonado por agencias de Estados Unidos y Canadá.

Como principales aspectos que son posibles configurar bajando desde las políticas de dominio encontramos que la herramienta permite:

Principales configuraciones de equipo permitidas:

Solicitar clave ante cambios en cada preferencia del sistema.

Deshabilitar el ingreso (login) automático.

Utilizar memoria virtual segura.

Solicitar credenciales una vez transcurridos una cantidad de minutos de inactividad.

Habilitar la utilización de "Smart card".

Solicitar el ingreso por medio del uso de "Smart card".

Configuraciones de seguridad del cortafuegos.

Habilitación del cortafuegos y configuración por servicios.

Bloqueo de tráfico UDP (user datagram protocol).

Configuración de dominios de búsqueda y servidores DNS.

Habilitación y configuración de Proxies.

Habilitación del registro de actividad de Firewall.

Deshabilitar todo compartimiento de Internet.

Habilitar el modo sigiloso de Firewall.

Mostrar los botones de "Restart, Sleep y Shutdown".

Ajustar la visualización de anuncios.

Controlar la ventana de inicio de sesión para mostrar ya sea nombre y contraseña o la lista de usuarios.

Habilitar el intercambio rápido de usuarios.

Configurar los grupos de administración de dominio con los grupos de administración local.

Configurar diferentes configuraciones de ahorro de energía con el equipo conectado a la corriente alterna o funcionando con baterías.

Apagar la pantalla ante inactividad.

Apagar el equipo ante inactividad.

Configurar el bajo consumo del disco duro cuando es posible.

Activar el equipo por medio de eventos del modem, acceso de administradores de redes Ethernet.

Habilitar el botón de reposo del equipo.

Reiniciar el equipo automáticamente ante inconvenientes de energía.

Configuraciones de actualizaciones del sistema operativo.

Principales configuraciones de usuario permitidas:

Controlar el acceso a aplicaciones específicas, incluyendo el Mac App Store.

Controlar el acceso a las herramientas y utilidades de UNIX.

Aplicar protector de pantalla.

Tiempo de espera de ahorro de energía.

Tamaño de la barra de programas “Dock”, ampliación y posición en la pantalla.

Animación para la apertura de la aplicación.

Ocultar automáticamente el Dock.

Definir las aplicaciones de control que aparecen en el Dock.

Bloquear el Dock.

Controlar el acceso a los CD, CD-ROMs y DVDs.

Controlar el acceso a los discos grabables.

Controlar el acceso a los discos externos (incluidos los discos flash USB y el iPod).

Configuración de sincronización de perfiles de movilidad.

Control de sincronización de directorios.

Sincronización de control en conexiones / desconexiones en segundo plano.

Controlar lo que los elementos que se sincronizarán y omitirán.

Solicitar contraseña para reactivar el equipo si está en reposo o con el protector de pantalla.

Habilitación de las actualizaciones automáticas de software.

Especificar el servidor de actualizaciones de software para todas las actualizaciones.

Limitar los elementos que se mostrarán en las Preferencias del Sistema.

Control de visualización de cada elemento en Preferencias del Sistema.

Existe una herramienta para proceder a la instalación de la solución que se denomina “Centrify DirectManage Deployment Manager” que brinda la posibilidad de detectar automáticamente cuando un equipo MacBook se conecta a la red de dominio permitiendo la instalación a distancia. Existe

también la posibilidad de obtener el programa instalador y proceder a instalar manualmente por un administrador si así se desea.

1.2.2.1- Instalación

Descargar el cliente “Centrify Agent for Mac 10.6, 10.7, 10.8” y desde el equipo MacBook contando con un usuario con los privilegios adecuados de administración local se procede a la instalación.

Hacer doble clic en el archivo CentrifyDC-5.1.1-mac10.6.dmg donde se muestra la siguiente pantalla.



Imagen 6

Hacer clic en el icono AD Check.app para realizar la verificación de condiciones necesarias de conexión. Se muestra la siguiente pantalla en la cual hay que indicar el dominio donde se ingresará la MacBook (en el ejemplo el dominio es appplerules.com)

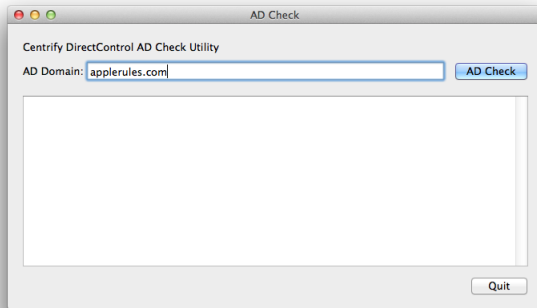


Imagen 7

Al hacer clic en el botón “AD Check” comienza la verificación.

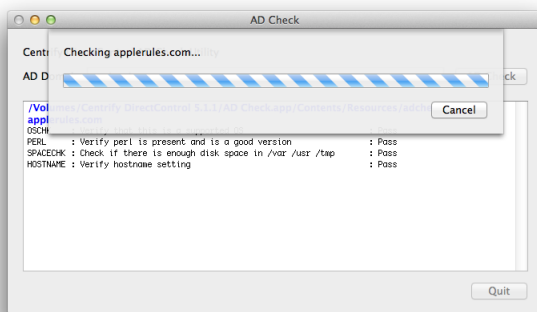


Imagen 8

Tras ejecutar la verificación se presenta la siguiente pantalla donde se observa la batería de chequeos y su resultado.

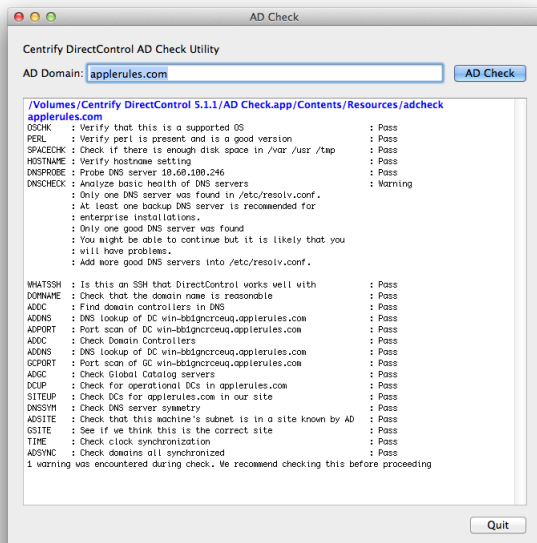


Imagen 9

Una vez realizado el control y que el resultado es satisfactorio se debe proceder a hacer clic en el icono CentriflyDC-5.1.1.pkg que lanza la instalación del producto:

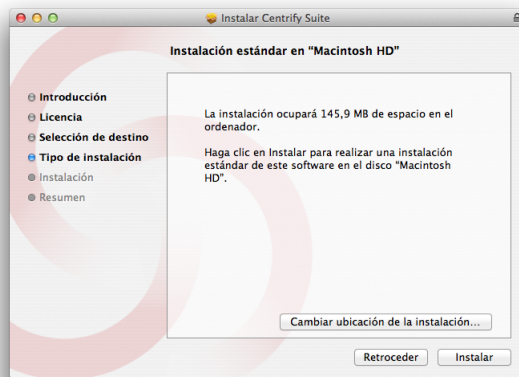


Imagen10

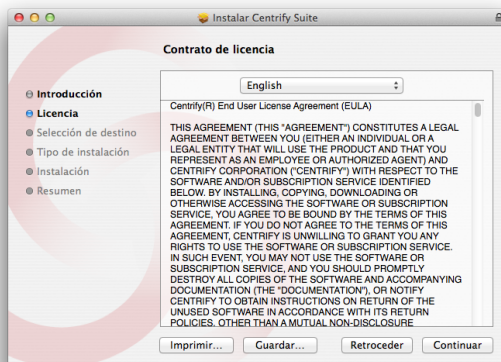


Imagen 11

Se solicitará el ingreso de credenciales del usuario administrador local del equipo MacBook:

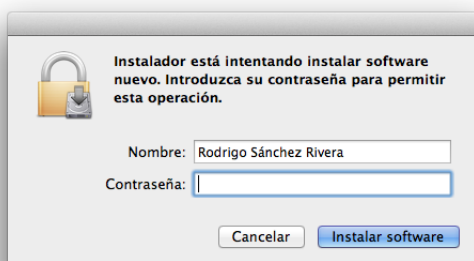


Imagen 12

Tras el ingreso efectivo continúa la instalación y se escriben los archivos en el disco.

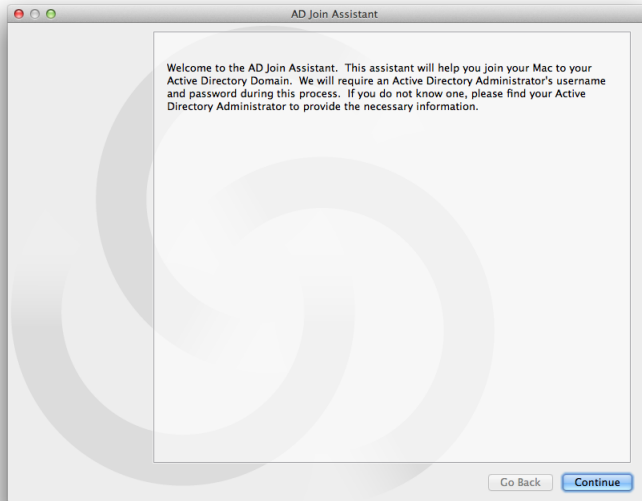


Imagen 13

Al hacer clic en el botón "Continúe" se solicitarán usuario y clave de un administrador del dominio donde se vinculará el equipo MacBook.

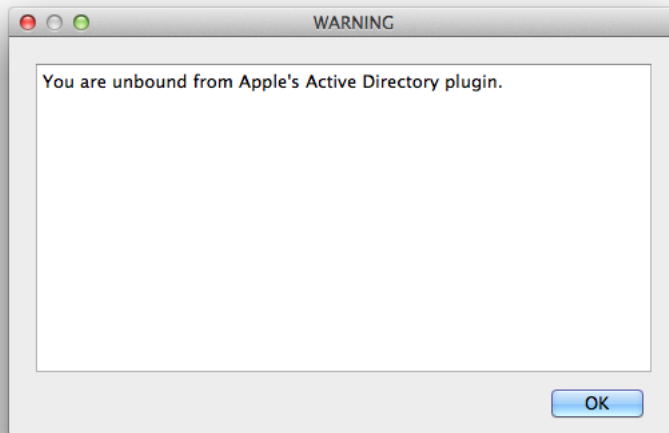


Imagen 14

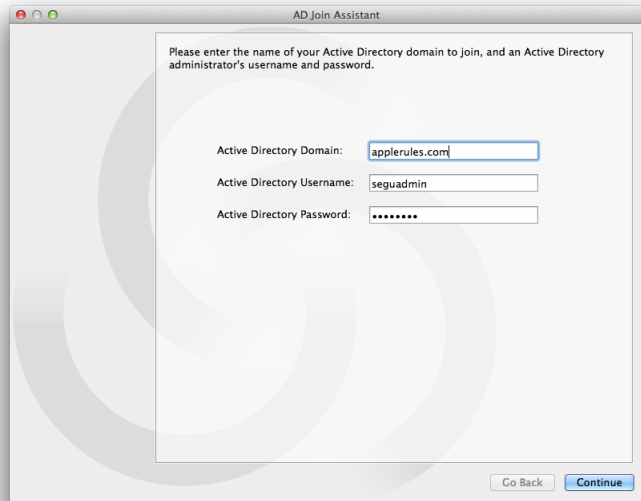


Imagen 15

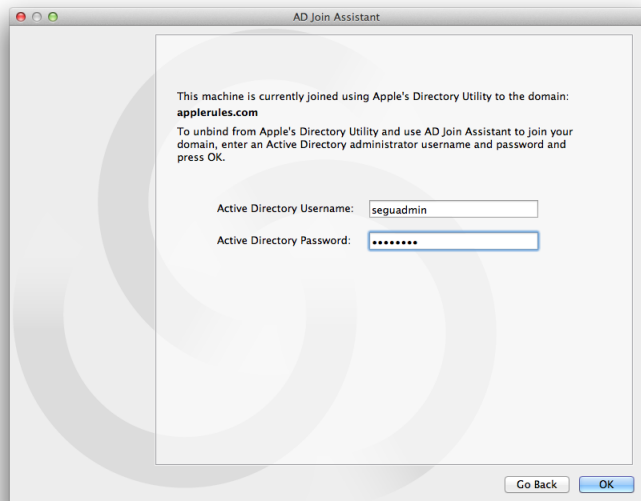


Imagen 16

En la siguiente pantalla se deberá indicar el tipo de instalación seleccionando la opción "Auto". Es posible ya en esta instancia indicar un contenedor LDAP para su orden administrativo marcando la opción "Container DN" y un server Domain Controller que atenderá los requerimientos del equipo en el campo "Preferred Domain Server".

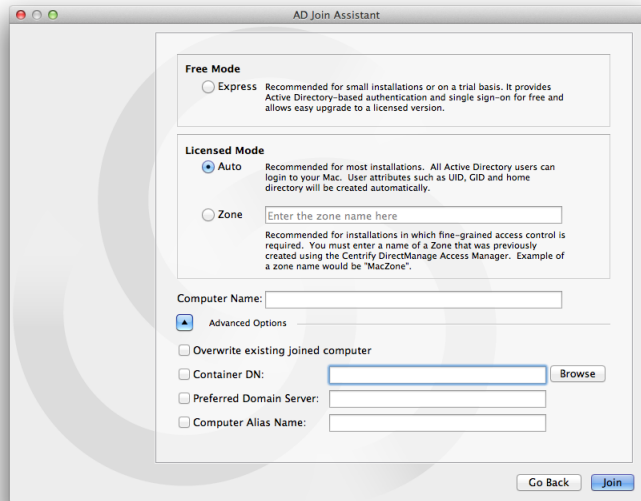


Imagen 17

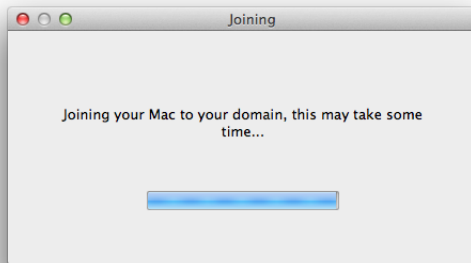


Imagen 18

Tras aguardar unos momentos se mostrará el siguiente mensaje:

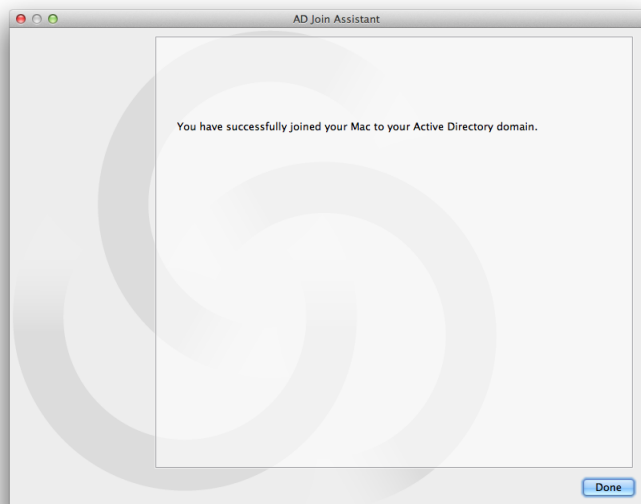


Imagen 19

En esta instancia el equipo MacBook se encuentra dentro del dominio elegido siendo regido por las políticas de dominio (GPOs).

Se pueden observar las opciones del producto instalado desde las Preferencias del Sistema -> Complementos -> Centrify



Imagen 20

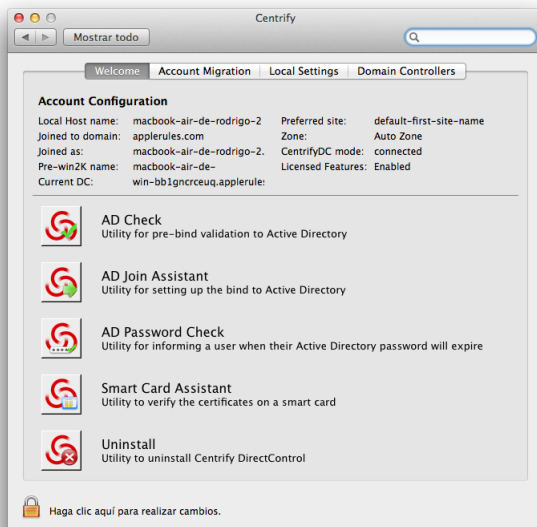


Imagen 21

En las diversas pestañas se pueden configurar la carpeta de Home del usuario:

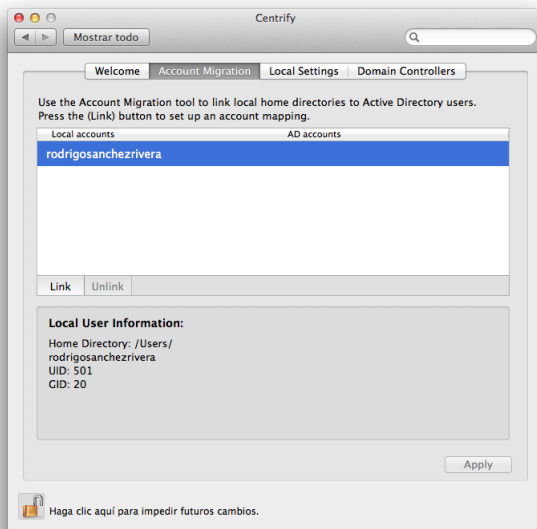


Imagen 22

También es posible indicar el protocolo a ser utilizado en la opción “Network protocol to be used”

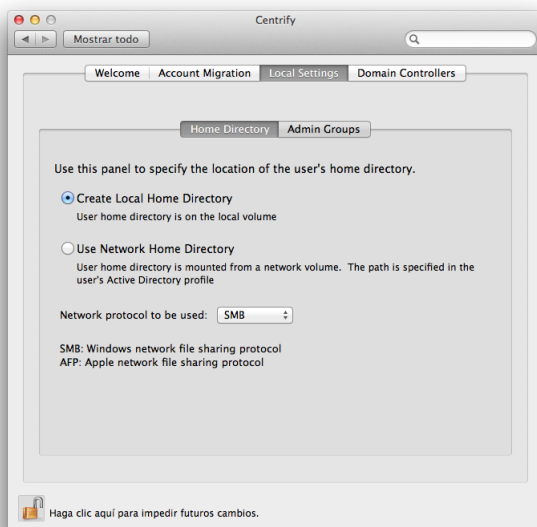


Imagen 23

Así mismo es posible definir los grupos de dominio que serán Administradores locales del equipo MacBook:

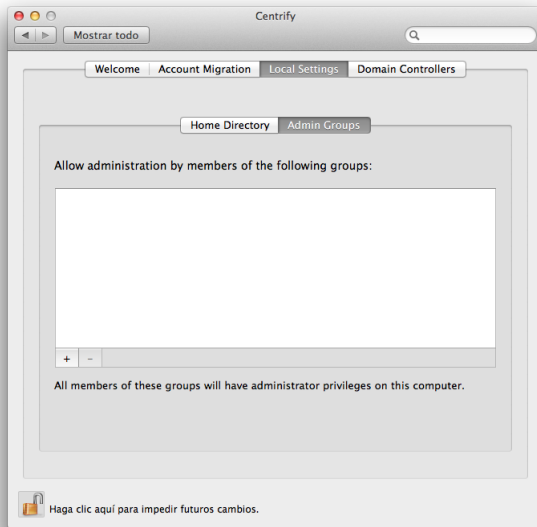


Imagen 24

Y por último indicar las preferencias del servidor Domain Controller que atenderá los requerimientos del equipo MacBook.

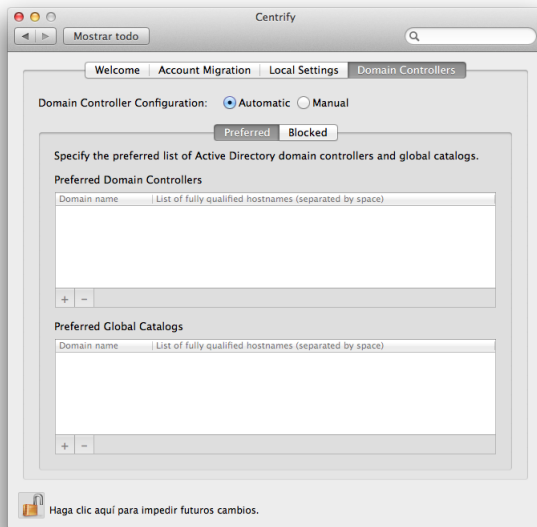


Imagen 25

Una vez que el equipo se encuentra configurado en principio cualquier usuario de dominio podrá iniciar sesión en el mismo. Se puede observar a continuación como se crea la cuenta dentro de la opción Usuarios y Grupos de las Preferencias del Sistema.



Imagen 26

Se puede comprobar también la visibilidad de las carpetas de dominio Netlogon y Sysvol con la información que Microsoft Windows Server comparte en los equipos del dominio con la información de las políticas de grupo.

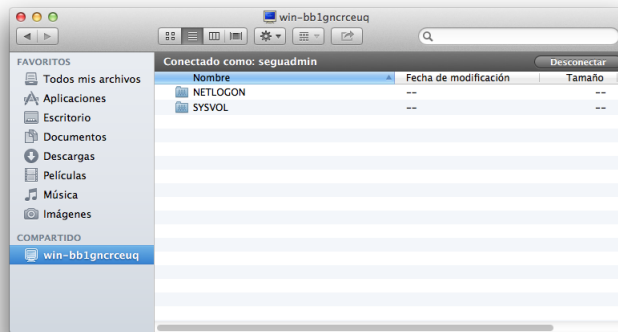


Imagen 27

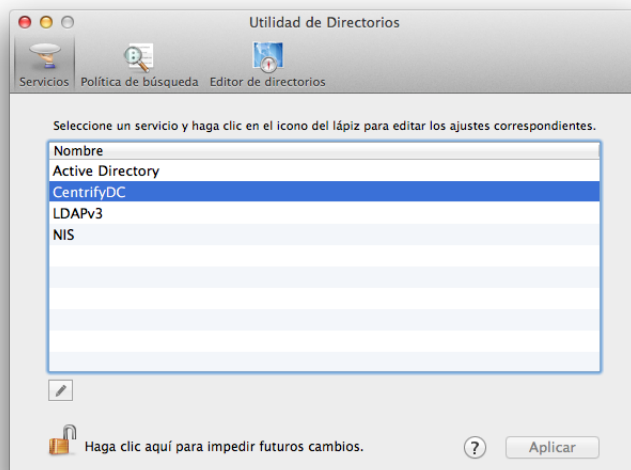


Imagen 28

A modo de ejemplo de la aplicación de la integración con el dominio se procedió a caducar la clave del usuario utilizado (seguadmin) y a continuación se muestra el efecto de la caducidad y solicitud de cambio de clave.

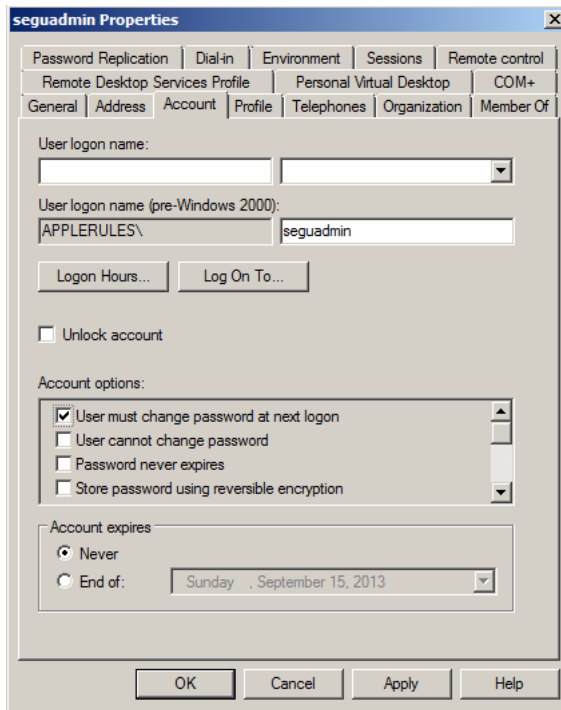


Imagen 29

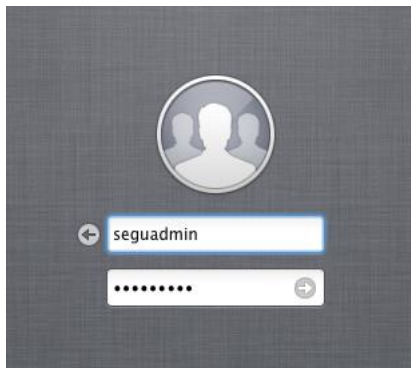


Imagen 30



Imagen 31

De esta manera el equipo MacBook queda bajo la órbita de las políticas de dominio que la organización define sin modificar el esquema del Active Directory u otros componentes internos del dominio.

A continuación se debe descargar el cliente “Centrify DirectManage Express 5.1.1 for 64-bit Windows” y se procede a instalar el mismo en el controlador de dominio donde se contará entonces con la consola de administración centralizada. Se hace clic en el programa [CentrifyDM-5.1.1-win64.exe](#):

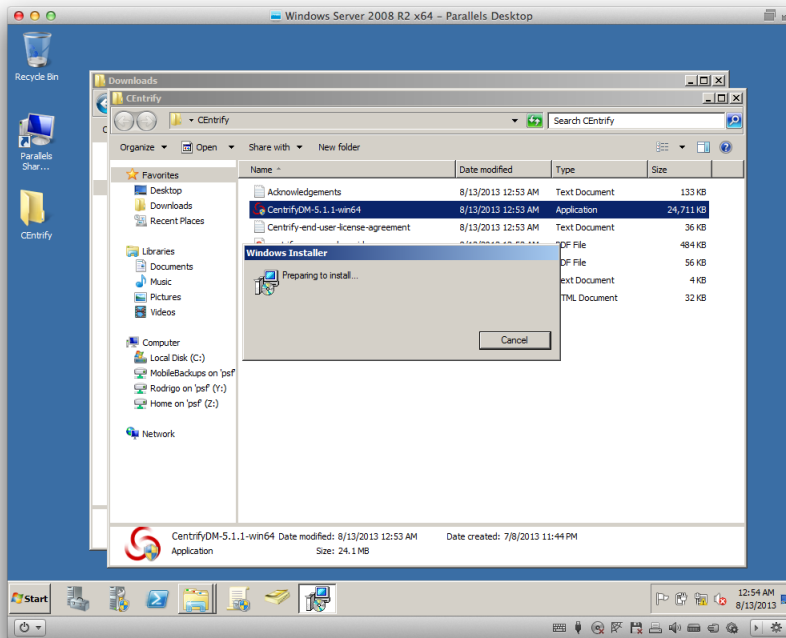


Imagen 32

Haciendo click en el botón siguiente, aceptando los términos de la licencia y eligiendo la carpeta de instalación se procede a completar el proceso:

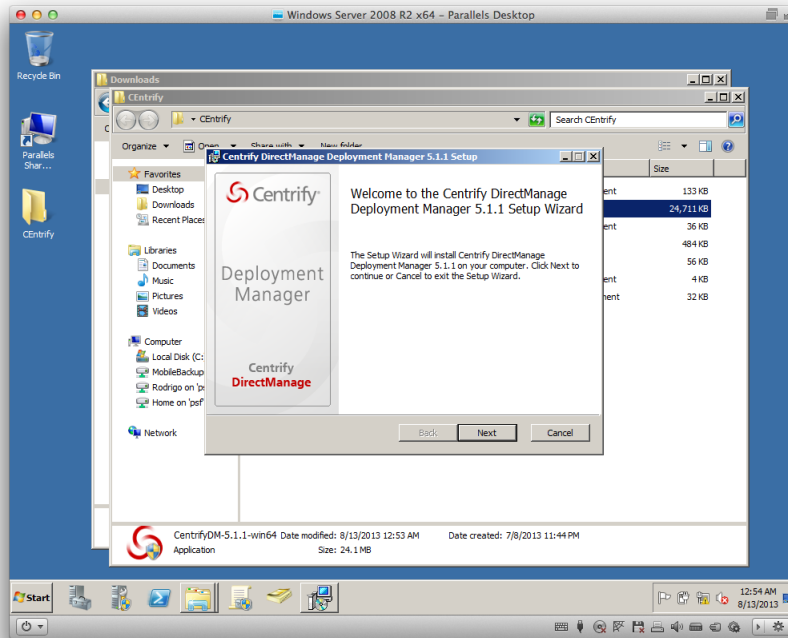


Imagen 34

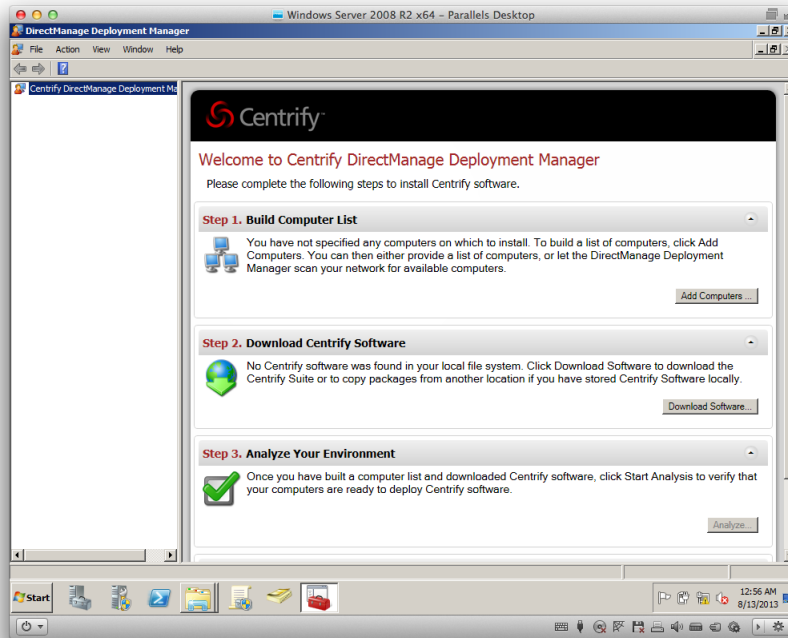


Imagen 35

Haciendo clic en Add Computers del primer paso el software realiza un descubrimiento de la red y localiza los equipos que posean instalado el producto.

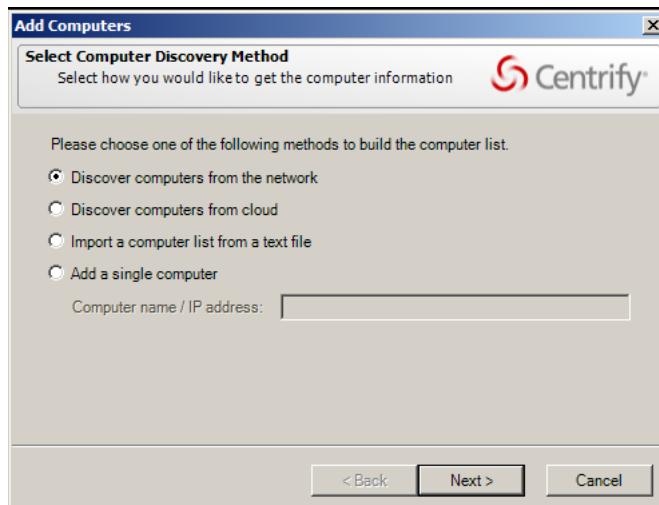


Imagen 36

Al finalizar en la consola centralizada se visualizan los equipos disponibles.

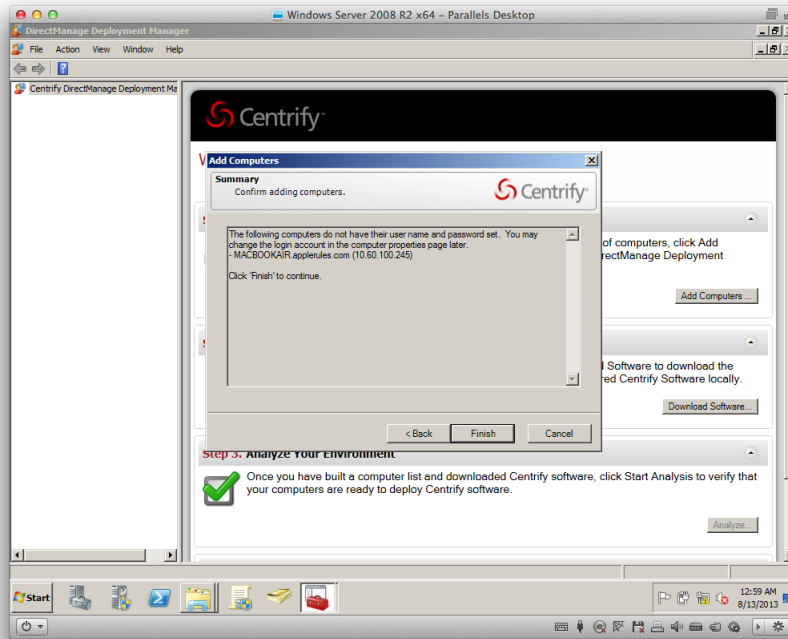


Imagen 37

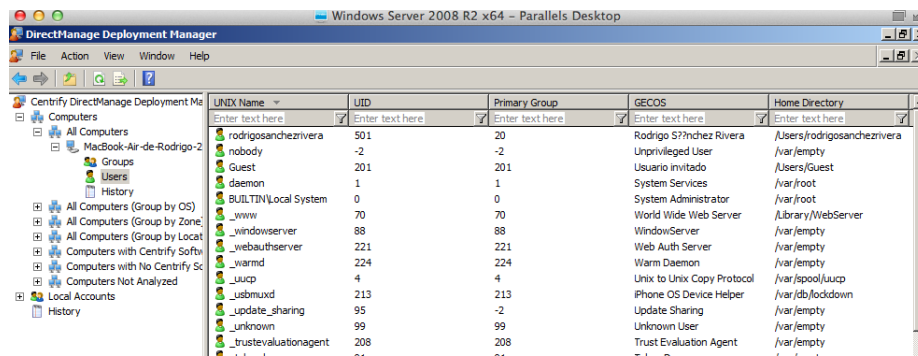


Imagen 38

1.2.3- ADmitMac v7

Otra de las alternativas consideradas en la documentación de Apple es el producto ADmitMac v7 de la firma Thursby Software [13].

La solución también permite transformar el equipo MacBook en un cliente real de Active Directory [14] que se instala directamente en el Mac OSX sin realizar modificaciones sobre el esquema de dominio.

Incluye soporte para acceso a carpetas compartidas Microsoft DSF (Distributed File System), la utilización de Kerberos para la autenticación de usuarios, la utilización de las políticas de dominio (GPO) para la configuración de componentes del sistema, permite la utilización de las impresoras del dominio, configura las restricciones de claves de usuarios definidas, habilita el soporte para formato de archivo NTFS, el manejo de Microsoft Windows ACL (Access Control List), permite utilizar grupos de dominio como administradores locales del equipo, manejo del escritorio personalizado y documentos por usuario que inicie sesión en el equipo, soporta nombres largos de acciones compatibles con Windows 2003 y 2008.

También posee soporte para conexiones bidireccionales con firma SMB, NTLM SSP y NTLMv2. Los administradores de Windows pueden administrar los componentes del sistema operativo Mac y aplicaciones en Active Directory mediante Directiva de grupo. Posee soporte para múltiples dominios de un bosque Active Directory. Soporte de DNS dinámico para registro de los equipos. Con la herramienta "AD Commander" permite a los administradores editar usuarios y grupos como si estuviera utilizando herramientas de administración nativas de Active Directory.

1.2.3.1- Instalación

Descargar el cliente “ADmitMac v7” y desde el equipo MacBook contando con un usuario con los privilegios adecuados de administración local se procede a la instalación [13].

Hacer doble clic en el archivo admitmac70.iso donde se muestra la siguiente pantalla, hacer clic en “Continuar” y luego “Aagree”:

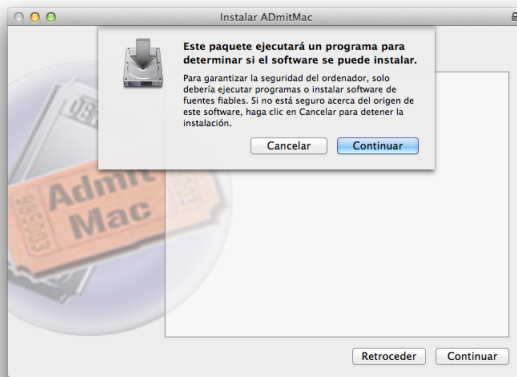


Imagen 38

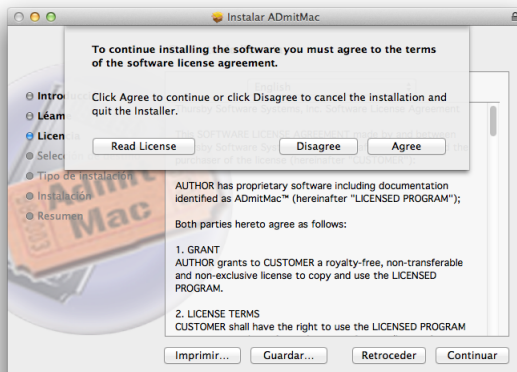


Imagen 39

Una vez finalizada la instalación se solicitaran las credenciales suficientes en el equipo MacBook a fin de modificar los servicios requeridos:

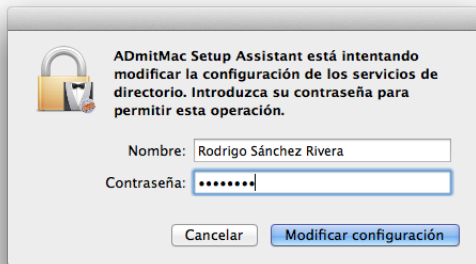


Imagen 40

Al finalizar la instalación de forma automática se lanza el asistente de configuración:



Imagen 41

En la primera pantalla se debe seleccionar “Using DHCP”

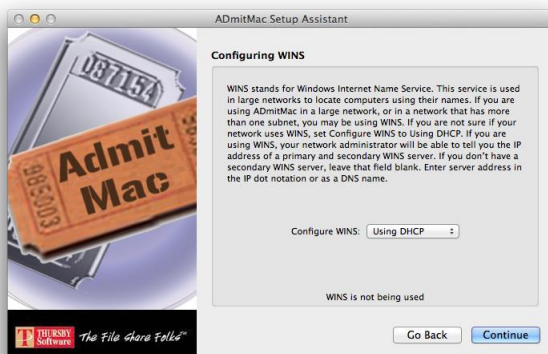


Imagen 42

En segunda instancia se debe indicar el nombre del dominio al cual el equipo va a ser integrado:

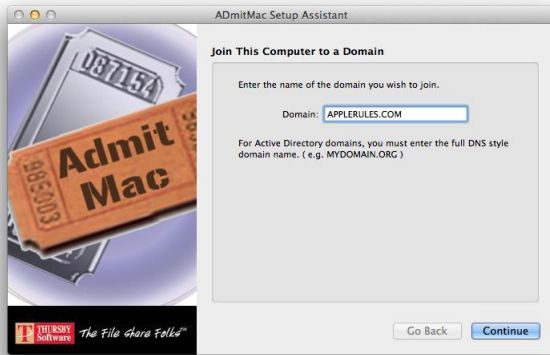


Imagen 43

Luego se deben ingresar el nombre y la ubicación del equipo y se solicitarán las credenciales suficientes del dominio a sumarse.

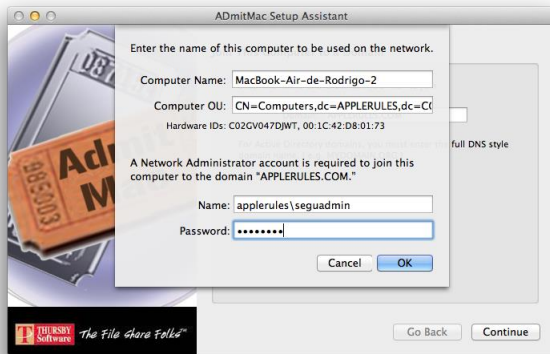


Imagen 44

Por último nuevamente se solicita el nombre del dominio pero en esta oportunidad se debe ingresar solamente el principio del nombre.

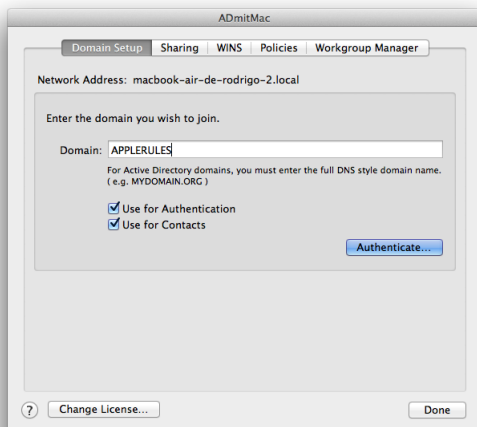


Imagen 45

Se puede observar ya el equipo dentro del dominio.

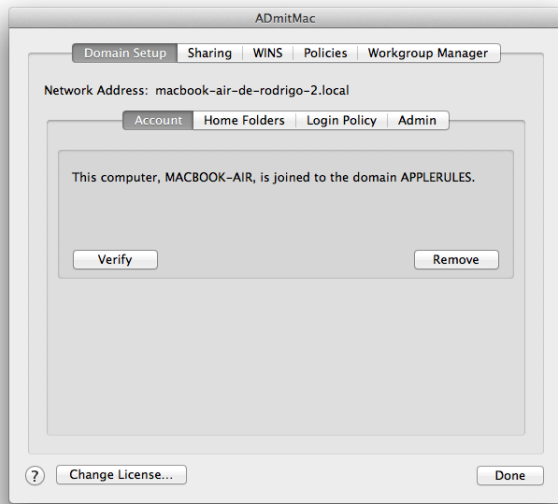


Imagen 46

1.2.4- Authentication Services

La tercera alternativa relevante mencionada en la documentación de Apple sobre soluciones de terceros para la integración de los equipos MacBook al dominio Active Directory es el producto Authentication Services de la firma Dell Inc.

La solución propone como las demás, resolver el inconveniente de administrar las diversas identidades y medidas de seguridad que se enfrenta la organización al tener la infraestructura de la red en entornos Microsoft Windows y ciertos equipos con otros sistemas operativos como ser Mac, Unix, Linux entre otros, con sus correspondientes características de seguridad, organizando y generando participación, integración completa con el Active Directory creando lo que denominan un puente [16].

Principalmente se logra para la organización:

Eficiencia, dado que se achican las identidades, los usuarios en diversos sistemas operativos, siendo más efectiva y ágil la administración.

Seguridad, al extender la autenticación de Kerberos, una fuerte política de claves y el control de acceso de Active Directory aplicado al Mac OSX.

Cumplimiento pues al centralizar la administración de los diversos sistemas operativos utilizando uno único y con gran nivel de seguridad y robustez como es el Active Directory de Microsoft, las políticas internas y regulaciones externas son más fáciles de alcanzar.

1.2.4.1- Instalación

Descargar el cliente “Privileged Access Suite for Unix” y desde el equipo MacBook contando con un usuario con los privilegios adecuados de administración local se procede a la instalación [22].

Hacer doble clic en el archivo VAS-4.1.0.20185.dmg donde se muestra la siguiente pantalla, hacer clic en “Continuar” y luego “Cerrar”:

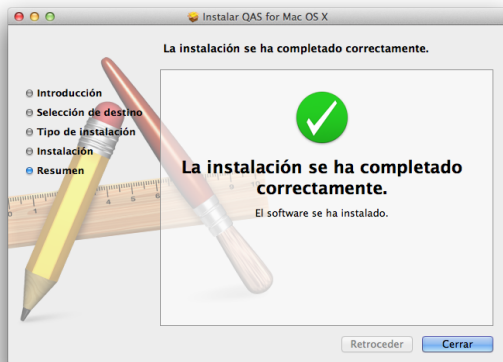


Imagen 47

Una vez finalizada la instalación dirigirse a “Utilidad de directorios” para proceder a la configuración del cliente. Se solicitará un usuario y su clave con los suficientes privilegios del dominio Active Directory donde se desea realizar la integración.

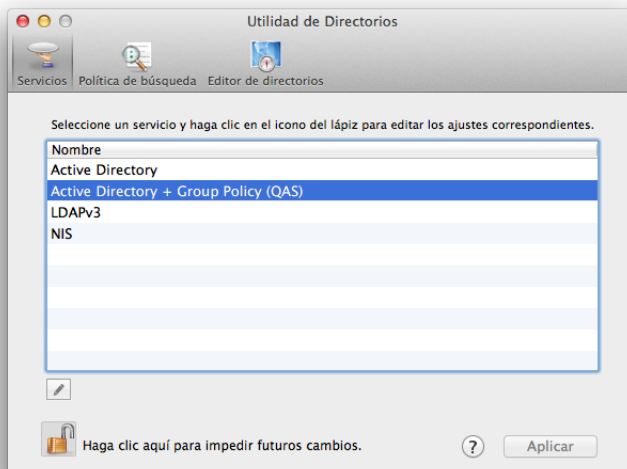


Imagen 48

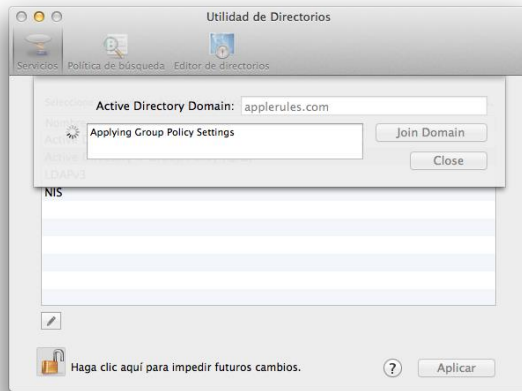


Imagen 49

Una vez que finaliza el proceso se observa el mensaje de bienvenida y el reporte con el detalle del proceso.

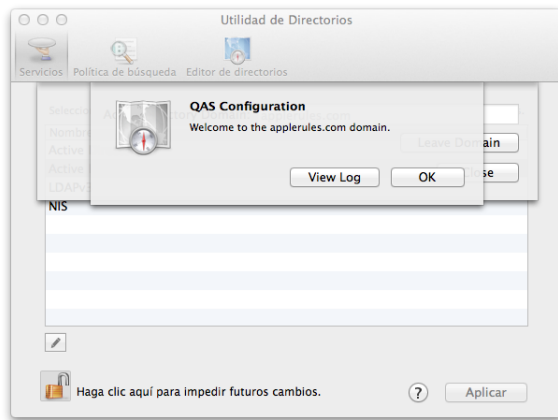


Imagen 50

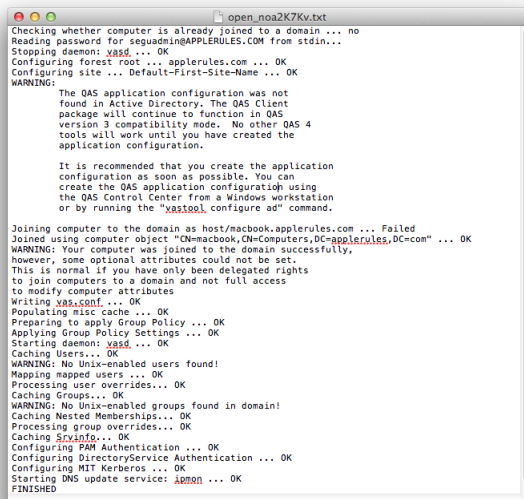


Imagen 51

A modo de ejemplo ya es posible configurar a que usuarios de dominio les será permitido realizar el ingreso en el equipo MacBook

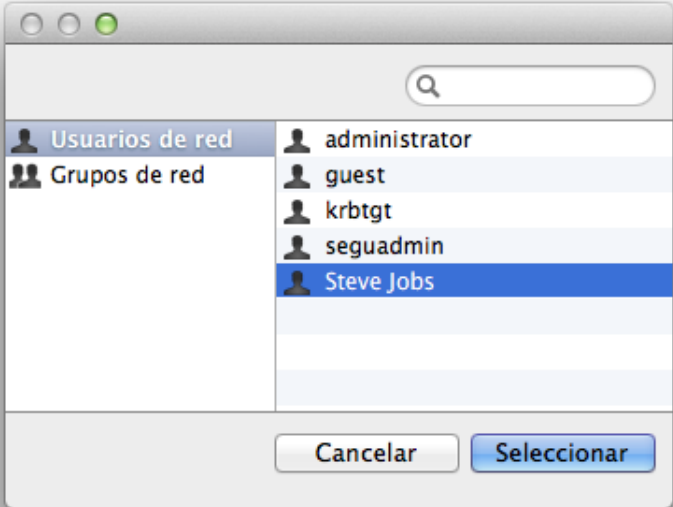


Imagen 52

1.2.5- PowerBroker Identity Services Open for "AD Bridge"

Si bien no es una alternativa recomendada en la documentación oficial, dado su gran reconocimiento en el mercado como solución efectiva de integración de equipos Mac OSX a dominios Active Directory de Microsoft se muestra a continuación las bondades del mismo [22].

La herramienta permite unir equipos con sistema operativo Mac OSX dentro de un dominio Active Directory en un solo paso a través de una herramienta de interfaz gráfica de usuario o desde la línea de comandos.

Autentica a los usuarios con un único nombre de usuario y contraseña en los sistemas Windows y no Windows.

Aplica las directivas de contraseña en todos los sistemas Windows y no Windows.

Mantiene un caché de credenciales por si se pierde el acceso de red o el controlador de dominio se ha reducido, que le permiten seguir trabajando.

Resuelve ciertos inconvenientes como por ejemplo:

Mantiene un single sign on para aplicaciones.

Permite el manejo de SuDo (Super User Do).

Implementa seguridad de acceso a la red de forma granular.

Centraliza la administración de los equipos.

1.2.5.1- Instalación

Descargar el cliente “PowerBroker Open Edition” y desde el equipo MacBook contando con un usuario con los privilegios adecuados de administración local se procede a la instalación [22].

Hacer doble clic en el archivo [pbis-open-7.5.1.1517.dmg](#) donde se muestra la siguiente pantalla, hacer clic en “Continuar” y luego “Aagree”:

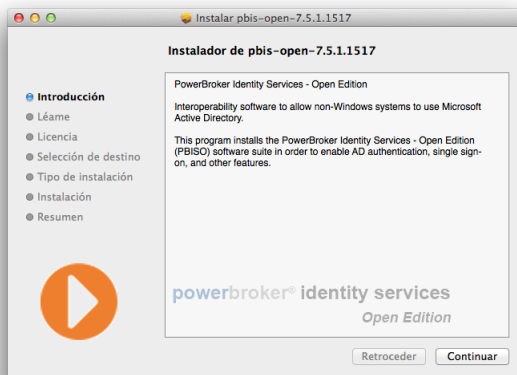


Imagen 53

Al avanzar con la instalación se debe indicar el dominio Active Directory al cual se pretende unir el equipo MacBook.

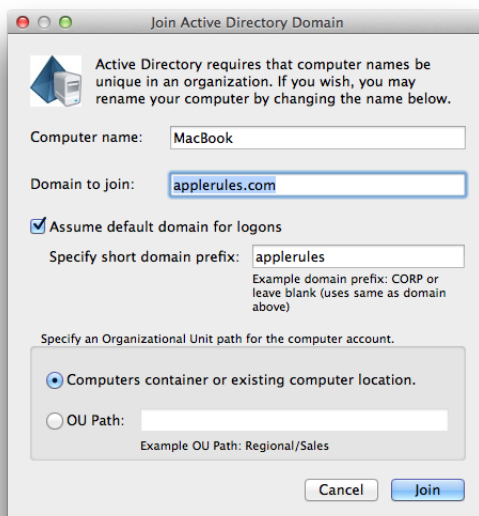


Imagen 54

Tras ingresar un usuario con credenciales suficientes para la tarea se muestra un mensaje de bienvenida.

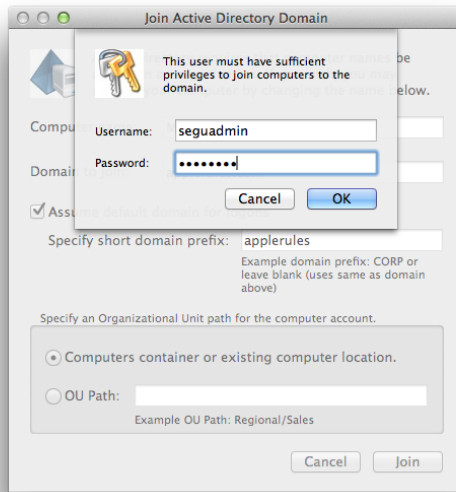


Imagen 55

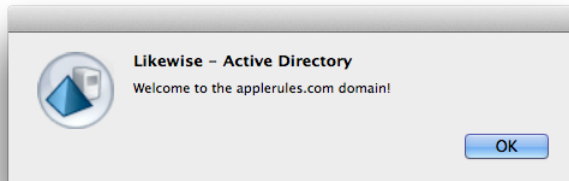


Imagen 56

Y se pueden observar las características de la conexión en la Utilidad de Directorios:

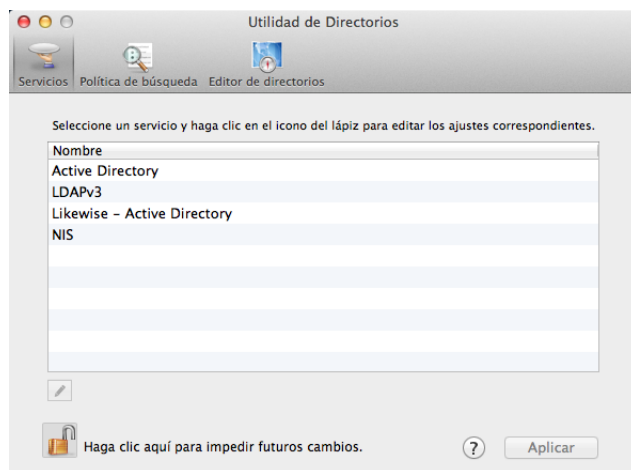


Imagen 57

A modo de prueba se creó un usuario de dominio denominado Steve Jobs cuyo nombre de usuario es “sjobs” y se le configuró la caducidad de la clave para que en el primer ingreso le sea solicitado el cambio de la misma:

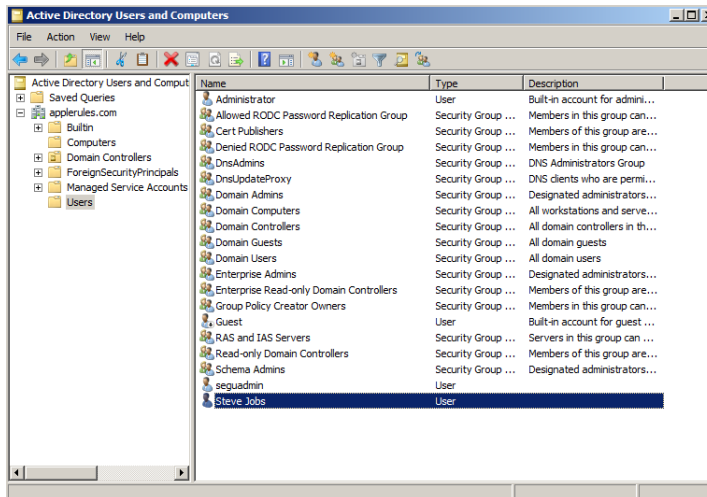


Imagen 58

Al realizar el primer ingreso se solicita el cambio de clave:

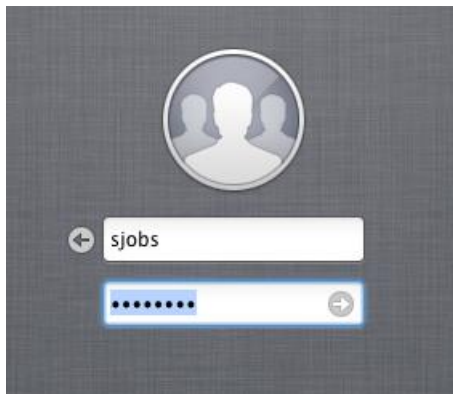


Imagen 59



Imagen 60

Finalmente se puede observar el escritorio del usuario de dominio Active Directory dentro del equipo MacBook:



Imagen 61

¿Qué producto elegir?

Las soluciones mostradas en todos los casos resuelven correctamente la integración de los equipos con el dominio Active Directory.

Si es importante destacar lo costoso de la solución Open Directory recomendada solamente en casos de contar con un importante porcentaje de los equipos de la organización de marca Apple.

En el común de los casos donde solo pocos equipos forman parte del parque informático la evaluación debe pasar fundamentalmente por los costos que cada empresa pueda ofrecer y que debe ser evaluado en el momento de encarar el proyecto de integración siendo los cuatro productos de excelentes prestaciones.

1.3- Antivirus

Suele creerse erróneamente que los equipos con sistemas operativos OSX no poseen amenazas de virus o malware llevando esta falacia a poner en riesgo la información contenida en el equipo y una posible infección dentro de la red corporativa. Por este motivo es de suma importancia contar con un software antivirus que proteja al sistema operativo del portátil.

Transcurriendo el año 2013 podemos observar como en estos ejemplos que cada día crecen las amenazas sobre el SO siendo ya imprescindible la utilización de un antivirus y un anti-malware profesional.

El caso del backdoor OSX/Pint sized. A qué cifra el tráfico de comandos con una clave RSA (8) o como publica la revista PCWorld que acaba de descubrirse una vulnerabilidad de Microsoft Office que permite instalar un troyano que permite el acceso remoto al equipo con Mac OSX [9].

Desde los comienzos existen programas como el histórico Disinfectant [5] que desde el año 1995 y de forma gratuita analizaba diversos aspectos del sistema operativo con la gráfica y estilo respetando los estándares Apple del momento, brindando protección para virus y malware de diversa índole. Desde la misma web de Apple fue promocionado el producto

[4].

Hoy en día existen comparativas especializadas de donde optar por la mejor alternativa de cada momento. De ser posible es importante mantener en caso de ya contar una solución antivirus para la plataforma Windows de forma centralizada, con la opción de la instalación en los equipos Mac OS X manteniendo una sola consola de control y monitoreo.

Un trabajo de gran profundidad realizado por la organización Antivirus Comparatives (www.av-comparative.org) que de forma independiente realiza diversas pruebas y analiza las cualidades de cada producto que brinda información valiosa para definir la solución más adecuada a la organización.

En la última entrega a octubre del año 2012 los productos analizados fueron los siguientes y cuyas conclusiones se muestran a continuación [6]:

avast! Free Antivirus for Mac ofrece un producto libre de preocupaciones que casi no requiere configuración de parte del usuario y está disponible de forma gratuita. Los componentes del navegador completan la solución.

Avira Free Mac Security ofrece un paquete fácil de utilizar y gratuito. El programador es muy práctico, pero hay opciones podrían ser mejoradas.

eScan Anti - Virus for Mac es un escáner de virus de una amplia gama de opciones de configuración y un planificador bien diseñado, también ofrece bloqueo de los dispositivos de almacenamiento USB. En términos de facilidad de uso, todavía hay cierto margen para la optimización.

ESET Cyber Security Pro es mucho más que un antivirus. La suite de seguridad, además, ofrece un firewall, control parental y un potente programador, así como funciones innovadoras, como los procesos en ejecución. Se trata de un producto muy bien pensado.

F - Secure Anti - Virus for Mac es un programa antivirus que incorpora además un Firewall, con una interfaz clara y fácil de usar y opciones sencillas de configuración. Los usuarios avanzados se beneficiarán de informes más detallados de análisis de virus.

[Kaspersky Security for Mac](#) es un producto de seguridad bien diseñado, que se destaca sobre todo por las características de control parental. Otros puntos a favor son las extensiones del navegador y la interfaz de usuario intuitiva.

[ZeoBit MacKeeper](#) es una suite muy completa, que puede ser vista más como una herramienta de optimización de sistema que de una suite de seguridad. El componente de Internet Security ofrece todo lo que se podía esperar de una suite de antivirus. Zeobit es el único fabricante en nuestro test que ofrece un convincente anti-robo de componentes.

1.4- Cifrado del disco rígido

El cifrado de los datos del disco es la solución real para la protección de la información en equipos portátiles que la organización dispone. Los equipos son altamente vulnerable de ser robados o hurtados siendo un eslabón muy débil si no se toman los recaudos adecuados.

Existen diversos aspectos a considerar en lo referente a la inscripción de los datos del disco rígido. Como punto de partida es tomar la decisión de cifrar ciertas carpetas donde pueden encontrarse almacenados los datos críticos, siendo una alternativa que depende del uso adecuado de cada usuario dejando en manos de los mismos la responsabilidad de que lo importante quede realmente protegido.

La alternativa más adecuada es el cifrado del disco completo siendo más costoso a nivel de procesamiento o tiempo de CPU pero garantizando la total protección de los datos y la baja o nula dependencia del usuario del equipo tornando transparente para el mismo el estado de los archivos de información.

Avanzando por la segunda opción del cifrado completo del disco existen diversas soluciones en el mercado donde el aspecto fundamental en que pueden diferenciarse de la solución nativa propia del Mac OSX, es contar con una consola de administración centralizada del estado de cada dispositivo MacBook.

1.4.1- McAfee Endpoint Encryption

El producto McAfee Endpoint Encryption brinda la posibilidad de integrar el producto dentro de la consola centralizada McAfee ePolicy Orchestrator (ePO) permitiendo realizar tareas de administración y control, asignar usuario con sus diversos permisos, definir características del cifrado tanto para Workstation Microsoft como para equipos MacBook de Apple [21].

El procedimiento consiste en como primer instancia incorporar el objeto maquina existente en el Active Directory dentro de la consola ePO. Realizar la asignación de los usuarios que tendrán la posibilidad de arrancar la sesión y encender el equipo y la configuración de las opciones de cifrado.

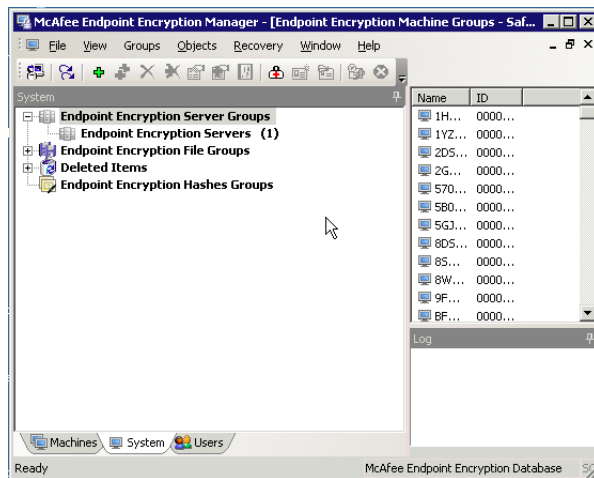


Imagen 62



Imagen 63

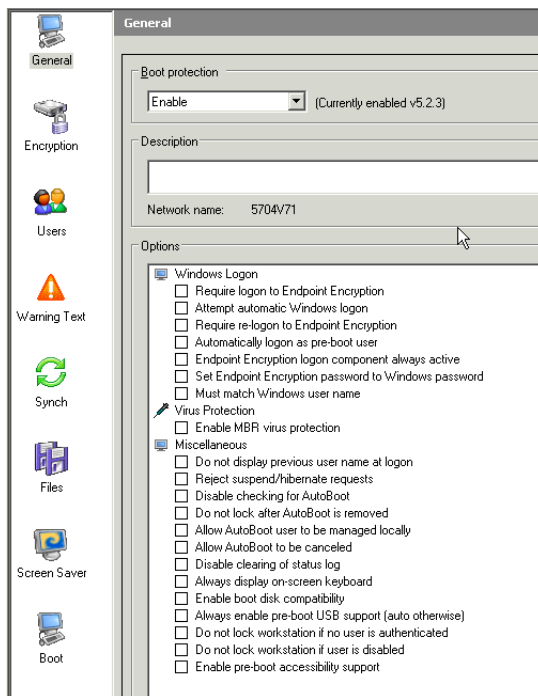


Imagen 64

El proceso continua con la instalación del cliente en los dispositivos, dicho cliente se conecta a la consola central quien le envía la configuración para luego comenzar con el cifrado del disco.

Una vez que el producto se encuentra instalado, en cada oportunidad que es encendido presenta una pantalla donde se debe ingresar un usuario y clave válidos que permite continuar con el proceso de inicio. Como la solución se posiciona al inicio del MBR no es posible de ninguna manera acceder siquiera al sistema operativo instalado y mucho menos a los datos almacenados en el resto del disco rígido.

Dentro del equipo MacBook queda residente un agente que se comunica con la consola central de la cual recibe cualquier tipo de modificación sobre la configuración.

El producto resulta ser de gran robustez y la consola centralizada permite la recuperación de la información del disco que en caso de extravío de la clave u

otro inconveniente como ser el deterioro del disco por medio del des-cifrado del mismo.

El proceso de des-cifrado se lleva a cabo generando la base de datos que contiene la clave asignada al equipo desde la consola, que luego se transporta a un medio que permita realizar el inicio del equipo (dispositivo USB con arranque del SO por ejemplo), tarea realizada por un usuario con los permisos suficiente que se recomienda sea personal de Seguridad Informática.

Una vez que se cuenta con el disco se debe acceder físicamente al equipo, realizar el inicio e ingresar la clave de la base de datos que había sido previamente configurada para luego aguardar el des-cifrado de los datos y eliminación del producto.

1.4.2- FileVault (Aplicación nativa)

El propio Mac OSX posee una solución que cifra todo el contenido del disco [18] y en tiempo real realiza la operación inversa. Esta operación es sumamente rápida utilizando el algoritmo XTS-AES 128. Posee la ventaja de ser un cifrado en tiempo real transparente para el usuario pero que en equipos con discos rígidos de plato se va a notar una degradación de la performance del mismo, se puede optar por unidades de estado sólido (SSD - Solid State Disk) donde la diferencia se tornará imperceptible.

Otra desventaja es que si la clave se pierde es imposible en un tiempo de cómputo razonable, recuperar la información. Es por esto que siendo la opción que por defecto trae el sistema operativo y de gran comodidad, si es sumamente importante que la administración de las claves de cifrado sea realizado por personal especializado de la organización y sean las claves resguardadas con recelo.

Para habilitar el cifrado se deben seguir los siguientes pasos:

Desde las “Preferencias del sistema” ingresar en la opción de “Seguridad y privacidad” y haga clic en la pestaña “FileVault”



Imagen 65

Se debe hacer clic en el candado ubicado en la parte inferior izquierda de la pantalla para poder operar con la opción. Luego se puede hacer clic en el botón “Activar FileVault...” para configurar el cifrado.

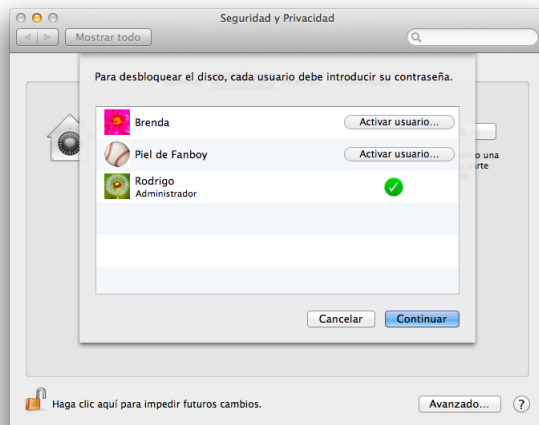


Imagen 66

En el caso que el equipo posea múltiples usuarios definidos se deberá configurar una clave para cada uno para que puedan utilizar los datos del disco rígido haciendo clic en “Activar usuario...”. Una vez ingresadas las claves se debe realizar clic en “Continuar”.



Imagen 67

A continuación el Mac OSX presenta en pantalla una clave de recuperación en caso que se olviden las contraseñas de acceso de los usuarios. La misma

deberá ser resguardada con sumo cuidado a fin de garantizar que la información contenida en el disco podrá ser recuperada. Al hacer clic en el botón “Continuar” se presenta la siguiente opción donde Apple le permite resguardar la clave de recuperación en los servidores propios de Apple siendo la clave también cifrada por medio de las preguntas y respuestas que se permiten seleccionar.

Esto último queda a criterio de la organización, si se va a confiar en la seguridad de resguardo de Apple o bien se realizará el correcto resguardo dentro de los servidores de la propia organización sin comprometer la confidencialidad del equipo. Si bien la posibilidad de ocurrencia es sumamente baja no es nula.



Imagen 68

Una vez decidido el paso anterior y tras hacer clic en el botón “Continuar” se comienza el cifrado del disco tras su reinicio.

El proceso demora a razón de entre 5 a 15 minutos cada 50 Gb de información en un disco rígido de 5400 rpm. Los tiempos se verán sumamente reducidos en caso de utilizar una unidad SSD.

En caso de necesitar quitar el cifrado se deben ingresar a la misma ubicación y simplemente hace clic en el botón “Apagar FileVault”.

Esta opción descrita es la alternativa que Apple denomina “Café” siendo una configuración por cada equipo puntualmente con asesoramiento de personal de Tecnología Informática de la compañía. Existe una opción de administración centralizada que dada su complejidad debe ser evaluada como alternativa en caso de contar con un gran número de equipos MacBook [20].

1.4.2.1- Eliminar el almacenamiento de clave en Suspensión del equipo

A fin de maximizar la seguridad en la utilización del cifrado de disco con la herramienta FileVault se recomienda la eliminación de la clave al momento de entrar en hibernación.

Esto sucede en el momento que el equipo a fin de resguardar la energía de la batería pasa del modo hibernación tras estar un tiempo en modo de reposo.

Cuando el equipo se encuentra utilizando el cifrado de disco Filevault al ingresar en modo de hibernación la clave de cifrado es guardada en el EFI (firmware) del equipo para poder restablecer rápidamente el equipo a su actividad normal.

Eliminar el resguardo de la clave de cifrado robustece la fiabilidad de la medida de seguridad agregando una pequeña molestia al usuario ya que deberá ingresar la clave de Filevault para acceder al equipo pero considerando la relación costo-beneficio es sumamente recomendable implementarla.

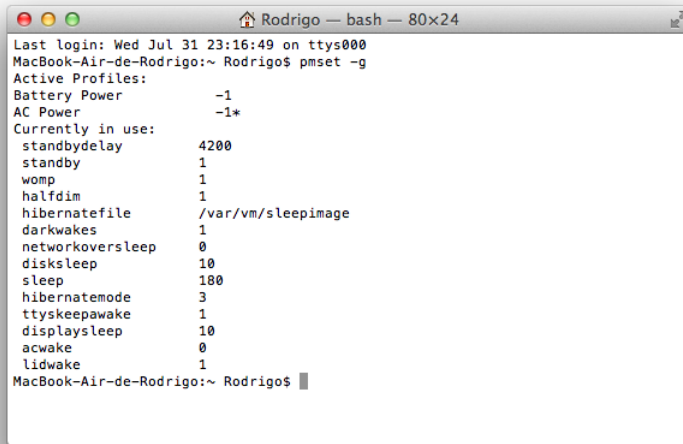
Para habilitar la opción se debe ejecutar el siguiente comando desde la consola:

```
sudo pmset -a destroyfvkeyonstandby 1
```

Para deshabilitar la opción se debe ingresar el siguiente comando desde la consola:

```
sudo pmset -a destroyfvkeyonstandby 0
```

En caso de necesitar consultar el estado del parámetro se debe ingresar el siguiente comando desde la consola: **pmset -g**



```
MacBook-Air-de-Rodrigo — bash — 80x24
Last login: Wed Jul 31 23:16:49 on ttys000
MacBook-Air-de-Rodrigo:~ Rodrigo$ pmset -g
Active Profiles:
Battery Power      -1
AC Power           -1*
Currently in use:
standbydelay       4200
standby            1
womp               1
halfdim            1
hibernatefile      /var/vm/sleepimage
darkwakes          1
networkoversleep   0
disksleep          10
sleep              180
hibernatemode      3
ttyskeepawake     1
displaysleep       10
acwake             0
lidwake            1
MacBook-Air-de-Rodrigo:~ Rodrigo$
```

Imagen 69

CAPITULO SEGUNDO

2- iOS (Sistema Operativo de dispositivos iPhone, iPod Touch y iPad)

¿Qué debe tener?

Los dispositivos móviles de Apple que poseen el sistema operativo iOS son el iPhone, el iPad y el iPod Touch, los dos primeros son los generalmente elegidos por las organizaciones dada su capacidad de telefonía y datos, limitando al iPod Touch solamente a conexión WiFi.

El sistema operativo iOS ya integra varias medidas de seguridad que es importante mantenerlas configuradas para lograr la mayor protección posible.

Como indica el Centro de Seguridad TIC de la Comunidad Valenciana, existen aspectos a considerar a saber:

“Las nuevas tecnologías, en su constante evolución, han permitido que se desarrollen nuevas herramientas para desempeñar labores profesionales de forma más eficaz. Se ha evolucionado, del ordenador como principal herramienta de trabajo, a utilizar dispositivos móviles como smartphones o tablets en entornos de trabajo donde la movilidad es fundamental.

Sin embargo, esa movilidad conlleva unos riesgos asociados a la posibilidad de pérdida o robo del dispositivo, produciéndose una pérdida de confidencialidad de la información contenida en el mismo.” [7]

Apple posee una herramienta denominada “Apple Configurator” [24] con la cual podremos crear perfiles de configuración ajustando los dispositivos a la medida que la organización y las diversas regulaciones indiquen.

Estos perfiles permiten una gran cantidad de ajustes que a priori lograrán como principales mejoras en el nivel de seguridad [23]:

El impedir que el equipo sea utilizado por personal no autorizado.

Protección de los datos contenidos en el equipo ya sea por pérdida o robo del mismo.

Protocolos de red y cifrado de datos en tránsito. Es importante destacar que los dispositivos Apple iPhone, iPad trabajan con un cifrado por hardware AES 256 bits que no es posible desactivar y se encuentra siempre protegiendo los datos contenidos en los mismos.

Restricción a las aplicaciones que serán habilitadas y ejecutadas en el dispositivo.

2.1- Apple Configurator configuración

Descargar la aplicación “Apple Configurator” desde la App Store sobre un equipo MacBook contando con un usuario con los privilegios adecuados [24].

La aplicación posee tres grandes situaciones consideradas que permite fácilmente configurar dispositivos a fin de ser entregados al personal asignado de la organización [24].

“Preparar dispositivos. Se puede preparar todo un grupo de dispositivos iOS nuevos con una misma configuración central para después entregarlos entre los usuarios. La aplicación automáticamente actualiza los dispositivos a la última versión de iOS, instala los perfiles de configuración y aplicaciones, se los registra en el servidor MDM de la empresa y ya se encuentra listo para ser entregado al usuario. La preparación de dispositivos es una opción de implantación fantástica para empresas que quieren ofrecer dispositivos iOS a sus empleados para su uso diario.

Supervisar dispositivos. Otra opción es supervisar un conjunto de dispositivos iOS manteniendo el control directo para poder configurarlos de forma continua. Aplica una configuración a cada dispositivo y volverá a aplicarse automáticamente después de cada uso con solo conectar el dispositivo a Apple Configurator. La supervisión es ideal para implantar dispositivos para tareas específicas (por ejemplo, ventas minoristas, trabajos de campo o servicios médicos), compartir dispositivos entre alumnos de un aula o un laboratorio, o entregar temporalmente dispositivos iOS a clientes (en hoteles, restaurantes, hospitales, etc.).

Asignar dispositivos. Por último, se pueden asignar dispositivos supervisados a usuarios concretos de una empresa. Presta un dispositivo a un usuario determinado y restaura su copia de seguridad (incluidos sus datos). Cuando se

vuelva a registrar el dispositivo, haz una copia de seguridad de los datos de ese usuario para utilizarlos en el futuro, incluso en un dispositivo distinto. Esta opción resulta útil para los usuarios que necesitan trabajar en los mismos datos y documentos durante un largo periodo de tiempo, con independencia del dispositivo que se les entregue.”

Una vez que se encuentra instalado abrir la aplicación y definir la configuración principal antes de comenzar con la creación de los perfiles que sean necesarios.

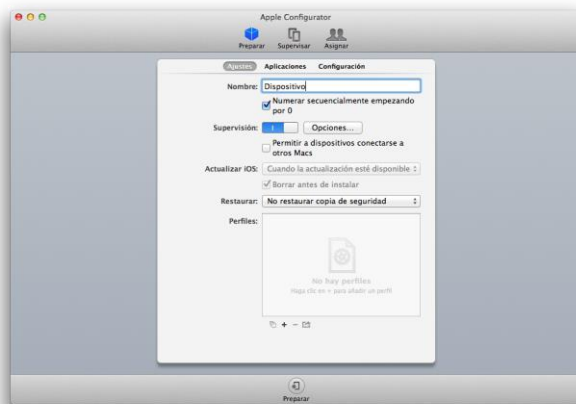


Imagen 70

Una facilidad que posee la herramienta es auto-numerar el nombre de los dispositivos. Así mismo a fin de identificarlos ante una posible pérdida es posible configurar la información de la organización con datos del contacto.

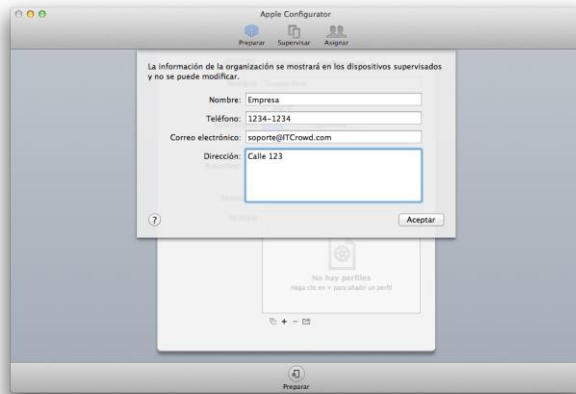


Imagen 71

Armado de perfiles

A continuación se detallan las opciones mínimas recomendadas para la adecuada configuración del entorno de seguridad de los dispositivos. Es posible crear una variedad de perfiles que incorporen diferentes medidas restrictivas. Se detallan por pestaña las opciones que se modifican a las presentadas por defecto al crear un nuevo perfil.

Sección General

Se debe otorgar un nombre que identifique al perfil junto con datos generales con fines administrativos. Es conveniente configurar una contraseña para evitar que sea posible eliminar el perfil.



Imagen 72

Sección Código

Según la regulación del BCRA A4609 existen requisitos mínimos que deben ser cumplidos, algunos enunciados de forma taxativa en el apartado 3 de la mencionada norma en lo referente a las características de las claves de acceso.

Por este motivo la configuración debe respetar:

Un largo mínimo de clave de 8 caracteres, ser alfanumérica, debe caducar cada 30 días y no podrá ser repetida la misma clave por al menos 12 veces. A los 3 intentos fallidos la cuenta debe inhabilitarse.



Imagen 73

Sección Restricciones

Pestaña Funcionalidad

Se recomienda deshabilitar el Permitir AirDrop ya que es una vía de transferencia de archivos con otros dispositivos limitando (aunque sea solo dificultando) la diseminación de información.

Denegar la posibilidad de instalar aplicaciones, de eliminar aplicaciones instaladas y Compras desde aplicaciones, de esta manera se podrá mantener los dispositivos con las aplicaciones necesarias para llevar adelante las tareas de cada función. El usuario deberá solicitar las aplicaciones y el personal de mantenimiento de los equipos procederá a la instalación.

Se debe denegar la opción Permitir la modificación de ajustes de Buscar a mis amigos para mantener la configuración de privacidad definida por la organización. De similar manera se debe denegar la posibilidad de Enviar información de diagnóstico y uso a Apple reforzando el concepto de confidencialidad que posee una herramienta de la organización.

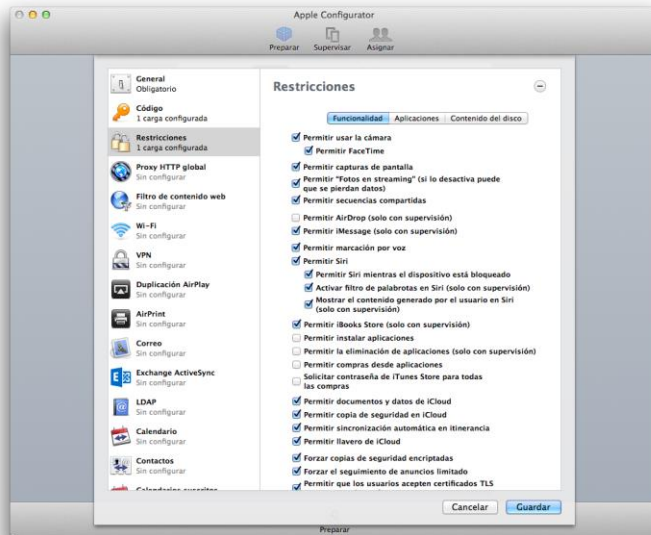


Imagen 74



Imagen 75

Pestaña Aplicaciones

Se debe denegar el uso de iTunes Store a fin de limitar posibles erogaciones de compras no deseadas por la organización. En este caso existe la posibilidad de denegar el uso de YouTube, por defecto se recomienda la denegación de la aplicación pero descansa la decisión final en cada gerencia responsable.

Se debe denegar el uso de Game Center dado que solamente es utilizado para los juegos en línea.

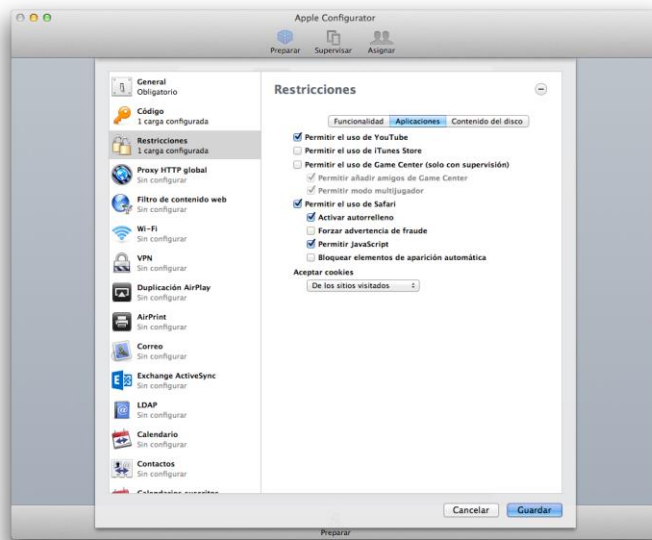


Imagen 76

Pestaña Contenido del disco

No hay modificaciones adicionales de la configuración que se provee por defecto en la pestaña.



Imagen 77

Sección Proxy http global

Esta sección permite configurar los ajustes del servidor proxy por el que pasará todo el tráfico http del dispositivo.

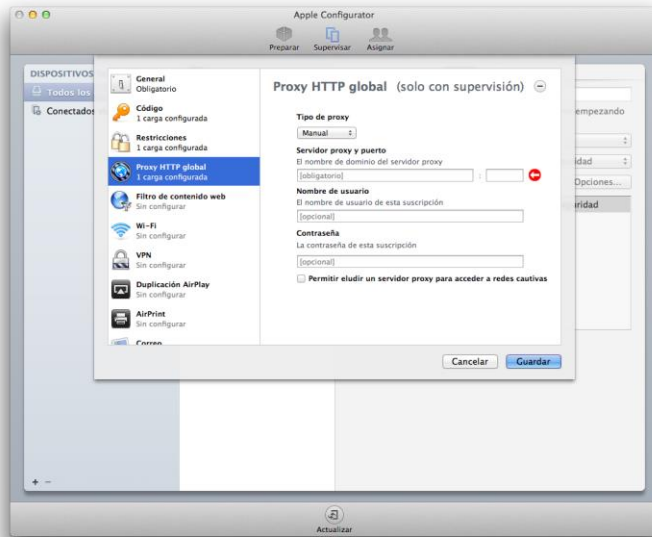


Imagen 78

Sección Filtro de contenido Web

Generalmente las organizaciones poseen una solución para la administración de las categorías autorizadas de navegación Web que coincide con la misión, visión y valores que la organización define.

En caso de no contar con una solución de este tipo es posible en esta sección definir qué direcciones es válido que sean accedidas, limitar solo a una lista o denegar otras determinadas direcciones. La solución puede otorgar una gran valor para limitar el dispositivo a la tarea específica que coinciden con las funciones del colaborador.

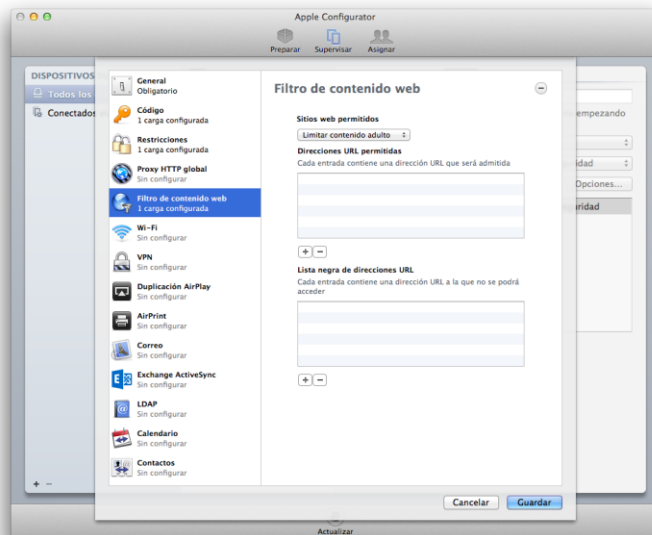


Imagen 79

Sección Wi-Fi

Es posible limitar el uso de las redes Wi-Fi a una determinada cantidad de conexiones conocidas, ingresando los datos técnicos necesarios de autenticación. De acuerdo a la criticidad de la información que el usuario maneje en el dispositivo se recomienda habilitar solamente las redes a las cuales sea necesario que el equipo se conecte evitando posibles puntos de ataque a la información.

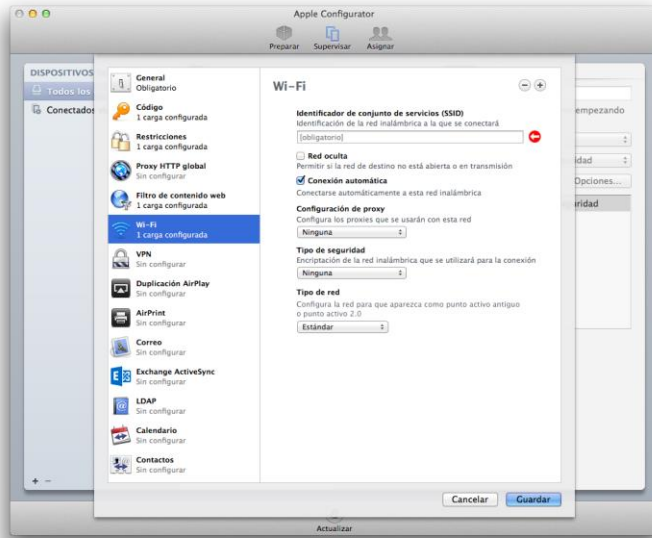


Imagen 80

Sección VPN

En esta sección se indica como configurar la conexión del dispositivo a través de una VPN (Virtual Private Network – Red Privada Virtual) incluida la información de autenticación necesaria.

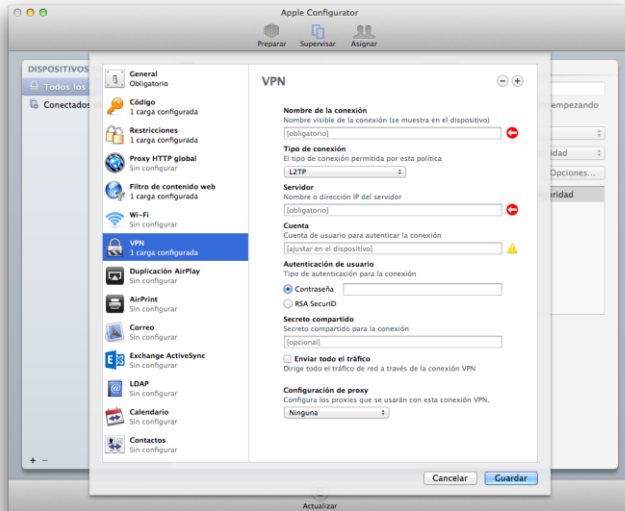


Imagen 81

Sección Duplicación AirPlay

Esta sección permite definir los ajustes de la conexión a destinos de duplicación AirPlay. AirPlay de Apple permite reproducir el contenido del dispositivo iOS en un televisor o altavoces conectados por un Apple TV o bien espejar la pantalla.

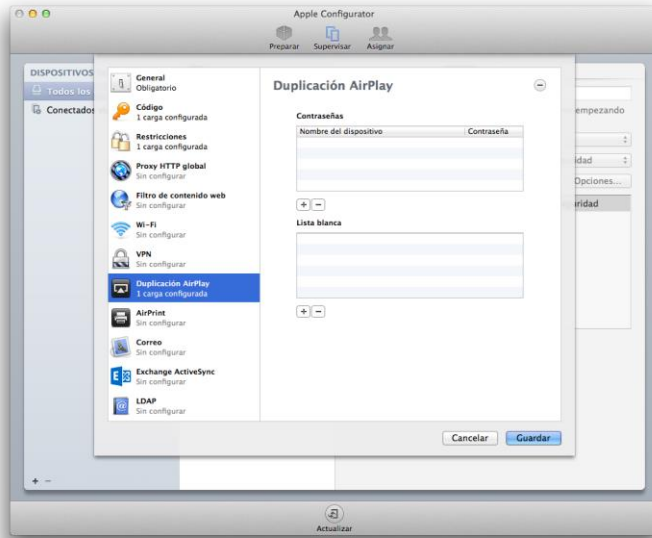


Imagen 82

Sección AirPrint

Permite realizar la configuración de conexión a impresoras AirPrint.

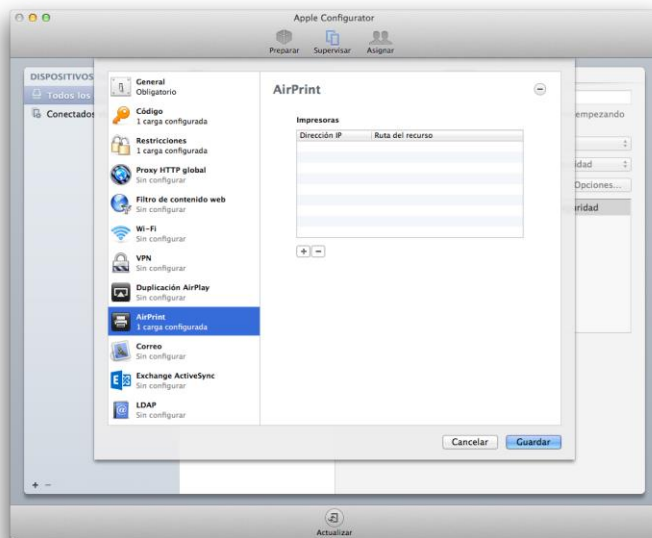


Imagen 83

Sección Correo

Permite la configuración de la cuenta de correo corporativa que la organización utilice. Las diversas opciones de configuración dejan activo el servicio de correo ya sea con protocolo POP o IMAP.



Imagen 84

Exchange ActiveSync

A partir del software de correo Microsoft Exchange 2003 SP2 se incluye la posibilidad de utilizar el protocolo ActiveSync a fin de configurar la cuenta de correo corporativa que la organización utilice. Las diversas opciones de configuración dejan activo el servicio de correo listo para ser utilizado.



Imagen 85

LDAP

Permite configurar las opciones de conexión a servidores LDAP de la organización.

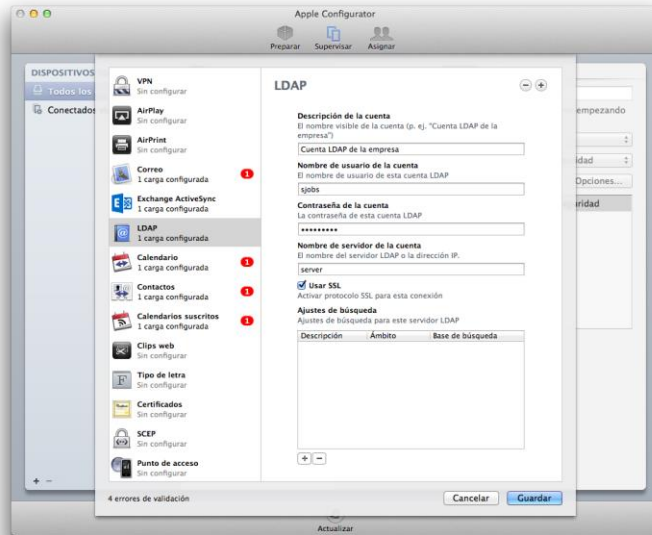


Imagen 86

Calendario

Permite la configuración de la conexión a calendarios del tipo CalDAV de la organización.

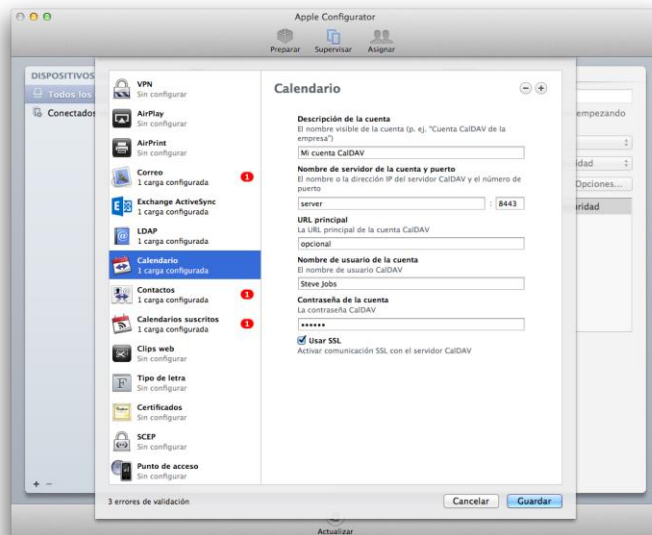


Imagen 87

Contactos

Permite la configuración de la conexión a la base de los de contactos del tipo CarDAV de la organización.

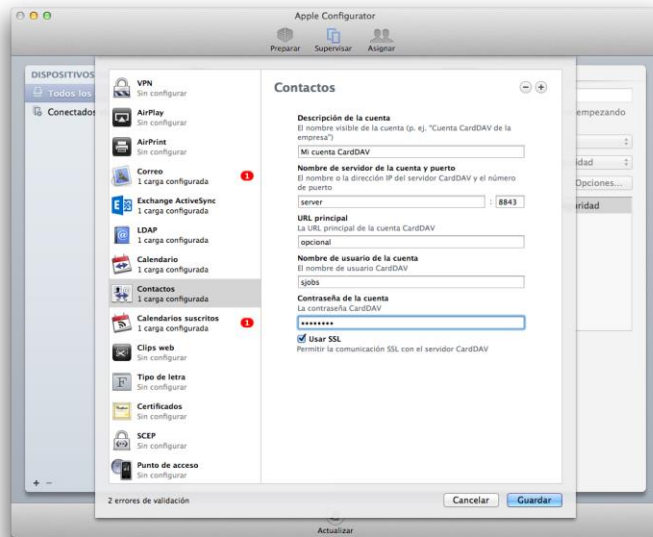


Imagen 88

Calendarios suscritos

Permite la configuración de la conexión a calendarios suscritos de la organización.



Imagen89

Clips Web

Permite configurar videos que se desee instalar en los dispositivos de ser necesario.

Tipo de letra

Permite la instalación de tipografías tipo TrueType o OpenType que se desee instalar en los dispositivos.

Certificados

Permite la instalación de certificados digitales tipos PKCS1 o PKCS12 que sea necesario contar en los dispositivos.

SCEP

Permite definir los ajustes de configuración para obtener certificados de servidores SCEP.

Punto de acceso

Permite la configuración de los detalles de conexión al operador móvil.

3- Conclusión

Creo personalmente que el manejo de equipos móviles con la cantidad de información que hoy pueden almacenar es una tarea que propone un desafío a los profesionales de la seguridad y del área de tecnología en general. Cada día nuevas amenazas son descubiertas y a su vez nuevas tecnologías son desarrolladas, que generalmente en sus inicios presentan gran cantidad de nuevas vulnerabilidades que luego al ser utilizadas, explotadas con fines no santos, son estudiadas y finalmente corregidas.

Este círculo de nuevas tecnologías, amenazas, parches puede tentarnos a bajar la guardia y tomar varias actitudes, negar (o prohibir) las nuevas tecnologías,

utilizarlas sin tomar la seriedad del caso o bien la sana actitud de involucrarse y con análisis e investigación lograr la mejor protección posible.

Entiendo que la tercera opción es la más redituable dado que, en el caso de la primer opción es solamente retrasar lo inevitable (tarde o temprano tendremos datos en la nube, tarde o temprano utilizaremos tabletas u otros dispositivos, etc.) y la segunda opción es riesgosa y sobre todo peligrosa porque la falta de conocimiento no nos permite siquiera imaginar los riesgos a los que nos enfrentamos como para poder evaluar métodos que los minimicen hasta tanto puedan ser resueltos de una forma adecuada.

¿Es suficiente con seguir los diversos pasos de configuración?

¿Es suficiente para quedarnos tranquilos y descansar en que contaremos con la información absolutamente protegida?

La respuesta lamentablemente es que no.

Constantemente dado el complejo entorno cambiante, nuevas problemáticas surgen y es necesario por medio de la inteligencia, la capacitación constante y el involucramiento con nuevas tecnologías, comprender el negocio, comprender las necesidades de los usuarios y acompañar con soluciones, con configuraciones y porque no con capacitación activa, simple y amigable, a llevar a niveles aceptables de protección el activo más importante que posee la organización, la información.

Nuevas herramientas parecen confiables, nos muestran ciertos aspectos que cumplen con ciertos aspectos regulatorios o al menos pareciera que los cumplen, sin embargo es importante estudiar las diversas posibilidades y lo que va ocurriendo a medida que las herramientas son utilizadas. Es recomendable realizar controles sobre los equipos entregados periódicamente, tanto sobre el hardware y software como así también indagando a los usuarios de los mismos para intentar descubrir riesgos ocultos, errores no reportados u otros temas

relacionados que pudieren afectar directamente a los intereses de la organización.

En lo que respecta al sistema operativo de los equipos de escritorio Mac OSX en sus diversas versiones que afecta a las MacBook Pro y MacBook Air como hemos visto en las configuraciones, dado el poder del mismo es necesario configurar varios aspectos a fin de mantener la seguridad.

Lo referente a la validación del usuario y las características que deben poseer la clave y demás definiciones (ya sean por regulaciones o buenas prácticas y sentido común), generalmente al contar con un esquema definido a nivel de dominio de la red lo trascendente es lograr que esas mismas políticas de definiciones se trasladen automáticamente a los equipos MacBook.

Por otro lado definir la configuración de lo que le es permitido al usuario realizar ya sea dentro del propio equipo (como restringir para que pueda realizar cómodamente las funciones del día a día), y como ese equipo podrá integrarse a diversas fuentes de información, internas y externas a la organización (como servicios en internet o granjas de almacenamiento de archivos).

Es importante recordar que Apple libera nuevas versiones del sistema operativo Mac OSX regularmente una vez al año donde nuevas propiedades se incorporan y deberán ser estudiadas y analizadas.

Algo similar ocurre con el sistema operativo iOS de los dispositivos iPhone, iPad y iPod Touch en sus diferentes versiones. En este caso el sistema operativo se encuentra ya por definición más acotado y limitado al hardware y sus posibilidades pero no por eso se han disminuido las características de seguridad que son posibles configurar en los mismos.

Como se ha descrito el uso de la herramienta automatizada de configuración con el armado de perfiles simplifica enormemente la tarea de configuración y administración, que bajo mi experiencia en muchas oportunidades debido a la gran demanda del negocio por brindar soluciones portables y económicas, no se destina el suficiente tiempo para poder aplicar los conocimientos y el criterio a fin de proteger los mismos impulsando a que sea puestos en producción sin las medidas básicas de seguridad.

En este caso los dispositivos mencionados cuentan con una ventaja dado que fácilmente es configurable una gran cantidad de medidas de seguridad que se suman a la protección que por defecto trae el sistema operativo que ya a partir de la versión 5 del mismo por ejemplo, cuenta con un cifrado por medio del hardware de toda la información contenida en él.

Los dispositivos pueden ser borrados remotamente en caso de robo o extravío y al encontrarse configurados mínimamente con una contraseña ya puede garantizarse que ni siquiera con métodos de investigación forense la información no podrá ser accedida.

Como ejemplo de actualidad, el nuevo dispositivo de telefonía que cuenta con una interfaz de reconocimiento de huella dactilar cuya tecnología es denominada Touch ID, no permite de ninguna forma acceder a la información si no se cuenta con la huella asignada, esto también crea un desafío a los administradores dado que si por alguna razón el empleado ya no perteneciere a la organización y es necesario acceder a la información de la organización contenida en el dispositivo y no fueron configuradas otras vías de acceso adecuadas, la información se habrá perdido.

Con este último ejemplo quiero demostrar la importancia de mantenerse actualizado y en contacto permanente con las nuevas tecnologías que nos

brindan soluciones y a su vez una constante revisión de lo aprendido, de lo conocido con sus virtudes y debilidades.

Para concluir creo que en ambos casos de los sistemas operativos vistos lo importante es que se mantenga un equilibrio que permita lograr el máximo posible de seguridad, de protección de la información y de los recursos de la organización sin castigar de sobremanera las funciones y utilidades que en cada caso brindan los equipos y dispositivos que tanto potencial poseen y que Apple día a día trabaja para que sea una combinación de performance, elegancia y seguridad.

Bibliografía Inicial

[1] Mobile Application Security - Himanshu Dwivedi - Chris Clark – David Thiel - Mc Graw Hill (ISBN: 978-0-07-163357-4)

[2] Mobile Malware Attacks and Defense – Ken Dunham - Syngress Publishing, Inc. (ISBN 13: 978-1-59749-298-0)

[3] Windows and Linux integration – Hands On Solutions for a mixed environment – Jeremy Moskowitz and Thomas Boutell. (ISBN-13: 978-0-7821-4428-6)

Referencias

[4] http://support.apple.com/kb/TA38539?viewlocale=en_US&locale=en_US

[5] <http://www.seguridadapple.com/2013/02/antimalware-historico-en-mac-os.html?m=1>

[6] http://www.av-comparatives.org/images/docs/mac_review_2012_en.pdf

[7] [CSIRTcv] Buenas_practicas_dispositivos_moviles.pdf

[8] <http://www.seguridadapple.com/2013/02/osxpintsizeada-nuevo-backdoor.html?m=1>

[9] http://www.pcworld.com/article/252839/malware_infects_macos_through_microsoft_office_vulnerability.html

[10] Best Practices for Integrating OS X with Active Directory - http://training.apple.com/pdf/wp_integrating_active_directory_ml.pdf

[11] <http://www.youtube.com/watch?v=ukNs1pgCoz8>

[12] http://www.centrify.com/directcontrol/mac_os_x.asp

[13] <http://www.thursby.com/products/admitmac.html>

[14] http://www.thursby.com/sites/default/files/images/ADmitMac_SPD.pdf

[15] <http://www.quest.com/authentication-services/>

- [16] https://www.quest.com/Quest_Site_Assets/WhitePapers/Choosing_the_Right_AD_Bridge_Solution_060710.pdf
- [17] <http://www.mcafee.com/mx/products/endpoint-encryption.aspx>
- [18] <http://osxdaily.com/2013/05/22/filevault-disk-encryption-mac/>
- [19] <http://osxdaily.com/2013/07/06/maximize-filevault-security-destroy-key-storage-standby/>
- [20] http://training.apple.com/pdf/WP_FileVault2.pdf
- [21] <http://www.mcafee.com/es/products/endpoint-encryption.aspx>
- [22] <http://www.powerbrokeropen.org/powerbroker-open-edition-evaluation/>
- [23] http://images.apple.com/es/ipad/business/docs/iOS_Security_Introduction_Mar12-es.pdf
- [24] <https://itunes.apple.com/app/apple-configurator/id434433123?mt=12&ls=1>

Otras referencias y manuales:

Mac OS X Server - Open Directory Administration Version 10.6 Snow Leopard

http://manuals.info.apple.com/en_US/OpenDirAdmin_v10.6.pdf

Choosing the Right Active Directory Bridge Solution – White Paper

https://www.quest.com/Quest_Site_Assets/WhitePapers/Choosing_the_Right_Active_Directory_Bridge_Solution_060710.pdf