Soluciones IBM® Client Security

Guía de instalación de Client Security Software Versión 5.3

Soluciones IBM® Client Security

Guía de instalación de Client Security Software Versión 5.3

Primera edición (mayo de 2004)

Antes de utilizar esta información y el producto al que da soporte, no olvide leer el Apéndice A, “Normativas de exportación de los EE.UU. para Client Security Software”, en la página 49 y el Apéndice C, “**Avisos y marcas registradas**”, en la página 55.

Este manual es la traducción del original inglés *IBM® Client Security Solutions, Client Security Software Version 5.3 Installation Guide*.

Contenido

Prefacio

Este apartado proporciona información sobre el uso de esta guía.

Acerca de esta guía

Esta guía contiene información sobre cómo instalar IBM Client Security Software en un sistema de red de IBM, también denominado cliente de IBM, que contenga IBM Embedded Security Subsystem. Esta guía también contiene instrucciones sobre cómo habilitar IBM Embedded Security Subsystem y cómo establecer la contraseña del administrador para el subsistema de seguridad.

La guía está organizada de la forma siguiente:

El ″Capítulo 1, “Introducción”″ contiene un breve resumen sobre los conceptos de seguridad básicos, una visión general de las aplicaciones y componentes incluidos en el software, así como una descripción de las características PKI (Public Key Infrastructure).

El ″Capítulo 2, “Cómo empezar”″ contiene los requisitos previos de hardware y software para la instalación, así como instrucciones para bajar el software.

El ″Capítulo 3, “Antes de instalar el software”″ contiene instrucciones de requisitos previos para instalar IBM Client Security Software.

El ″Capítulo 4, “Instalación, actualización y desinstalación del software”″ contiene instrucciones para instalar, actualizar y desinstalar el software.

El ″Capítulo 5, “Resolución de problemas”″ contiene información útil para resolver problemas que podría experimentar mientras sigue las instrucciones proporcionadas en esta guía.

El ″Apéndice A, “Normativas de exportación de los EE.UU. para Client Security Software”″ contiene información sobre las normativas de exportación de los EE.UU. sobre este software.

El ″Apéndice B, “Información sobre contraseñas y frases de paso”″ contiene criterios para las frases de paso que se pueden aplicar a una frase de paso de UVM y normas para las contraseñas del administrador.

El ″Apéndice C, “**Avisos y marcas registradas**”″ contiene avisos legales e información de marcas registradas.

A quién va dirigida esta guía

Esta guía va dirigida a los administradores de red y del sistema que configuren la seguridad de sistemas personales en los clientes de IBM. Se precisan conocimientos de los conceptos de seguridad, como PKI (Public Key Infrastructure) y gestión de certificados digitales dentro de un entorno de red.

Utilización de esta guía

Utilice esta guía para instalar y configurar la seguridad de sistemas personales en los clientes de IBM. Esta guía acompaña a los manuales *Guía del administrador de Client Security Software*, *Utilización de Client Security con Tivoli Access Manager* y *Guía del usuario de Client Security Software*.

Esta guía y la demás documentación de Client Security puede bajarse desde el sitio Web de IBM en http://www.pc.ibm.com/us/security/secdownload.html.

Referencias a la *Guía del administrador de Client Security Software*

En este documento se hacen referencias a la *Guía del administrador de Client Security Software*. La *Guía del administrador* contiene información sobre la utilización de User Verification Manager (UVM) y el trabajo con la política de UVM, así como información sobre la utilización de Administrator Utility y User Configuration Utility.

Después de instalar el software, utilice las instrucciones de la *Guía del administrador* para configurar y mantener la política de seguridad para cada cliente.

Referencias a la *Guía del usuario de Client Security Software*

La *Guía del usuario de Client Security Software*, que acompaña a la *Guía del administrador de Client Security Software*, contiene información útil sobre cómo efectuar tareas de usuario con Client Security Software, como la utilización de la protección de inicio de sesión de UVM, la creación de un certificado digital y la utilización de User Configuration Utility.

Información adicional

Puede obtener información adicional y actualizaciones de productos de seguridad, cuando estén disponibles, desde el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html.

Capítulo 1. Introducción

Algunos sistemas ThinkPad™ y ThinkCentre™ vienen equipados con hardware criptográfico integrado que funciona junto con tecnologías de software que pueden bajarse para proporcionar un alto nivel de seguridad en una plataforma PC cliente. De forma conjunta este hardware y software se denominan IBM Embedded Security Subsystem (ESS). El componente de hardware es el chip IBM Security Chip incorporado y el componente de software es IBM Client Security Software (CSS).

Client Security Software está diseñado para sistemas de IBM que utilizan el chip IBM Security Chip incorporado para cifrar archivos y almacenar claves de cifrado. Este software está constituido por aplicaciones y componentes que permiten a los sistemas cliente de IBM utilizar las características de seguridad para clientes a través de una red local, una corporación o Internet.

IBM Embedded Security Subsystem

IBM ESS soporta soluciones de gestión de claves como PKI (Public Key Infrastructure) y consta de las aplicaciones locales siguientes:

- Cifrado de archivos y carpetas (FFE)
- Password Manager
- Inicio de sesión seguro de Windows
- Varios métodos de autenticación configurables, que incluyen:
  - Frase de paso
  - Huella dactilar
  - Smart Card
  - Tarjeta de identificación por contacto

Para poder utilizar las características de IBM ESS de forma efectiva, el administrador de seguridad debe estar familiarizado con algunos conceptos básicos. Los apartados siguientes describen los conceptos de seguridad básicos.

El chip IBM Security Chip incorporado

IBM Embedded Security Subsystem es una tecnología de hardware criptográfico integrado que proporciona un nivel adicional de seguridad para plataformas IBM PC seleccionadas. Con la aparición de este subsistema de seguridad, los procesos de cifrado y autenticación son transferidos de un software más vulnerable al entorno seguro de un hardware dedicado. La mejora en la seguridad que esto proporciona es palpable.

IBM Embedded Security Subsystem soporta:

- Operaciones PKI RSA3, como cifrado para información confidencial y firmas digitales para autenticación
- Generación de claves RSA
- Generación de números seudo-aleatorios
- Cálculo de funciones RSA en 200 milisegundos
- Memoria EEPROM para el almacenamiento de pares de claves RSA
- Todas las funciones TCPA definidas en la especificación Vs. 1.1
- Comunicación con el procesador principal a través del bus LPC (Low Pin Count)

IBM Client Security Software

IBM Client Security Software se compone de las siguientes aplicaciones y componentes de software:

- **Administrator Utility:** se trata de la interfaz que utiliza un administrador para activar o desactivar el subsistema de seguridad incorporado y para crear, archivar y volver a generar las claves de cifrado y las frases de paso. Además, un administrador puede utilizar este programa de utilidad para añadir usuarios a la política de seguridad proporcionada por Client Security Software.
- **Consola del administrador:** la Consola del administrador de Client Security Software permite al administrador configurar una red de itinerancia de credenciales para crear y configurar archivos que permiten el despliegue y para crear una configuración de no administrador y un perfil de recuperación.
- **User Configuration Utility:** permite a un usuario cliente cambiar la frase de paso de UVM, para hacer que UVM reconozca las contraseñas de inicio de sesión de Windows, para actualizar los archivadores de claves y para registrar las huellas dactilares. Un usuario también puede crear copias de seguridad de los certificados digitales creados con IBM Embedded Security Subsystem.
- **User Verification Manager (UVM):** Client Security Software utiliza UVM para gestionar las frases de paso y otros elementos para autenticar los usuarios del sistema. Por ejemplo, UVM puede utilizar un lector de huellas dactilares para la autenticación del inicio de sesión. Client Security Software permite utilizar las características siguientes:
  - **Protección de política de cliente de UVM:** Client Security Software permite a un administrador de seguridad establecer la política de seguridad del cliente, que define la forma en la que se autentica un usuario cliente en el sistema.

    Si la política indica que son necesarias las huellas dactilares para el inicio de sesión y el usuario no tiene huellas dactilares registradas, se le dará la opción de registrar las huellas dactilares como parte del inicio de sesión. Asimismo, si es necesaria la comprobación de huellas dactilares y no hay ningún escáner conectado, UVM informará de un error. Además, si no se ha registrado la contraseña de Windows o, se ha registrado de forma incorrecta, con UVM, el usuario tendrá la oportunidad de proporcionar la contraseña de Windows correcta como parte del inicio de sesión.
  - **Protección de inicio de sesión del sistema de UVM:** Client Security Software permite a un administrador de seguridad controlar el acceso al sistema mediante una interfaz de inicio de sesión. La protección de UVM asegura que sólo los usuarios reconocidos por la política de seguridad pueden acceder al sistema operativo.

Relación entre contraseñas y claves

Las contraseñas y las claves trabajan juntas, junto con otros dispositivos de autenticación opcionales, para verificar la identidad de los usuarios del sistema. Comprender la relación entre las contraseñas y las claves es vital para comprender el funcionamiento de IBM Client Security Software.

Contraseña del administrador

La contraseña del administrador se utiliza para autenticar al administrador en IBM Embedded Security Subsystem. Esta contraseña, que debe tener una longitud de ocho caracteres, se mantiene y autentica dentro de los límites del hardware del subsistema de seguridad incorporado. Una vez autenticado, el administrador puede realizar las acciones siguientes:

- Inscribir usuarios
- Iniciar la interfaz de políticas
- Cambiar la contraseña del administrador

La contraseña del administrador se puede establecer de las formas siguientes:

- Mediante el Asistente de instalación de IBM Client Security
- Mediante Administrator Utility
- Mediante scripts
- Mediante la interfaz del BIOS (sólo sistemas ThinkCentre)

Es importante contar con una estrategia para la creación y mantenimiento de la contraseña del administrador. La contraseña del administrador se puede cambiar si la seguridad está en peligro o se ha olvidado la contraseña.

Para aquellos que están familiarizados con los conceptos y terminología del TCG (Trusted Computing Group), la contraseña del administrador es lo mismo que el valor de autorización del propietario. Como la contraseña del administrador está asociada a IBM Embedded Security Subsystem, a veces también se denomina *contraseña de hardware*.

Claves públicas y privadas de hardware

La premisa básica de IBM Embedded Security Subsystem es la de proporcionar una *raíz* de confianza muy fiable en un sistema cliente. Esta raíz se utiliza para proteger otras aplicaciones y funciones. Parte del proceso para establecer una raíz de confianza es la creación de una clave pública de hardware y una clave privada de hardware. Una clave pública y una privada, también denominadas *par de claves*, están relacionadas matemáticamente de tal forma que:

- Los datos cifrados con la clave pública sólo pueden descifrarse con la clave privada correspondiente.
- Los datos cifrados con la clave privada sólo pueden descifrarse con la clave pública correspondiente.

La clave privada de hardware se crea, almacena y utiliza dentro de los límites seguros del hardware del subsistema de seguridad. La clave pública de hardware está disponible para varios fines (de ahí el nombre de clave pública), pero nunca se expone fuera de los límites seguros del hardware del subsistema de seguridad. Las claves públicas y privadas de hardware son parte importante de la jerarquía de intercambio de claves de IBM descrita en un apartado más adelante.

Las claves públicas y privadas de hardware se crean de las formas siguientes:

- Mediante el Asistente de instalación de IBM Client Security
- Mediante Administrator Utility
- Mediante scripts

Para aquellos que están familiarizados con los conceptos y terminología del TCG (Trusted Computing Group), las claves públicas y privadas de hardware se conocen como la *clave raíz de almacenamiento* (SRK).

Claves públicas y privadas del administrador

Las claves públicas y privadas del administrador son parte integral de la jerarquía de intercambio de claves de IBM. También permiten efectuar copias de seguridad y restaurar datos específicos del usuario en caso de una anomalía en la placa del sistema o en el disco duro.

Las claves públicas y privadas del administrador pueden ser exclusivas en todos los sistemas o pueden ser comunes en todos los sistemas o grupos de sistemas. Hay que tener en cuenta que estas claves del administrador deben gestionarse, por lo que tener una estrategia para utilizar claves únicas en lugar de claves conocidas es importante.

Las claves públicas y privadas del administrador pueden crearse de una de las formas siguientes:

- Mediante el Asistente de instalación de IBM Client Security
- Mediante Administrator Utility
- Mediante scripts

Archivador ESS

Las claves públicas y privadas del administrador permiten efectuar copias de seguridad y restaurar datos específicos del usuario en caso de una anomalía en la placa del sistema o en el disco duro.

Claves públicas y privadas del usuario

IBM Embedded Security Subsystem crea claves públicas y privadas del usuario para proteger datos específicos del usuario. Estos pares de claves se crean cuando se inscribe un usuario en IBM Client Security Software. Estas claves se crean y gestionan de forma transparente mediante el componente User Verification Manager (UVM) de IBM Client Security Software. Las claves se gestionan basándose en el usuario de Windows que inicie una sesión en el sistema operativo.

Jerarquía de intercambio de claves de IBM

Un elemento esencial de la arquitectura de IBM Embedded Security Subsystem es la jerarquía de intercambio de claves de IBM. La base (o raíz) de la jerarquía de intercambio de claves de IBM la constituyen las claves públicas y privadas de hardware. Las claves públicas y privadas de hardware, denominadas el *par de claves de hardware*, son creadas por IBM Client Security Software y son estadísticamente únicas en cada cliente.

El siguiente “nivel” de claves hacia arriba en la jerarquía (después de la raíz) son las claves públicas y privadas del administrador o *par de claves del administrador*. El par de claves del administrador puede ser único en cada máquina o puede ser el mismo en todos los clientes o en un subconjunto de los clientes. La forma de gestionar este par de claves depende de cómo desea gestionar la red. La clave privada del administrador es única en cuanto a que reside en el sistema cliente (protegida por la clave pública de hardware) en una ubicación definida por el administrador.

IBM Client Security Software inscribe a los usuarios de Windows en el entorno Embedded Security Subsystem. Cuando se inscribe un usuario, se crean las claves públicas y privadas de usuario (el *par de claves de usuario*) y se crea un nuevo ″nivel″ de claves. La clave privada del usuario se cifra con la clave pública del administrador. La clave privada del administrador se cifra con la clave pública de

hardware. Por lo tanto, para utilizar la clave privada del usuario, debe estar cargada en el subsistema de seguridad la clave privada del administrador (que está cifrada con la clave pública de hardware). Una vez cargada en el chip, la clave privada de hardware descifra la clave privada del administrador. La clave privada del administrador está ahora lista para utilizarse dentro del subsistema de seguridad de modo que los datos que están cifrados con la clave pública del administrador correspondiente pueden intercambiarse dentro del subsistema de seguridad, descifrarse y utilizarse. La clave privada del usuario actual de Windows (cifrada con la clave pública del administrador) se pasa dentro del subsistema de seguridad. También se pasarán dentro del chip todos los datos que necesite una aplicación que aproveche el subsistema de seguridad incorporado, se descifrarán y se aprovecharán dentro del entorno seguro del subsistema de seguridad. Un ejemplo de esto lo constituye una clave privada utilizada para autenticar una red inalámbrica.

Siempre que se necesite una clave, ésta se intercambia dentro del subsistema de seguridad. Las claves privadas cifradas se intercambian dentro del subsistema de seguridad y después pueden utilizarse en el entorno protegido del chip. Las claves privadas no se muestran ni utilizan nunca fuera de este entorno de hardware. Esto permite proteger casi una cantidad ilimitada de datos mediante el chip IBM Security Chip incorporado.

Las claves privadas se cifran porque deben estar muy protegidas y porque hay un espacio de almacenamiento limitado en IBM Embedded Security Subsystem. En cualquier momento dado, sólo puede haber almacenadas en el subsistema de seguridad una pareja de claves. Las claves públicas y privadas de hardware son las únicas claves que permanecen almacenadas en el subsistema de seguridad de arranque a arranque. Para admitir varias claves y varios usuarios, CSS utiliza una jerarquía de intercambio de claves de IBM. Siempre que se necesite una clave, ésta se intercambia dentro de IBM Embedded Security Subsystem. Las claves privadas cifradas relacionadas se intercambian dentro del subsistema de seguridad y después pueden utilizarse en el entorno protegido del chip. Las claves privadas no se muestran ni utilizan nunca fuera de este entorno de hardware.

La clave privada del administrador se cifra con la clave pública de hardware. La clave privada de hardware, que sólo está disponible en el subsistema de seguridad, se utiliza para descifrar la clave privada del administrador. Una vez descifrada la clave privada del administrador en el subsistema de seguridad, puede pasarse dentro del subsistema de seguridad una clave privada de usuario (cifrada con la clave pública del administrador) y descifrarla con la clave privada del administrador. Pueden cifrarse varias claves privadas de usuario con la clave pública del administrador. Esto permite que haya prácticamente un número ilimitado de usuarios en un sistema con IBM ESS; sin embargo, se recomienda limitar la inscripción a 25 usuarios por sistema para garantizar un rendimiento óptimo.

IBM ESS utiliza una jerarquía de intercambio de claves en la que las claves públicas y privadas de hardware del subsistema de seguridad se utilizan para proteger otros datos almacenados fuera del chip. La clave privada de hardware se genera en el subsistema de seguridad y nunca abandona este entorno seguro. La clave pública de hardware está disponible fuera del subsistema de seguridad y se utiliza para cifrar o proteger otros elementos de datos como una clave privada. Una vez cifrados estos datos con la clave pública de hardware sólo pueden ser descifrados por la clave privada de hardware. Ya que la clave privada de hardware sólo está disponible en el entorno seguro del subsistema de seguridad, los datos cifrados sólo pueden descifrarse y utilizarse en este mismo entorno seguro. Es importante tener en cuenta que cada sistema tendrá una clave pública y privada de

hardware exclusivas. La posibilidad de números aleatorios de IBM Embedded Security Subsystem garantiza que cada par de claves de hardware sea estadísticamente único.

Características PKI (Public Key Infrastructure) de CSS

Client Security Software proporciona todos los componentes necesarios para crear una infraestructura de claves públicas (PKI) en su empresa, como:

- **Control del administrador sobre la política de seguridad del cliente.** La autenticación de los usuarios finales en el nivel del cliente es una cuestión importante de la política de seguridad. Client Security Software proporciona la interfaz necesaria para gestionar la política de seguridad de un cliente de IBM. Esta interfaz forma parte del software de autenticación User Verification Manager (UVM), que es el componente principal de Client Security Software.
- **Gestión de claves de cifrado para criptografía de claves públicas.** Los administradores crean claves de cifrado para el hardware del sistema y los usuarios cliente con Client Security Software. Cuando se crean claves de cifrado, se enlazan al chip IBM Security Chip incorporado mediante una jerarquía de claves, en la que se utiliza una clave de hardware de nivel base para cifrar las claves que están sobre ella, incluidas las claves de usuario que están asociadas con cada usuario cliente. El cifrado y almacenamiento de las claves en el chip IBM Security Chip incorporado añade una capa extra esencial de la seguridad del cliente, ya que las claves están enlazadas de una forma segura al hardware del sistema.
- **Creación y almacenamiento de certificados digitales protegidos por el chip IBM Security Chip incorporado.** Cuando se solicita un certificado digital que pueda utilizarse para la firma digital o cifrado de un mensaje de correo electrónico, Client Security Software permite elegir IBM Embedded Security Subsystem como proveedor de servicio criptográfico para las aplicaciones que utilicen Microsoft CryptoAPI. Estas aplicaciones incluyen Internet Explorer y Microsoft Outlook Express. Esto asegura que la clave privada del certificado digital se cifre con la clave pública de usuario en IBM Embedded Security Subsystem. Además, los usuarios de Netscape pueden elegir IBM Embedded Security Subsystem como el generador de claves privadas para los certificados digitales utilizados para seguridad. Las aplicaciones que utilizan PKCS#11 (Public-Key Cryptography Standard), como Netscape Messenger, pueden aprovecharse de la protección proporcionada por IBM Embedded Security Subsystem.
- **Posibilidad de transferir certificados digitales a IBM Embedded Security Subsystem.** La Herramienta de transferencia de certificados de IBM Client Security Software permite mover los certificados que se han creado con el CSP de Microsoft por omisión al CSP de IBM Embedded Security Subsystem. Esto aumenta enormemente la protección ofrecida a las claves privadas asociadas con los certificados porque éstos se almacenarán de forma segura en IBM Embedded Security Subsystem, en lugar de en un software vulnerable.

  Nota: los certificados digitales protegidos con el CSP de IBM Embedded Security Subsystem no se pueden exportar a otro CSP.
- **Un archivador de claves y una solución de recuperación.** Una función importante de PKI es la creación de un archivador de claves a partir del cual se pueden restaurar las claves si se pierden o dañan las originales. IBM Client Security Software proporciona una interfaz que permite definir un archivador para las claves y certificados digitales creados con IBM Embedded Security Subsystem y restaurar estas claves y los certificados si es necesario.

- **Cifrado de archivos y carpetas.** El cifrado de archivos y carpetas permite a un usuario cliente cifrar o descifrar archivos o carpetas. Esto proporciona un mayor nivel de seguridad de los datos añadido a las medidas de seguridad del sistema CSS.
- **Autenticación de huellas dactilares.** IBM Client Security Software soporta el lector de huellas dactilares PC card Targus y el lector de huellas dactilares USB Targus para la autenticación. Debe estar instalado Client Security Software antes de que se instalen los controladores de dispositivo de huellas dactilares de Targus para su funcionamiento correcto.
- **Autenticación de smart card.** IBM Client Security Software soporta determinadas smart cards como dispositivo de autenticación. Client Security Software permite utilizar las smart cards como una señal de autenticación para un sólo usuario a la vez. Cada smart card está enlazada a un sistema a menos que se utilice la itinerancia de credenciales. La utilización de una smart card hace que el sistema sea más seguro porque esta tarjeta debe proporcionarse junto con una contraseña.
- **Itinerancia de credenciales.** La itinerancia de credenciales permite que un usuario de red autorizado utilice cualquier sistema de la red, como si estuviese en su propia estación de trabajo. Después de que un usuario reciba autorización para utilizar UVM en cualquier cliente registrado en Client Security Software, podrá importar sus datos personales en cualquier otro cliente registrado de la red de itinerancia de credenciales. Después sus datos personales se actualizan y mantienen automáticamente en el archivador de CSS y en cualquier sistema en el que se hayan importado. Las actualizaciones de sus datos personales, como certificados nuevos o cambios de la frase de paso, están disponibles inmediatamente en todos los demás sistemas conectados a la red de itinerancia.
- **Certificación en FIPS 140-1.** Client Security Software soporta bibliotecas criptográficas certificadas en FIPS 140-1. Las bibliotecas RSA BSAFE certificadas en FIPS se utilizan en sistemas TCPA.
- **Caducidad de las frases de paso.** Client Security Software establece una frase de paso y una política de caducidad de frases de paso específica para cada usuario cuando éste se añade a UVM.

Capítulo 2. Cómo empezar

Este apartado contiene los requisitos de compatibilidad del hardware y software que puede utilizarse con IBM Client Security Software. También se proporciona información sobre cómo bajar IBM Client Security Software.

Requisitos de hardware

Antes de bajar e instalar el software, asegúrese de que el hardware del sistema es compatible con IBM Client Security Software.

La información más reciente sobre los requisitos de hardware y software está disponible en el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html.

IBM Embedded Security Subsystem

IBM Embedded Security Subsystem es un microprocesador criptográfico que está incorporado en la placa del sistema del cliente de IBM. Este componente esencial de IBM Client Security transfiere las funciones de política de seguridad de un software vulnerable a un hardware seguro, aumentando radicalmente la seguridad del cliente local.

Sólo los sistemas y estaciones de trabajo de IBM que contengan IBM Embedded Security Subsystem soportan IBM Client Security Software. Si intenta bajar e instalar el software en un sistema que no contenga IBM Embedded Security Subsystem, el software no se instalará o ejecutará correctamente.

Modelos de IBM soportados

Se concede licencia y soporte de Client Security Software para numerosos sistemas de sobremesa y portátiles de IBM. Para obtener una lista completa de los modelos soportados, consulte la página Web http://www.pc.ibm.com/us/security/index.html.

Requisitos de software

Antes de bajar e instalar el software, asegúrese de que el software y el sistema operativo del sistema son compatibles con IBM Client Security Software.

Sistemas operativos

IBM Client Security Software precisa uno de los sistemas operativos siguientes:

- Windows XP
- Windows 2000 Professional

Productos preparados para UVM

IBM Client Security incluye el software User Verification Manager (UVM) que permite personalizar la autenticación de su sistema de sobremesa. El primer nivel de control basado en política aumenta la protección de sus equipos y la eficiencia de la gestión de contraseñas. UVM, que es compatible con programas de políticas de seguridad para toda la empresa, permite utilizar productos preparados para UVM, incluidos los siguientes:

- **Dispositivos biométricos, como lectores de huellas dactilares**

UVM proporciona una interfaz conectar y listo para dispositivos biométricos. Debe instalar IBM Client Security Software *antes* de instalar un sensor preparado para UVM.

Para utilizar un sensor preparado para UVM que ya esté instalado en un cliente de IBM, debe desinstalar el sensor preparado para UVM, instalar IBM Client Security Software y después reinstalar el sensor preparado para UVM.

- **Tivoli Access Manager versiones 3.8 ó 3.9**

  El software UVM simplifica y mejora la gestión de políticas mediante una sencilla integración con una solución centralizada de control de accesos basada en política, como Tivoli Access Manager.

  El software UVM hace cumplir la política localmente, tanto si el sistema está en red (de sobremesa) o de forma autónoma, creando así un único modelo de política unificado.

- **Lotus Notes versión 4.5 o posterior**

  UVM trabaja con IBM Client Security Software para mejorar la seguridad del inicio de sesión de Lotus Notes (Lotus Notes versión 4.5 o posterior).

- **Entrust Desktop Solutions 5.1, 6.0 ó 6.1**

  El soporte de Entrust Desktop Solutions mejora las posibilidades de seguridad de Internet, de modo que los procesos corporativos críticos pueden trasladarse a Internet. Entrust Entelligence proporciona una sola capa de seguridad que puede englobar el conjunto completo de necesidades de seguridad mejorada de una corporación, incluidas la identificación, privacidad, verificación y gestión de seguridad.

- **RSA SecurID Software Token**

  RSA SecurID Software Token permite que el mismo registro de número generador que se utiliza en las señales de hardware RSA tradicionales se incorpore en las plataformas de usuario existentes. En consecuencia, los usuarios pueden autenticarse en los recursos protegidos accediendo al software incorporado en lugar de tener que utilizar dispositivos de autenticación dedicados.

- **Lector de huellas dactilares Targus**

  El lector de huellas dactilares Targus proporciona una interfaz sencilla que permite incluir la autenticación de huellas dactilares en la política de seguridad.

- **Tarjeta de identificación por contacto de Ensure**

  IBM Client Security Software 5.2 y superior requiere que los usuarios de tarjetas de identificación por contacto actualicen el software Ensure a la versión 7.41. Al actualizar IBM Client Security Software desde una versión anterior, actualice el software Ensure *antes* de actualizar a Client Security Software 5.2 o superior.

- **Lector de smart cards Gemplus GemPC400**

  El lector de smart cards Gemplus GemPC400 permite incluir la autenticación de smart cards en la política de seguridad, lo que añade una capa adicional de seguridad a la protección mediante frase de paso estándar.

Navegadores Web

IBM Client Security Software soporta los navegadores Web siguientes para solicitar certificados digitales:

- Internet Explorer 5.0 o posterior
- Netscape 4.51-4.7x y Netscape 7.1

Información del nivel cifrado del navegador

Si está instalado el soporte para un cifrado fuerte, utilice la versión de 128 bits del navegador Web. Para comprobar el nivel cifrado del navegador Web, consulte el sistema de ayuda proporcionado con el navegador.

Servicios criptográficos

IBM Client Security Software soporta los servicios criptográficos siguientes:

- **Microsoft CryptoAPI:** CryptoAPI es el servicio criptográfico por omisión para los sistemas operativos y aplicaciones de Microsoft. Con el soporte de CryptoAPI integrado, IBM Client Security Software permite utilizar las operaciones criptográficas de IBM Embedded Security Subsystem cuando se crean certificados digitales para aplicaciones de Microsoft.
- **PKCS#11:** PKCS#11 es el estándar criptográfico para Netscape, Entrust, RSA y otros productos. Después de instalar el módulo PKCS#11 de IBM Embedded Security Subsystem, puede utilizar IBM Embedded Security Subsystem para generar certificados digitales para Netscape, Entrust, RSA y otras aplicaciones que utilicen PKCS#11.

Aplicaciones de correo electrónico

IBM Client Security Software soporta los siguientes tipos de aplicaciones que utilizan correo electrónico seguro:

- Las aplicaciones de correo electrónico que utilizan Microsoft CryptoAPI para operaciones criptográficos, como Outlook Express y Outlook (cuando se utiliza con una versión soportada de Internet Explorer)
- Las aplicaciones de correo electrónico que utilizan PKCS#11 (Public Key Cryptographic Standard #11) para operaciones criptográficas, como Netscape Messenger (cuando se utiliza con una versión soportada de Netscape)

Cómo bajar el software

Client Security Software puede bajarse desde el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html.

Formulario de registro

Cuando baja el software, debe completar un formulario de registro y un cuestionario, y aceptar los términos de la licencia. Siga las instrucciones proporcionadas en el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html para bajar el software.

Los archivos de instalación de IBM Client Security Software están incluidos dentro del archivo autoextraíble denominado `csec53.exe`.

Normativas de exportación

IBM Client Security Software contiene código de cifrado que puede bajarse dentro de Norteamérica e internacionalmente. Si vive en un país en el que esté prohibido bajarse software de cifrado de un sitio Web de los Estados Unidos, no puede bajarse IBM Client Security Software. Para obtener más información sobre las normativas de exportación que regulan IBM Client Security Software, consulte el Apéndice A, “Normativas de exportación de los EE.UU. para Client Security Software”, en la página 49.

Capítulo 3. Antes de instalar el software

Este apartado contiene instrucciones sobre los requisitos previos para ejecutar el programa de instalación y configurar IBM Client Security Software en clientes de IBM.

Todos los archivos necesarios para la instalación de Client Security Software se proporcionan en el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html. El sitio Web proporciona información que ayuda a comprobar que su sistema tiene IBM Embedded Security Subsystem y que le permite seleccionar la oferta de IBM Client Security adecuada para su sistema.

Antes de instalar el software

El programa de instalación instala IBM Client Security Software en el cliente de IBM y habilita IBM Embedded Security Subsystem; no obstante, los detalles de la instalación varían en función de una serie de factores.

Instalación en clientes que ejecutan Windows XP y Windows 2000

Los usuarios de Windows XP y Windows 2000 deben iniciar una sesión con derechos de administrador para instalar IBM Client Security Software.

Instalación para utilizarlo con Tivoli Access Manager

Si tiene previsto utilizar Tivoli Access Manager para controlar los requisitos de autenticación para el sistema, debe instalar algunos componentes de Tivoli Access Manager *antes* de instalar IBM Client Security Software. Para obtener detalles, consulte el manual *Utilización de Client Security con Tivoli Access Manager*.

Consideraciones sobre las características de arranque

Hay dos características de arranque de IBM que pueden afectar la forma en la que se habilita IBM Embedded Security Subsystem y en la que se generan las claves de cifrado. Estas características son la contraseña del administrador y Seguridad ampliada y pueden accederse desde el programa Configuration/Setup Utility de un sistema de IBM. IBM Client Security Software tiene una contraseña del administrador aparte. Para evitar confusiones, la contraseña del administrador establecida en el programa Configuration/Setup Utility se denomina *contraseña del administrador del BIOS* en los manuales de Client Security Software.

Contraseña del administrador del BIOS

La contraseña del administrador del BIOS evita que las personas no autorizadas cambien los valores de configuración de un sistema de IBM. Esta contraseña se establece utilizando el programa Configuration/Setup Utility en un sistema NetVista o ThinkCentre o el programa IBM BIOS Setup Utility en un sistema ThinkPad. Puede acceder al programa apropiado pulsando F1 durante la secuencia de arranque del sistema. Esta contraseña se denomina Administrator Password (Contraseña del administrador) en los programas Configuration/Setup Utility e IBM BIOS Setup Utility.

Seguridad ampliada

Seguridad ampliada proporciona protección extra para la contraseña del administrador del BIOS, así como para los valores de la secuencia de arranque.

Puede determinar si Seguridad ampliada está habilitada o inhabilitada utilizando el programa Configuration/Setup Utility, al que se accede pulsando F1 durante la secuencia de arranque del sistema.

Para obtener más información sobre las contraseñas y Seguridad ampliada, consulte la documentación proporcionada con el sistema.

Seguridad ampliada en los modelos NetVista 6059, 6569, 6579, 6649 y todos los modelos NetVista Q1x: Si se ha establecido una contraseña del administrador en estos modelos NetVista (6059, 6569, 6579, 6649, 6646 y todos los modelos Q1x), debe abrir Administrator Utility para habilitar IBM Embedded Security Subsystem y generar las claves de cifrado.

Si Seguridad ampliada está habilitada en estos modelos, debe utilizar Administrator Utility para habilitar IBM Embedded Security Subsystem y generar las claves de cifrado *después* de instalar IBM Client Security Software. Si el programa de instalación detecta que Seguridad ampliada está habilitada, se le notificará al final del proceso de instalación. Reinicie el sistema y abra Administrator Utility para habilitar IBM Embedded Security Subsystem y generar las claves de cifrado.

Seguridad ampliada en todos los demás modelos NetVista (distintos de los modelos 6059, 6569, 6579, 6649 y de todos los modelos NetVista Q1x): Si se ha establecido una contraseña del administrador en otros modelos NetVista, *no* se le solicita que escriba la contraseña del administrador durante el proceso de instalación.

Si Seguridad ampliada está habilitada en estos modelos NetVista, puede utilizar el programa de instalación para instalar el software, pero debe utilizar el programa Configuration/Setup Utility para habilitar IBM Embedded Security Subsystem. *Después* de haber habilitado IBM Embedded Security Subsystem, puede utilizar Administrator Utility para generar las claves de cifrado.

Información sobre actualizaciones del BIOS

Antes de instalar el software, es posible que necesite bajarse el último código del BIOS (sistema de entrada/salida básico) para el sistema. Para determinar el nivel del BIOS que utiliza el sistema, reinicie el sistema y pulse F1 para iniciar el programa Configuration/Setup Utility. Cuando se abra el menú principal del programa Configuration/Setup Utility, seleccione Product Data (Datos del producto) para ver información sobre el código del BIOS. El nivel del código del BIOS también se denomina nivel de revisión de la EEPROM.

Para ejecutar IBM Client Security Software 2.1 o posterior en modelos NetVista (6059, 6569, 6579, 6649), debe utilizar el nivel del BIOS xxxx22axx o posterior; para ejecutar IBM Client Security Software 2.1 o posterior en modelos NetVista (6790, 6792, 6274, 2283), debe utilizar el nivel del BIOS xxxx20axx o posterior. Para obtener más información, consulte el archivo README incluido con el software bajado.

Para encontrar las últimas actualizaciones del código del BIOS para su sistema, acceda al sitio Web de IBM en http://www.pc.ibm.com/support, escriba `bios` en el campo Search (buscar) y seleccione downloads en la lista desplegable; después pulse Intro. Se muestra una lista de las actualizaciones del código del BIOS. Pulse el número de modelo adecuado y siga las instrucciones de la página Web.

Utilización del par de claves del administrador para archivar claves

El par de claves del archivador es simplemente una copia del par de claves del administrador que se almacena en un sistema remoto para su restauración. Ya que para crear el par de claves del archivador se utiliza Administrator Utility, debe instalar IBM Client Security Software en un cliente de IBM inicial antes de crear el par de claves del administrador.

Capítulo 4. Instalación, actualización y desinstalación del software

Este apartado contiene instrucciones para bajar, instalar y configurar IBM Client Security Software en clientes de IBM. Este apartado contiene también instrucciones para desinstalar el software. Asegúrese de instalar IBM Client Security Software antes de instalar cualquiera de los distintos programas de utilidad que amplían la funcionalidad de Client Security.

Importante: si va a actualizar desde una versión anterior a IBM Client Security Software 5.0, *debe* descifrar todos los archivos cifrados *antes* de instalar Client Security Software 5.1 o posterior. IBM Client Security Software 5.1 o posterior no puede descifrar los archivos que fueron cifrados utilizando versiones anteriores a Client Security Software 5.0, debido a cambios en su implementación del cifrado de archivos.

Cómo bajar e instalar el software

Todos los archivos necesarios para la instalación de Client Security Software se proporcionan en el sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html. El sitio Web proporciona información que ayuda a comprobar que su sistema tiene IBM Embedded Security Subsystem y que le permite seleccionar la oferta de IBM Client Security adecuada para su sistema.

Para bajarse los archivos adecuados para su sistema, complete el procedimiento siguiente:

1. Mediante un navegador Web, acceda al sitio Web de IBM en http://www.pc.ibm.com/us/security/index.html.
2. Pulse **Download instructions and links** (Instrucciones sobre descargas y enlaces).
3. En el área de información sobre descargas de IBM Client Security Software, pulse el botón **Continue** (Continuar).
4. Pulse **Detect my system & continue** (Detectar mi sistema y continuar) o entre el número de siete dígitos del modelo de tipo de máquina en el campo proporcionado.
5. Cree un ID de usuario, regístrese con IBM rellenando el formulario en línea y revise el Acuerdo de licencia; después pulse **Accept Licence** (Acepto la licencia).

   Se le redirigirá automáticamente a la página para bajarse IBM Client Security.
6. Siga los pasos de esta página para bajarse todos los controladores de dispositivo necesarios, los archivos readme, el software, los documentos de referencia y los programas de utilidad adicionales que constituyen IBM Client Security Software. Siga la secuencia para bajarlo especificada en el sitio Web.
7. En el escritorio de Windows, pulse **Inicio > Ejecutar**.
8. En el campo Ejecutar, escriba `d:\directory\csec53.exe`, donde d:\directorio\ es la letra de la unidad y el directorio donde se encuentra el archivo.
9. Pulse **Aceptar**.

   Se abre la ventana Bienvenido al Asistente de InstallShield para IBM Client Security Software.
10. Pulse **Siguiente**.

El asistente extraerá los archivos e instalará el software. Cuando se haya completado la instalación, se le dará la opción de reiniciar el sistema en ese momento o hacerlo más tarde.

11. Seleccione reiniciar el sistema ahora y pulse **Aceptar**.

    El Asistente de instalación de IBM Client Security Software se abrirá cuando se reinicie el sistema.

Utilización de asistente de instalación de IBM Client Security Software

El Asistente de instalación de IBM Client Security Software proporciona una interfaz que ayuda a instalar Client Security Software y a habilitar el chip IBM Security Chip incorporado. El Asistente de instalación de IBM Client Security Software también guía a los usuarios a través de las tareas necesarias relacionadas con la configuración de una política de seguridad en un cliente de IBM.

Estos pasos son los siguientes:

- **Establecimiento de una contraseña del administrador de seguridad**

  La contraseña del administrador de seguridad se utiliza para controlar el acceso a IBM Client Security Administrator Utility, que se utiliza para cambiar los valores de seguridad para este sistema. Esta contraseña debe tener exactamente una longitud de ocho caracteres.

- **Creación de las claves de seguridad del administrador**

  Las claves de seguridad del administrador son un conjunto de claves digitales que se almacenan en un archivo del sistema. Estos archivos de claves también se conocen como claves del administrador, par de claves del administrador o el par de claves del archivador. Es aconsejable que guarde estas claves de seguridad vitales en un disco o unidad extraíble. Cuando se hace un cambio en la política de seguridad en Administrator Utility, se le solicitará una clave del administrador para comprobar que el cambio de política está autorizado.

  También se guarda información de seguridad de copia de seguridad por si necesita alguna vez sustituir la placa del sistema o la unidad de disco duro del sistema. Almacene esta información de copia de seguridad en alguna parte fuera del sistema local.

- **Protección de aplicaciones con IBM Client Security**

  Seleccione las aplicaciones que desea proteger con IBM Client Security. Es posible que algunas opciones no estén disponibles si no tiene instaladas otras aplicaciones necesarias.

- **Autorización de los usuarios**

  Es necesario autorizar a los usuarios para que puedan acceder al sistema. Cuando autoriza a un usuario, debe especificar la frase de paso de ese usuario. No se permite que los usuarios no autorizados utilicen el sistema.

- **Selección de un nivel de seguridad del sistema**

  La selección de un nivel de seguridad permite establecer rápida y fácilmente una política de seguridad básica. Puede definir una política de seguridad personalizada posteriormente en IBM Client Security Administrator Utility.

Para utilizar el Asistente de instalación de IBM Client Security Software, complete el procedimiento siguiente:

1. Si el Asistente no está abierto ya, pulse **Inicio > Programas > Access IBM > IBM Client Security Software > Asistente de instalación de IBM Client Security**.

La pantalla Bienvenido al Asistente de instalación de IBM Client Security muestra una visión general de los pasos del asistente.

Nota: si tiene previsto utilizar autenticación de huellas dactilares, debe instalar el lector de huellas dactilares y el software antes de continuar.

2. Pulse **Siguiente** para comenzar a utilizar el asistente.

   Se muestra la pantalla Establecer la contraseña del administrador de seguridad.

3. Escriba la contraseña del administrador de seguridad en el campo Entre la contraseña del administrador y pulse **Siguiente**.

   Nota: durante la instalación inicial o después de haber borrado la información del chip IBM Security Chip incorporado, se le solicitará que confirme la contraseña del administrador de seguridad en el campo Confirme la contraseña del administrador. También es posible que se le solicite que proporcione la contraseña del supervisor, si es aplicable.

   Se muestra la pantalla Crear las claves de seguridad del administrador.

4. Efectúe una de las acciones siguientes:
   - **Crear claves de seguridad nuevas**

     Para crear claves de seguridad nuevas, utilice el procedimiento siguiente:

     a. Pulse el botón de selección **Crear claves de seguridad nuevas**.

     b. Especifique dónde desea guardar las claves de seguridad del administrador; para ello escriba el nombre de la vía de acceso en el campo que se proporciona o pulse **Examinar** y seleccione la carpeta adecuada.

     c. Si desea dividir la clave de seguridad para una mayor protección, pulse el recuadro de selección **Dividir la clave de seguridad de copia de seguridad para mejorar la seguridad** para que aparezca una marca de selección en él y después utilice las flechas para seleccionar el número deseado en el recuadro de desplazamiento **Número de divisiones**.

   - **Utilizar una clave de seguridad existente**

     Para utilizar una clave de seguridad existente, utilice el procedimiento siguiente:

     a. Pulse el botón de selección **Utilizar una clave de seguridad existente**.

     b. Especifique la ubicación de la clave pública; para ello escriba el nombre de la vía de acceso en el campo que se proporciona o pulse **Examinar** y seleccione la carpeta adecuada.

     c. Especifique la ubicación de la clave privada; para ello escriba el nombre de la vía de acceso en el campo que se proporciona o pulse **Examinar** y seleccione la carpeta adecuada.

5. Especifique dónde desea guardar las copias de seguridad de la información de seguridad; para ello escriba el nombre de la vía de acceso en el campo que se proporciona o pulse **Examinar** y seleccione la carpeta adecuada.

6. Pulse **Siguiente**.

   Se muestra la ventana Proteger las aplicaciones con IBM Client Security.

7. Habilite la protección de IBM Client Security; para ello seleccione los recuadros de selección adecuados para que aparezca una marca de selección en cada recuadro seleccionado y pulse **Siguiente**. Las selecciones disponibles de Client Security son las siguientes:

- **Proteger el acceso al sistema mediante la sustitución del inicio de sesión de Windows normal por el inicio de sesión seguro de Client Security**

  Seleccione este recuadro para sustituir el inicio de sesión de Windows normal por el inicio de sesión seguro de Client Security. Esto aumenta la seguridad del sistema y permite iniciar una sesión sólo después de haberse autenticado con el chip IBM Security Chip incorporado y dispositivos opcionales, como lectores de huellas dactilares o smart cards.
- **Habilitar el cifrado de archivos y carpetas**

  Seleccione este recuadro si desea proteger los archivos de la unidad de disco duro con el chip IBM Security Chip incorporado. Es necesario que baje el programa de utilidad Cifrado de archivos y carpetas de IBM Client Security.
- **Habilitar el soporte de IBM Client Security Password Manager**

  Seleccione este recuadro si desea utilizar IBM Password Manager para almacenar, de una forma cómoda y segura, las contraseñas para los inicios de sesión en sitios Web y para las aplicaciones. Es necesario que baje la aplicación IBM Client Security Password Manager.
- **Sustituir el inicio de sesión de Lotus Notes por el inicio de sesión de IBM Client Security**

  Seleccione este recuadro si desea que Client Security autentique los usuarios de Lotus Notes mediante el chip IBM Security Chip incorporado.
- **Habilitar el soporte de Entrust**

  Seleccione este recuadro si desea habilitar la integración con los productos de software de seguridad de Entrust.
- **Proteger Microsoft Internet Explorer**

  Esta protección permite proteger las comunicaciones de correo electrónico y la navegación en la Web con Microsoft Internet Explorer (se necesita un certificado digital). El soporte de Microsoft Internet Explorer está habilitado por omisión.

Después de haber seleccionado los recuadros de selección adecuados, se muestra la pantalla Autorizar a los usuarios.

8. Complete la pantalla Autorizar a los usuarios mediante uno de los procedimientos siguientes:
   - Para autorizar a los usuarios para que utilicen las funciones de IBM Client Security, haga lo siguiente:
     a. Seleccione un usuario en el área Usuarios no autorizados.
     b. Pulse **Autorizar usuario**.
     c. Escriba y confirme la frase de paso de IBM Client Security en los campos proporcionados y pulse **Siguiente**.

        Aparece la pantalla Caducidad de la frase de paso de UVM.
     d. Establezca la caducidad de la frase de paso para el usuario y pulse **Finalizar**.
     e. Pulse **Siguiente**.
   - Para quitar la autorización a los usuarios para que utilicen las funciones de IBM Client Security, haga lo siguiente:
     a. Seleccione un usuario en el área Usuarios autorizados.
     b. Pulse **Desautorizar usuario**.

        Aparece el mensaje ″¿Está seguro de que desea desautorizarlo?″.
     c. Pulse **Sí**.

d. Pulse **Siguiente**.

Se muestra la pantalla Seleccionar el nivel de seguridad del sistema.

9. Seleccione un nivel de seguridad del sistema efectuando una de las acciones siguientes:
   - Seleccione los requisitos de autenticación deseados pulsando los recuadros de selección adecuados. Puede seleccionar más de un requisito de autenticación. El recuadro de selección **Utilizar frase de paso de UVM** aparece seleccionado por omisión.
   - El controlador del dispositivo de lectura de huellas dactilares y el del lector de smart cards deben estar instalados antes de iniciar el Asistente de instalación de IBM Client Security para que estos dispositivos estén disponibles en el Asistente de instalación.
   - Seleccione un nivel de seguridad del sistema arrastrando el selector deslizante al nivel de seguridad deseado y pulse **Siguiente**.

     Nota: puede definir una política de seguridad personalizada posteriormente utilizando el Editor de política en Administrator Utility.
10. Revise los valores de seguridad y efectúe una de las acciones siguientes:
    - Para aceptar los valores, pulse **Finalizar**.
    - Para cambiar los valores, pulse **Atrás** y haga los cambios apropiados; después vuelva a esta pantalla y pulse **Finalizar**.

    IBM Client Security Software configurar los valores mediante el chip IBM Security Chip incorporado. Se muestra un mensaje confirmando que el sistema está protegido ahora por IBM Client Security.
11. Pulse **Aceptar**.

    Ahora puede instalar y configurar los programas de utilidad IBM Client Security Password Manager y Cifrado de archivos y carpetas de IBM Client Security.

Habilitación de IBM Security Subsystem

IBM Security Subsystem debe estar habilitado antes de que se pueda utilizar Client Security Software. Si no se ha habilitado el chip, puede habilitarlo utilizando Administrator Utility. Puede encontrar instrucciones sobre la utilización del Asistente de instalación en el apartado anterior.

Para habilitar IBM Security Subsystem mediante Administrator Utility, complete el procedimiento siguiente:

1. Pulse **Inicio > Configuración > Panel de control > IBM Embedded Security Subsystem**.

   Aparece una pantalla que muestra un mensaje indicando que IBM Security Subsystem no se ha habilitado y que pregunta si desea habilitarlo.
2. Pulse **Sí**.

   Se muestra un mensaje indicando que si tiene habilitada una contraseña del supervisor o una contraseña del administrador del BIOS, debe inhabilitarla en el programa BIOS Setup Utility antes de continuar.
3. Efectúe una de las acciones siguientes:
   - Si tiene habilitada una contraseña del supervisor, pulse **Cancelar**, inhabilite la contraseña del supervisor y después complete este procedimiento.
   - Si no tiene habilitada una contraseña del supervisor, pulse **Aceptar** para continuar.
4. Cierre todas las aplicaciones abiertas y pulse **Aceptar** para reiniciar el sistema.

5. Después de que se reinicie el sistema, pulse **Inicio > Configuración > Panel de control > IBM Embedded Security Subsystem** para abrir Administrator Utility.

   Se muestra un mensaje indicando que IBM Security Subsystem no se ha configurado o se ha borrado su información. En este momento se necesita una contraseña nueva.
6. Entre y confirme una contraseña del administrador nueva en los campos adecuados y pulse **Aceptar**.

   Nota: la contraseña debe tener una longitud de ocho caracteres.

   Se completa la operación y se muestra la pantalla principal de Administrator Utility.

Instalación del software en otros clientes de IBM cuando está disponible la clave pública del administrador - sólo instalaciones desatendidas

Si ha instalado el software en el primer cliente de IBM y ha creado un par de claves del administrador, puede instalar el software y habilitar el subsistema de seguridad en otros clientes de IBM mediante el programa de instalación.

Durante la instalación, debe elegir una ubicación para la clave pública del administrador, la clave privada del administrador y para el archivador de claves. Si desea utilizar una clave pública del administrador que se encuentra en un directorio compartido o guardar el archivador de claves en un directorio compartido, primero debe correlacionar una letra de unidad con el directorio de destino, antes de poder utilizar el programa de instalación. Para obtener información sobre cómo correlacionar una letra de unidad con un recurso de red compartido, consulte la documentación de su sistema operativo Windows.

Instalación desatendida

Una instalación desatendida permite al administrador instalar Client Security Software en un cliente de IBM remoto sin tener que ir físicamente al sistema cliente.

Antes de iniciar una instalación desatendida, lea el Capítulo 3, “Antes de instalar el software”, en la página 13. No se muestra ningún mensaje de error durante las instalaciones desatendidas. Si una instalación desatendida termina de forma prematura, debe efectuar una instalación atendida para ver los mensajes de error que pudieran aparecer.

Nota: los usuarios deben iniciar una sesión con derechos de usuario administrador para instalar Client Security Software.

Despliegue masivo

El despliegue masivo permite a los administradores de seguridad iniciar la política de seguridad en varios sistemas simultáneamente. Esto facilita la gestión y despliegue de medidas de seguridad y ayuda a garantizar que se implementan las políticas de seguridad correctas.

Los controladores de dispositivo siguientes deben instalarse antes de completar el procedimiento de despliegue masivo:

- El controlador de dispositivo del bus SM
- El controlador de dispositivo Atmel TPM (para sistemas TCPA)

Hay dos pasos principales para efectuar un despliegue masivo:
- Instalación masiva
- Configuración masiva

Instalación masiva

Debe efectuar una instalación desatendida para instalar IBM Client Security Software en varios clientes simultáneamente. Debe utilizar el parámetro de instalación desatendida cuando inicie un despliegue masivo.

Para iniciar una instalación masiva, complete el procedimiento siguiente:

1. Cree el archivo `csec.ini`.

   El archivo `csec.ini` se crea cuando el usuario completa el Asistente de instalación de IBM Client Security. Este paso sólo es necesario si desea efectuar una configuración masiva. Consulte “Configuración masiva” en la página 24 para obtener más detalles.
2. Extraiga el contenido del paquete de instalación de CSS con Winzip utilizando los nombres de carpeta.
3. Edite las entradas `szIniPath` y `szDir`, que son necesarias para una configuración masiva, en el archivo `Setup.iss`.

   El contenido completo de este archivo se lista a continuación. La ubicación de la carpeta se establece en el parámetro `szIniPath` del archivo `csec.ini`. El parámetro `szIniPath` sólo es necesario si desea efectuar una configuración masiva.
4. Copie los archivos en el sistema de destino.
5. Cree la sentencia de línea de mandatos `\setup -s`.

   Esta sentencia de línea de mandatos debe ejecutarse desde el escritorio de un usuario que tenga derechos de administrador. El grupo de programas Inicio o la clave Run es un buen lugar para hacerlo.
6. Elimine la sentencia de línea de mandatos en el siguiente arranque.

A continuación se lista el contenido completo del archivo `Setup.iss` con algunas descripciones, archivo incluido en el contenido del paquete de instalación de CSS extraído más arriba:

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szIniPath=d:\csssetup.ini
(El parámetro anterior es el nombre y la ubicación del archivo .ini, que es necesario
para la configuración masiva. Si es una unidad de red, debe estar correlacionada.
Cuando no se vaya a utilizar una configuración masiva con una instalación
silenciosa, elimine esta entrada).
[File Transfer]
OverwrittenReadOnly=NoToAll
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder]
Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0
Count=4
Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0
Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0
Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0
```

[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:\Archivos de programa\IBM\Security
(El parámetro anterior es el directorio usado para instalar Client Security. Debe ser un directorio local del sistema).
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0]
szFolder=IBM Client Security Software
(El parámetro anterior es el grupo de programas de Client Security).
Result=1
[Application]
Name=Client Security
Version=5.00.002f
Company=IBM
Lang=0009
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0]
Result=6
BootOption=3

Configuración masiva

El archivo siguiente también es esencial a la hora de iniciar una configuración masiva. El archivo puede tener cualquier nombre, siempre que tenga una extensión .ini. A continuación se muestra el contenido que debería tener el archivo. A un lado aparece una breve descripción que no debe incluirse en el archivo. El mandato siguiente ejecuta este archivo desde la línea de mandatos cuando la configuración masiva no se efectúa junto con una instalación masiva:

```
<Carpeta instalación CSS>\acamucli /ccf:c:\csec.ini
```

Nota: si cualquier archivo o vía de acceso está en una unidad de red, la unidad debe estar correlacionada con una letra.

[CSSSetup]	Cabecera de la sección para la configuración de CSS.
suppw=bootup	Contraseña del administrador/supervisor del BIOS. Déjela en blanco si no es necesaria.
hwpw=11111111	Contraseña del administrador para IBM Embedded Security Subsystem. Debe tener ocho caracteres. Es siempre necesaria. Debe ser correcta si ya se ha establecido una contraseña del administrador.
newkp=1	1 para generar un par de claves del administrador nuevo 0 para utilizar un par de claves del administrador existente.
keysplit=1	Cuando `newkp` es 1, este parámetro determina el número de componentes de clave privada. **Nota:** si el par de claves existente utiliza varias partes de clave privada, todas las partes de clave privada deben almacenarse en el mismo directorio.
kpl=c:\jgk	Ubicación del par de claves del administrador cuando `newkp` es 1, si es una unidad de red debe estar correlacionada.
kal=c:\jgk\archive	Ubicación del archivador de claves de usuario, si es una unidad de red debe estar correlacionada.
pub=c:\jk\admin.key	Ubicación de la clave pública del administrador cuando se utiliza un par de claves del administrador existente, si es una unidad de red debe estar correlacionada.
pri=c:\jk\private1.key	Ubicación de la clave privada del administrador cuando se utiliza un par de claves del administrador existente, si es una unidad de red debe estar correlacionada.

wiz=0	Determina si este archivo ha sido generado por el Asistente de instalación de CSS. Esta entrada no es necesaria. Si la incluye en el archivo el valor debería ser 0.
clean=0	1 para suprimir el archivo .ini después de la inicialización, 0 para dejar el archivo .ini después de la inicialización.
enableroaming=1	1 para habilitar la itinerancia para el cliente, 0 para inhabilitar la itinerancia para el cliente.
username= [promptcurrent]	[promptcurrent] para solicitar al usuario actual la contraseña de registro del cliente itinerante. [current] cuando la contraseña de registro del cliente itinerante para el usuario actual es proporcionada por la entrada `sysregpwd` y el usuario actual ha sido autorizado para registrar el sistema con el servidor de itinerancia. [<cuenta de usuario específica>] si el usuario especificado ha sido autorizado para registrar el sistema con el servidor de itinerancia y si la contraseña de registro del sistema para ese usuario es proporcionada por la entrada `sysregpwd`. No utilice esta entrada si el valor de `enableroaming` es 0, o si la entrada `enableroaming` no está presente.
sysregpwd=12345678	Contraseña de registro del sistema. Establezca este valor con la contraseña correcta para permitir que el sistema se registre con el servidor de itinerancia. No incluya esta entrada si el valor `username` está establecido en [promptcurrent] o si la entrada `username` no está presente.
[UVMEnrollment]	Cabecera de la sección para la inscripción de usuarios.
enrollall=0	1 para inscribir todas las cuentas de usuarios locales en UVM, 0 para inscribir cuentas de usuarios específicos en UVM.
defaultuvmpw=arriba	Cuando `enrollall` es 1, esta es la frase de paso de UVM para todos los usuarios.
defaultwinpw=abajo	Cuando `enrollall` es 1, esta es la contraseña de Windows registrada con UVM para todos los usuarios.
defaultppchange=0	Cuando `enrollall` es 1, esta entrada establecerá la política de cambio de frases de paso de UVM para todos los usuarios. 1 para pedir al usuario que cambie la frase de paso de UVM en el siguiente inicio de sesión, 0 para no pedir al usuario que cambie la frase de paso de UVM en el siguiente inicio de sesión.
defaultppexppolicy=1	Cuando `enrollall` es 1, esta entrada establecerá la política de caducidad de frases de paso de UVM para todos los usuarios. 0 para indicar que la frase de paso de UVM caduca 1 para indicar que la frase de paso de UVM no caduca
defaultppexpdays=0	Cuando `enrollall` es 1, esta entrada establecerá el número de días hasta que caduque la frase de paso de UVM para todos los usuarios. Cuando `ppexppolicy` esté establecida en 0, establezca este valor para indicar el número de días hasta que caduque la frase de paso de UVM.
enrollusers=2	Cuando `enrollall` es 0, este es el número de usuarios que se inscribirán en UVM.

user1=juan	Enumere el número de usuarios que se van a inscribir, empezando por 1; los nombres de usuario deben ser los nombres de las cuentas. Para obtener el nombre real de la cuenta en Windows 2000, haga lo siguiente: 1. Inicie Administración de equipos (Administrador de dispositivos). 2. Expanda el nodo Usuarios locales y grupos. 3. Abra la carpeta Usuarios. Los elementos listados en la columna Nombre son los nombres de las cuentas. Para obtener el nombre real de la cuenta en Windows XP desde el Panel de control de Windows, pulse el icono **Cuentas de usuario**. Se muestran las cuentas de usuario.
user1uvmpw=cromo	Enumere la frase de paso de UVM del número de usuarios que se van a inscribir, empezando por 1.
user1winpw=redondo	Enumere la contraseña de Windows registrada con UVM del número de usuarios que se van a inscribir, empezando por 1.
user1domain=0	0 para indicar que esta cuenta es local, 1 para indicar que esta cuenta está en el dominio.
user1ppchange=0	1 para pedir al usuario que cambie la frase de paso de UVM en el siguiente inicio de sesión, 0 para no pedir al usuario que cambie la frase de paso de UVM en el siguiente inicio de sesión.
user1ppexppolicy=1	0 para indicar que la frase de paso de UVM caduca, 1 para indicar que la frase de paso de UVM no caduca.
user1ppexpdays=0	Cuando ppexppolicy esté establecida en 0, establezca este valor para indicar el número de días hasta que caduque la frase de paso de UVM.
user2=elena user2uvmpw=izda user2winpw=dcha user2domain=0 user2ppchange=1 user2ppexppolicy=0 user2ppexpdays=90	
[UVMAppConfig]	Cabecera de la sección para la configuración de aplicaciones y módulos preparados para UVM.
uvmlogon=0	1 para utilizar la protección de inicio de sesión de UVM, 0 para utilizar el inicio de sesión de Windows.
entrust=0	1 para utilizar UVM para la autenticación de Entrust, 0 para utilizar la autenticación de Entrust.
notes=1	1 para habilitar el soporte de Lotus Notes, 0 para inhabilitar el soporte de Lotus Notes.
netscape=0	1 para firmar y cifrar los correos electrónicos con el módulo IBM PKCS#11, 0 para no firmar ni cifrar los correos electrónicos con el módulo IBM PKCS#11.
passman=0	1 para utilizar Password Manager, 0 para no utilizar Password Manager
folderprotect=0	1 para utilizar Cifrado de archivos y carpetas, 0 para no utilizar Cifrado de archivos y carpetas.

Actualización de la versión de Client Security Software

Los clientes que tengan instaladas versiones anteriores de Client Security Software deberían actualizar su software a esta versión para aprovechar las nuevas características de Client Security.

Importante: los sistemas TCPA que tuvieran instalado IBM Client Security Software Versión 4.0x deben desinstalar IBM Client Security Software Versión 4.0x y borrar la información del chip antes de instalar esta versión de IBM Client Security Software. El no hacerlo puede producir un error de instalación o que el software no responda.

Actualización utilizando nuevos datos de seguridad

Si desea eliminar por completo Client Security Software y empezar de cero, complete el procedimiento siguiente:

1. Desinstale la versión anterior de Client Security Software utilizando el applet Agregar o quitar programas del Panel de control.
2. Rearranque el sistema.
3. Borre la información del chip IBM Security Chip incorporado mediante el programa BIOS Setup Utility.
4. Rearranque el sistema.
5. Instale Client Security Software Release 5.1 y configúrelo utilizando el Asistente de instalación de IBM Client Security Software.

Actualización desde la versión 5.1 a versiones posteriores utilizando datos de seguridad existentes

Si desea actualizar desde Client Security Software Versión 5.1 a versiones posteriores del software utilizando los datos de seguridad existentes, complete el procedimiento siguiente:

1. Actualice el archivador completando los pasos siguientes:
   a. Pulse **Inicio > Programas > Access IBM > IBM Client Security Software > Modificar los valores de seguridad**.
   b. Pulse el botón **Actualizar archivador de claves** para asegurar que la información de copia de seguridad se actualiza.

      Anote el directorio del archivador.
   c. Salga de IBM Client Security Software User Configuration Utility.
2. Elimine la versión existente de Client Security Software completando los pasos siguientes:
   a. En el escritorio de Windows, pulse **Inicio > Ejecutar**.
   b. En el campo Ejecutar, escriba `d:\directorio\csec5xxus_00yy.exe`, donde d:\directorio\ es la letra de la unidad y el directorio donde se encuentra el archivo ejecutable. `xx` e `yy` son alfanuméricos.
   c. Seleccione **Actualizar**.
   d. Rearranque el sistema.

Desinstalación de Client Security Software

Asegúrese de desinstalar los distintos programas de utilidad (IBM Client Security Password Manager, programa de utilidad Cifrado de archivos y carpetas (FFE) de IBM Client Security) que amplían la funcionalidad de Client Security antes de desinstalar IBM Client Security Software. Los usuarios deben iniciar una sesión con derechos de administrador para desinstalar Client Security Software.

Nota: debe desinstalar todos los programas de utilidad de IBM Client Security Software y todo el software de los sensores preparados para UVM antes de desinstalar IBM Client Security Software. La contraseña del administrador es necesaria para desinstalar Client Security Software.

Para desinstalar Client Security Software, complete el procedimiento siguiente:

1. Cierre todos los programas Windows.
2. En el escritorio de Windows, pulse **Inicio > Configuración > Panel de control**.
3. Pulse el icono **Agregar o quitar programas**.
4. En la lista de software que puede eliminarse automáticamente, seleccione **IBM Client Security**.
5. Pulse **Agregar o quitar**.
6. Seleccione el botón de selección **Quitar**.
7. Pulse **Siguiente** para desinstalar el software.
8. Pulse **Aceptar** para confirmar esta acción.
9. Escriba la contraseña del administrador en la interfaz proporcionada y pulse **Aceptar**.
10. Efectúe una de las acciones siguientes:
    - Si ha instalado el módulo PKCS#11 del chip IBM Security Chip incorporado para Netscape, se muestra un mensaje que le pide que inicie el proceso para inhabilitar el módulo PKCS#11 del chip IBM Security Chip incorporado. Pulse **Sí** para continuar.

      Se mostrará una serie de mensajes. Pulse **Aceptar** para cada mensaje hasta que se haya eliminado el módulo PKCS#11 del chip IBM Security Chip.
    - Si no ha instalado el módulo PKCS#11 del chip IBM Security Chip incorporado para Netscape, se muestra un mensaje que le pregunta si desea suprimir los archivos DLL compartidos que se instalaron con Client Security Software.

      Pulse **Sí** para desinstalar estos archivos o pulse **No** para dejarlos instalados. El hecho de dejar los archivos instalados no tiene ningún efecto sobre el funcionamiento normal del sistema.

    Aparece el mensaje ″¿Desea eliminar la información del sistema del archivador?″. Si selecciona **No**, puede restaurar la información cuando reinstale la versión más reciente de IBM Client Security Software.
11. Pulse **Finalizar** después de que se elimine el software.

    Debe reiniciar el sistema después de desinstalar Client Security Software.

Cuando desinstala Client Security Software, elimina todos los componentes de software instalados de Client Security además de todas las claves de usuario, certificados digitales, huellas dactilares registradas y contraseñas almacenadas.

Capítulo 5. Resolución de problemas

El apartado siguiente presenta información que es útil para prevenir o identificar y corregir problemas que podrían surgir mientras se utiliza Client Security Software.

Funciones del administrador

Este apartado contiene información que un administrador podría encontrar útil a la hora de configurar y utilizar Client Security Software.

IBM Client Security Software sólo puede utilizarse en sistemas IBM que contengan IBM Embedded Security Subsystem. Este software consta de aplicaciones y componentes que permiten a los clientes de IBM proteger su información confidencial mediante hardware de seguridad en lugar de mediante software, más vulnerable.

Autorización de los usuarios

Antes de proteger la información de usuarios cliente, IBM Client Security Software **debe** estar instalado en el cliente y los usuarios **deben** estar autorizados para utilizar el software. Un Asistente de instalación de fácil uso le guiará en todo el proceso de instalación.

Importante: al menos un usuario cliente **debe** estar autorizado para utilizar UVM durante la instalación. Si no se autoriza a ningún usuario para utilizar UVM al configurar inicialmente Client Security Software, **no** se aplicarán sus valores de seguridad y la información **no** se protegerá.

Si ha terminado el Asistente de instalación sin autorizar a ningún usuario, concluya y reinicie el sistema; a continuación ejecute el cliente Asistente de instalación de Client Security desde el menú Inicio de Windows y autorice a un usuario de Windows para que utilice UVM. De esta forma permite a IBM Client Security Software aplicar los valores de seguridad y proteger su información confidencial.

Supresión de usuarios

Cuando suprime un usuario, el nombre del usuario se suprime de la lista de usuarios en Administrator Utility.

Establecimiento de una contraseña del administrador del BIOS (ThinkCentre)

Los valores de seguridad que están disponibles en el programa Configuration/Setup Utility permiten a los administradores hacer lo siguiente:

- Habilitar o inhabilitar IBM Embedded Security Subsystem
- Borrar la información de IBM Embedded Security Subsystem

Atención:

- Cuando se borra la información de IBM Embedded Security Subsystem, se pierden todas las claves de cifrado y los certificados almacenados en el subsistema.

Ya que se accede a los valores de seguridad mediante el programa Configuration/Setup Utility del sistema, establezca una contraseña del administrador para impedir que los usuarios no autorizados cambien estos valores.

Para establecer una contraseña del administrador del BIOS:

1. Concluya y reinicie el sistema.
2. Cuando aparezca en pantalla el indicador del programa Configuration/Setup Utility, pulse **F1**.

   Se abre el menú principal del programa Configuration/Setup Utility.
3. Seleccione **System Security** (Seguridad del sistema).
4. Seleccione **Administrator Password** (Contraseña del administrador).
5. Escriba la contraseña y pulse la flecha abajo en el teclado.
6. Vuelva a escribir la contraseña y pulse la flecha abajo.
7. Seleccione **Change Administrator password** (Cambiar la contraseña del administrador) y pulse Intro; después pulse Intro de nuevo.
8. Pulse **Esc** para salir y guardar los valores.

Después de establecer una contraseña del administrador del BIOS, se le solicitará cada vez que intente acceder al programa Configuration/Setup Utility.

Importante: conserve un registro de la contraseña del administrador del BIOS en un lugar seguro. Si pierde u olvida la contraseña del administrador del BIOS, no podrá acceder al programa Configuration/Setup Utility y no podrá cambiar o suprimir la contraseña del administrador del BIOS sin extraer la cubierta del sistema y mover un puente en la placa del sistema. Consulte la documentación del hardware incluida con el sistema para obtener más información.

Establecimiento de una contraseña del supervisor (ThinkPad)

Los valores de seguridad que están disponibles en el programa IBM BIOS Setup Utility permiten a los administradores efectuar las tareas siguientes:

- Habilitar o inhabilitar IBM Embedded Security Subsystem
- Borrar la información de IBM Embedded Security Subsystem

Atención:

- Es necesario inhabilitar temporalmente la contraseña del supervisor en algunos modelos de ThinkPad antes de instalar o actualizar Client Security Software.

Después de configurar Client Security Software, establezca una contraseña del supervisor para impedir que los usuarios no autorizados cambien estos valores.

Para establecer una contraseña del supervisor, complete uno de los procedimientos siguientes:

Ejemplo 1

1. Concluya y reinicie el sistema.
2. Cuando aparezca en pantalla el indicador del programa Setup Utility, pulse F1.

   Se abre el menú principal del programa Setup Utility.
3. Seleccione **Password** (Contraseña).
4. Seleccione **Supervisor Password** (Contraseña del supervisor).
5. Escriba la contraseña y pulse Intro.
6. Escriba la contraseña de nuevo y pulse Intro.
7. Pulse **Continue** (Continuar).
8. Pulse F10 para guardar y salir.

Ejemplo 2

1. Concluya y reinicie el sistema.
2. Cuando aparezca el mensaje ″To interrupt normal startup, press the blue Access IBM button″ (Para interrumpir el arranque normal, pulse el botón Access IBM azul), pulse el botón Access IBM azul.

   Se abre Access IBM Predesktop Area.
3. Efectúe una doble pulsación en **Start setup utility** (Iniciar programa de utilidad de configuración).
4. Seleccione **Security** (Seguridad) utilizando las teclas direccionales para desplazarse hacia abajo por el menú.
5. Seleccione **Password** (Contraseña).
6. Seleccione **Supervisor Password** (Contraseña del supervisor).
7. Escriba la contraseña y pulse Intro.
8. Escriba la contraseña de nuevo y pulse Intro.
9. Pulse **Continue** (Continuar).
10. Pulse F10 para guardar y salir.

Después de establecer una contraseña del supervisor, se le solicitará cada vez que intente acceder al programa BIOS Setup Utility.

Importante: conserve un registro de la contraseña del supervisor en un lugar seguro. Si pierde u olvida la contraseña del supervisor, no podrá acceder al programa IBM BIOS Setup Utility y no podrá cambiar o suprimir la contraseña. Consulte la documentación del hardware incluida con el sistema para obtener más información.

Protección de la contraseña del administrador

La contraseña del administrador protege el acceso a Administrator Utility. Proteja la contraseña del administrador para impedir que los usuarios no autorizados cambien valores en Administrator Utility.

Borrado de la información de IBM Embedded Security Subsystem (ThinkCentre)

Si desea borrar todas las claves de cifrado del usuario de IBM Embedded Security Subsystem y borrar la contraseña del administrador para el subsistema, debe borrar la información del chip. Lea la información que se detalla a continuación antes de borrar la información de IBM Embedded Security Subsystem.

Atención:

- Cuando se borra la información de IBM Embedded Security Subsystem, se pierden todas las claves de cifrado y los certificados almacenados en el subsistema.

Para borrar la información de IBM Embedded Security Subsystem, complete el procedimiento siguiente:

1. Concluya y reinicie el sistema.
2. Cuando aparezca en pantalla el indicador del programa Setup Utility, pulse F1.

   Se abre el menú principal del programa Setup Utility.
3. Seleccione **Security** (Seguridad).
4. Seleccione **IBM TCPA Feature Setup** (Configuración de la función IBM TCPA).

5. Seleccione **Clear IBM TCPA Security Feature** (Borrar la función de seguridad IBM TCPA) y pulse Intro.
6. Seleccione **Yes** (Sí).
7. Pulse F10 y seleccione **Yes** (Sí).
8. Pulse Intro. Se reiniciará el sistema.

Borrado de la información de IBM Embedded Security Subsystem (ThinkPad)

Si desea borrar todas las claves de cifrado del usuario de IBM Embedded Security Subsystem y borrar la contraseña del administrador, debe borrar la información del subsistema. Lea la información que se detalla a continuación antes de borrar la información de IBM Embedded Security Subsystem.

Atención:

- Cuando se borra la información de IBM Embedded Security Subsystem, se pierden todas las claves de cifrado y los certificados almacenados en el subsistema.

Para borrar la información de IBM Embedded Security Subsystem, complete el procedimiento siguiente:

1. Concluya el sistema.
2. Pulse y mantenga pulsada la tecla Fn cuando se reinicia el sistema.
3. Cuando aparezca en pantalla el indicador del programa Setup Utility, pulse F1.
   Se abre el menú principal del programa Setup Utility.
4. Seleccione **Config** (Configurar).
5. Seleccione **IBM Security Chip**.
6. Seleccione **Clear IBM Security Chip** (Borrar el chip IBM Security Chip).
7. Seleccione **Yes** (Sí).
8. Pulse Intro para continuar.
9. Pulse F10 para guardar y salir.

Limitaciones o problemas conocidos de CSS Versión 5.2

La información siguiente puede ser de ayuda cuando utilice las características de Client Security Software Versión 5.2.

Limitaciones de itinerancia

Utilización de un servidor de itinerancia CSS

El mensaje de solicitud de contraseña del administrador de CSS aparecerá siempre que alguien intente iniciar la sesión en el servidor de itinerancia CSS. No obstante, se puede utilizar el sistema con normalidad sin entrar esta contraseña.

Utilización de IBM Security Password Manager en un entorno de itinerancia

Las contraseñas almacenadas en un sistema que utilice IBM Client Security Password Manager se pueden utilizar en otros sistemas dentro del entorno de itinerancia. Las nuevas entradas se recuperan automáticamente del archivador cuando el usuario inicia la sesión en otro sistema (si el archivador está disponible) de la red de itinerancia. Por tanto, si un usuario ya ha iniciado la sesión en un

sistema, debe cerrar la sesión e iniciar la sesión de nuevo antes de que estén disponibles nuevas entradas en la red de itinerancia.

Retardo de renovación de certificado e itinerancia de Internet Explorer

Los certificados de Internet Explorer se renuevan en el archivador cada 20 segundos. Si un usuario de itinerancia genera un nuevo certificado de Internet Explorer, el usuario debe esperar al menos 20 segundos antes de importar, restaurar o cambiar su configuración de CSS en otro sistema. Si se intenta alguna de estas acciones antes del intervalo de renovación de 20 segundos, se perderá el certificado. Además, si el usuario no estaba conectado al archivador al generar el certificado, deberá esperar 20 segundos después de conectarse al archivador para asegurarse de que se actualiza el certificado en el archivador.

Contraseña de Lotus Notes e itinerancia de credenciales

Si está habilitado el soporte de Lotus Notes, UVM almacenará la contraseña de los usuarios de Lotus Notes. Los usuarios no necesitarán entrar su contraseña de Notes para iniciar la sesión de Lotus Notes. Se les pedirá su frase de paso, huellas dactilares, smart card, etc. de UVM (dependiendo de los valores de política de seguridad) para acceder a Lotus Notes.

Si un usuario cambia su contraseña de Notes desde Lotus Notes, el ID de archivo de Lotus Notes se actualiza con la nueva contraseña, y también se actualiza la copia de UVM de la nueva contraseña de Notes. En un entorno de itinerancia, las credenciales de usuario de UVM estarán disponibles en otros sistemas de la red de itinerancia a los que el usuario puede acceder. Es posible que la copia de UVM de la contraseña de Notes no coincida con la contraseña de Notes del archivo de ID de otros sistemas de la red de itinerancia si el archivo de ID de Notes con la contraseña actualizada no está tampoco disponible en el otro sistema. Si esto ocurre, el usuario no podrá acceder a Lotus Notes.

Si el archivo de ID de un usuario de Notes con la contraseña actualizada tampoco está disponible en otro sistema, el ID de archivo de Notes actualizado debe copiarse a los otros sistemas de la red de itinerancia de modo que la contraseña del archivo de ID coincida con la copia almacenada por UVM. De forma alternativa, los usuarios pueden ejecutar Modificar los valores de seguridad en el menú Inicio y cambiar la contraseña de Notes a su antiguo valor. A continuación se puede actualizar la contraseña de Notes mediante Lotus Notes.

Disponibilidad de credenciales en el inicio de sesión en un entorno de itinerancia

Cuando un archivador se encuentra en un recurso de red compartido, se descargan del archivador los últimos conjuntos de credenciales de usuario tan pronto como el usuario tiene acceso al archivador. Al iniciar la sesión, los usuarios aún no tienen acceso al recurso de red compartido, de modo que es posible que no se descarguen las últimas credenciales hasta que se complete el inicio de sesión. Por ejemplo, si se cambió la frase de paso de UVM en otro sistema de la red de itinerancia, o se registraron nuevas huellas dactilares en otro sistema, esas actualizaciones no estarán disponibles hasta que el proceso esté completo. Si no están disponibles las credenciales actualizadas, los usuarios deben probar la frase de paso anterior u otras huellas dactilares registradas para iniciar la sesión en el sistema. Una vez completado el inicio de sesión, las credenciales actualizadas del usuario estarán disponibles y la frase de paso y las huellas dactilares se registrarán con UVM.

Limitaciones de las tarjetas de identificación por contacto

Habilitación de la protección de inicio de sesión seguro de UVM con tarjetas de identificación por contacto de XyLoc

Para habilitar la protección de inicio de sesión seguro de UVM y utilizarla con el soporte de tarjeta de identificación por contacto de CSS, debe instalar los componentes en el orden siguiente:

1. Instale Client Security Software.
2. Habilite la protección de inicio de sesión seguro de UVM con CSS Administrator Utility.
3. Reinicie el sistema.
4. Instale el software de XyLoc para la tarjeta de identificación por contacto.

Nota: si se instala primero el software de la tarjeta de identificación por contacto de XyLoc, la interfaz de inicio de sesión de Client Security Software no se visualizará. Si ocurre esto, debe desinstalar Client Security Software y el software de XyLoc y reinstalarlos en el orden indicado más arriba para restaurar la protección de inicio de sesión seguro de UVM.

Soporte de tarjeta de identificación por contacto y Cisco LEAP

Habilitar la tarjeta de identificación por contacto y Cisco LEAP a la vez puede provocar resultados inesperados. Se recomienda no instalar ni utilizar estos componentes en el mismo sistema.

Soporte de software Ensure

Client Security Software 5.2 requiere que los usuarios de tarjetas de identificación por contacto actualicen el software Ensure a la versión 7.41. Al actualizar Client Security Software desde una versión anterior, actualice el software Ensure antes de actualizar a Client Security Software 5.2.

Restauración de las claves

Después de realizar una operación de restauración de claves, debe reiniciar el sistema para continuar utilizando Client Security Software.

Nombres de usuario local y de dominio

Si los nombres de usuario local y de dominio son iguales, debe utilizar la misma contraseña de Windows para ambas cuentas. IBM User Verification Manager sólo almacena una contraseña de Windows por ID, de modo que los usuarios deben utilizar la misma contraseña para el inicio de sesión local y de dominio. Si no es así, se les pedirá que actualicen la contraseña de Windows de IBM UVM al cambiar entre inicios de sesión local y de dominio si está habilitada la sustitución por el inicio de sesión seguro de IBM UVM.

CSS no proporciona la capacidad de inscribir usuarios locales y de dominio con el mismo nombre de cuenta. Si intenta inscribir usuarios locales y de dominio con el mismo ID, aparecerá el mensaje siguiente: The selected user ID has already been configured (El ID de usuario seleccionado ya está configurado). CSS no permite la inscripción separada de ID de usuario locales y de dominio comunes en un sistema, de forma que el usuario común tenga acceso al mismo conjunto de credenciales, como certificados, huellas dactilares almacenadas, etc.

Reinstalación del software de huellas dactilares Targus

Si se elimina y reinstala el software de huellas dactilares Targus, deben añadirse manualmente las entradas del registro necesarias para habilitar el soporte de huellas dactilares de Client Security Software o habilitar el soporte de huellas dactilares. Descargue el archivo de registro que contiene las entradas necesarias (atplugin.reg) y efectúe una doble pulsación sobre él para incluir las entradas en el registro. Pulse Sí cuando se le solicite confirmación de esta operación. Debe reiniciarse el sistema para que Client Security Software reconozca los cambios y habilitar el soporte de huellas dactilares.

Nota: debe tener privilegios de administrador en el sistema para añadir estas entradas de registro.

Frase de paso del supervisor del BIOS

IBM Client Security Software 5.2 y las versiones anteriores no dan soporte a la característica de frase de paso del supervisor del BIOS disponible en algunos sistemas ThinkPad. Si habilita el uso de la frase de paso del supervisor del BIOS, cualquier habilitación o inhabilitación del chip de seguridad debe realizarse desde el programa BIOS Setup.

Utilización de Netscape 7.x

Netscape 7.x tiene un funcionamiento distinto al de Netscape 4.x. El mensaje de solicitud de frase de paso no aparece al iniciar Netscape. En su lugar, el módulo PKCS#11 sólo se carga cuando es necesario, de modo que la frase de paso sólo aparece al efectuar una operación que requiera el módulo PKCS#11.

Utilización de un disquete para archivar

Si especifica un disquete como ubicación del archivador al configurar el software de seguridad, experimentará retardos prolongados, ya que el proceso de configuración escribe datos en el disquete. Algún otro medio, como un recurso de red compartido o una llave USB, podría ser una ubicación mejor para el archivador.

Limitaciones de las smart cards

Registro de smart cards

Las smart cards deben registrarse con UVM para que los usuarios puedan efectuar la autenticación satisfactoriamente con ellas. Si se asigna una tarjeta a varios usuarios, sólo el último usuario en registrar la tarjeta podrá utilizarla. En consecuencia, las smart cards sólo deben registrarse para una cuenta de usuario.

Autenticación de smart cards

Si es necesaria una smart card para la autenticación, UVM mostrará un diálogo solicitando la smart card. Al insertar la smart card en el lector, aparece un diálogo solicitando el PIN de la smart card. Si el usuario entra un PIN incorrecto, UVM solicitará de nuevo la smart card. Hay que retirar y reinsertar la smart card para volver a entrar el PIN. Los usuarios deben continuar retirando y reinsertando la smart card hasta que se entre el PIN correcto de la tarjeta.

El símbolo más (+) aparece en las carpetas después del cifrado

Después de cifrar archivos o carpetas, Windows Explorer podría mostrar un símbolo más (+) extraño ante el icono de carpeta. Este carácter extra desaparecerá cuando se actualice la ventana del Explorador.

Limitaciones de los usuarios limitados de Windows XP

Los usuarios limitados de Windows XP no pueden utilizar su frase de paso de UVM o contraseña de Windows ni actualizar su archivador de claves mediante User Configuration Utility.

Otras limitaciones

Este apartado contiene información sobre otras limitaciones o problemas conocidos en relación con Client Security Software.

Utilización de Client Security Software con sistemas operativos Windows

Todos los sistemas operativos Windows tienen la siguiente limitación conocida: si un usuario cliente que esté inscrito en UVM cambia su nombre de usuario de Windows, se pierde toda la funcionalidad de Client Security. El usuario tendrá que volver a inscribir el nombre de usuario nuevo en UVM y solicitar todas las credenciales nuevas.

Los sistemas operativos Windows XP tienen la siguiente limitación conocida: los usuarios inscritos en UVM cuyo nombre de usuario de Windows se haya cambiado previamente, no serán reconocidos por UVM. UVM señalará al nombre de usuario anterior mientras que Windows sólo reconocerá el nombre de usuario nuevo. Esta limitación se produce incluso si el nombre de usuario de Windows se cambió antes de instalar Client Security Software.

Utilización de Client Security Software con aplicaciones de Netscape

Netscape se abre después de una anomalía de autorización: si se abre la ventana de frase de paso de UVM, debe escribir la frase de paso de UVM y después pulsar **Aceptar** antes de poder continuar. Si escribe una frase de paso de UVM incorrecta (o proporciona una huella dactilar incorrecta para una exploración de huellas dactilares), se muestra un mensaje de error. Si pulsa **Aceptar**, Netscape se abrirá, pero el usuario no podrá utilizar el certificado digital generado por IBM Embedded Security Subsystem. Debe salir y volver a entrar en Netscape, y escribir la frase de paso correcta de UVM antes de poder utilizar el certificado de IBM Embedded Security Subsystem.

No se muestran los algoritmos: no todos los algoritmos hash soportados por el módulo PKCS#11 de IBM Embedded Security Subsystem se seleccionan si se ve el módulo en Netscape. Los algoritmos siguientes son soportados por el módulo PKCS#11 de IBM Embedded Security Subsystem, pero no son identificados como soportados cuando se ven en Netscape:

- SHA-1
- MD5

Certificado de IBM Embedded Security Subsystem y los algoritmos de cifrado

La información siguiente se proporciona para ayudar a identificar problemas en los algoritmos de cifrado que pueden utilizarse con el certificado de IBM Embedded Security Subsystem. Consulte a Microsoft o Netscape la información actual sobre los algoritmos de cifrado utilizados con sus aplicaciones de correo electrónico.

Cuando se envía correo electrónico desde un cliente Outlook Express (128 bits) a otro cliente Outlook Express (128 bits): si utiliza Outlook Express con la

versión de 128 bits de Internet Explorer 4.0 ó 5.0 para enviar correo electrónico cifrado a otros clientes que utilicen Outlook Express (128 bits), los mensajes de correo electrónico cifrados con el certificado de IBM Embedded Security Subsystem sólo pueden utilizar el algoritmo 3DES.

Cuando se envía correo electrónico entre un cliente Outlook Express (128 bits) y un cliente Netscape: una petición de cifrado RC2(40), RC2(64) o RC2(128) procedente de un cliente Netscape a un cliente Outlook Express (128 bits) siempre se devuelve al cliente Netscape con el algoritmo RC2(40).

Puede que algunos algoritmos no estén disponibles para seleccionarlos en el cliente Outlook Express (128 bits): en función de la forma en que fue configurada o actualizada la versión de Outlook Express (128 bits), puede que algunos algoritmos RC2 y otros algoritmos no estén disponibles para utilizarlos con el certificado de IBM Embedded Security Subsystem. Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con su versión de Outlook Express.

Utilización de la protección de UVM para un ID de usuario de Lotus Notes

La protección de UVM no funciona si cambia de ID de usuario dentro de una sesión de Notes: sólo puede configurar la protección de UVM para el ID de usuario actual de una sesión de Notes. Para cambiar de un ID de usuario que tenga habilitada la protección de UVM a otro ID de usuario, complete el procedimiento siguiente:

1. Salga de Notes.
2. Inhabilite la protección de UVM para el ID de usuario actual.
3. Entre en Notes y cambie el ID de usuario. Consulte la documentación de Lotus Notes para obtener información sobre el cambio de ID de usuario.

   Si desea configurar la protección de UVM para el ID de usuario al que ha cambiado, siga con el paso 4.
4. Entre en la herramienta Configuración de Lotus Notes proporcionada por Client Security Software y configure la protección de UVM.

Limitaciones de User Configuration Utility

Windows XP impone unas restricciones de acceso que limitan las funciones disponibles para un usuario cliente bajo determinadas circunstancias.

Windows XP Professional

En Windows XP Professional, pueden aplicarse restricciones al usuario cliente en las situaciones siguientes:

- Client Security Software está instalado en una partición que posteriormente se ha convertido a formato NTFS
- La carpeta de Windows está en una partición que posteriormente se ha convertido a formato NTFS
- La carpeta del archivador está en una partición que posteriormente se ha convertido a formato NTFS

En las situaciones anteriores, es posible que los usuarios limitados de Windows XP Professional no puedan efectuar las siguientes tareas de User Configuration Utility:

- Cambiar sus frases de paso de UVM
- Actualizar la contraseña de Windows registrada con UVM

- Actualizar el archivador de claves

Windows XP Home

Los usuarios limitados de Windows XP Home no podrán utilizar User Configuration Utility en ninguna de las situaciones siguientes:

- Client Security Software está instalado en una partición con formato NTFS
- La carpeta de Windows está en una partición con formato NTFS
- La carpeta del archivador está en una partición con formato NTFS

Limitaciones de Tivoli Access Manager

El recuadro de selección **Denegar todo acceso al objeto seleccionado** no se inhabilita cuando se selecciona el control de Tivoli Access Manager. En el editor de política de UVM, si selecciona **Tivoli Access Manager controla el objeto seleccionado** para hacer que Tivoli Access Manager controle un objeto de autenticación, no se inhabilita el recuadro de selección **Denegar todo acceso al objeto seleccionado**. Aunque el recuadro de selección **Denegar todo acceso al objeto seleccionado** permanezca activo, no puede seleccionarse para prevalecer sobre el control de Tivoli Access Manager.

Mensajes de error

Los mensajes de error relacionados con Client Security Software se generan en la anotación cronológica de sucesos: Client Security Software utiliza un controlador de dispositivo que puede generar mensajes de error en la anotación cronológica de sucesos. Los errores asociados con estos mensajes no afectan al funcionamiento normal del sistema.

UVM invoca los mensajes de error generados por el programa asociado si se deniega el acceso para un objeto de autenticación: si la política de UVM está establecida para denegar el acceso para un objeto de autenticación, por ejemplo descifrado de correos electrónicos, el mensaje que indica que se ha denegado el acceso variará en función del software que se esté utilizando. Por ejemplo, un mensaje de error de Outlook Express que indica que se ha denegado el acceso a un objeto de autenticación será diferente de un mensaje de error de Netscape indicando lo mismo.

Tablas de resolución de problemas

El apartado siguiente contiene tablas de resolución de problemas que podrían serle útiles si experimenta problemas con Client Security Software.

Información de resolución de problemas de instalación

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al instalar Client Security Software.

Síntoma del problema	**Posible solución**
Se muestra un mensaje de error durante la instalación del software	**Acción**
Cuando instala el software se muestra un mensaje que pregunta si desea eliminar la aplicación seleccionada y todos sus componentes.	Pulse **Aceptar** para salir de la ventana. Comience el proceso de instalación de nuevo para instalar la nueva versión de Client Security Software.

Síntoma del problema	Posible solución
Durante la instalación se muestra un mensaje indicando que debe actualizar o eliminar el programa.	Efectúe una de las acciones siguientes: • Si está instalada una versión anterior a Client Security Software 5.0, seleccione **Eliminar** y borre la información del subsistema de seguridad mediante el programa IBM BIOS Setup Utility. • En caso contrario, seleccione **Actualizar** y continúe con la instalación.
El acceso de instalación se ha denegado debido a una contraseña de administrador desconocida	**Acción**
Al instalar el software en un cliente de IBM con IBM Embedded Security Subsystem habilitado, la contraseña del administrador para IBM Embedded Security Subsystem es desconocida.	Borre la información del subsistema de seguridad para continuar con la instalación.

Información de resolución de problemas de Administrator Utility

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar Administrator Utility.

Síntoma del problema	Posible solución
El botón Siguiente no está disponible después de entrar y confirmar la frase de paso de UVM en Administrator Utility	**Acción**
Cuando se añaden usuarios a UVM, puede que el botón **Siguiente** no esté disponible después de entrar y confirmar la frase de paso de UVM en Administrator Utility.	Pulse el elemento **Información** en la barra de tareas de Windows y continúe el procedimiento.
Se muestra un mensaje de error al cambiar la clave pública del administrador	**Acción**
Cuando borra la información de IBM Embedded Security Subsystem y después restaura el archivador de claves, puede que aparezca un mensaje de error si cambia la clave pública del administrador.	Añada los usuarios a UVM y solicite nuevos certificados, si procede.
Se muestra un mensaje de error al intentar recuperar una frase de paso de UVM	**Acción**
Cuando cambia la clave pública del administrador y después intenta recuperar una frase de paso de UVM para un usuario, puede que aparezca un mensaje de error.	Efectúe una de las acciones siguientes: • Si no se necesita la frase de paso de UVM para el usuario, no se precisa ninguna acción. • Si se necesita la frase de paso de UVM para el usuario, debe añadir el usuario a UVM y solicitar nuevos certificados, si procede.
Se muestra un mensaje de error al intentar guardar el archivo de políticas de UVM	**Acción**

Síntoma del problema	Posible solución
Cuando intenta guardar un archivo de políticas de UVM (globalpolicy.gvm) pulsando **Aplicar** o **Guardar**, se muestra un mensaje de error.	Salga del mensaje de error, edite el archivo de políticas de UVM de nuevo para hacer los cambios que desee y después guarde el archivo.
Se muestra un mensaje de error al intentar abrir el editor de política de UVM	**Acción**
Si el usuario actual (que tiene iniciada una sesión en el sistema operativo) no se ha añadido a UVM, no se abrirá el editor de política de UVM.	Añada el usuario a UVM y abra el editor de política de UVM.
Se muestra un mensaje de error al utilizar Administrator Utility	**Acción**
Mientras utiliza Administrator Utility, puede mostrarse el mensaje de error siguiente: Se ha producido un error de E/S del almacenamiento intermedio al intentar acceder a IBM Embedded Security Subsystem. Esto podría resolverse mediante un rearranque.	Salga del mensaje de error y reinicie el sistema.
Se muestra un mensaje de inhabilitar chip cuando se cambia la contraseña del administrador	**Acción**
Cuando intenta cambiar la contraseña del administrador y pulsa Intro o Tab > Intro después de escribir la contraseña de confirmación, el botón **Inhabilitar chip** se habilita y aparece un mensaje de confirmación para inhabilitar el chip.	Haga lo siguiente: 1. Salga de la ventana de confirmación para inhabilitar el chip. 2. Para cambiar la contraseña del administrador, escriba la contraseña nueva, escriba la contraseña de confirmación y después pulse **Cambiar**. No pulse Intro ni Tab > Intro después de escribir la contraseña de confirmación.

Información de resolución de problemas de User Configuration Utility

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar User Configuration Utility.

Síntoma del problema	Posible solución
Los usuarios limitados no pueden realizar ciertas funciones de User Configuration Utility en Windows XP Professional	**Acción**
Es posible que los usuarios limitados de Windows XP Professional no puedan efectuar las siguientes tareas de User Configuration Utility: • Cambiar sus frases de paso de UVM • Actualizar la contraseña de Windows registrada con UVM • Actualizar el archivador de claves	Se trata de una limitación conocida con Windows XP Professional. No hay ninguna solución para este problema.
Los usuarios limitados no pueden utilizar User Configuration Utility en Windows XP Home	**Acción**

Síntoma del problema	Posible solución
Los usuarios limitados de Windows XP Home no podrán utilizar User Configuration Utility en ninguna de las situaciones siguientes: • Client Security Software está instalado en una partición con formato NTFS • La carpeta de Windows está en una partición con formato NTFS • La carpeta del archivador está en una partición con formato NTFS	Se trata de una limitación conocida con Windows XP Home. No hay ninguna solución para este problema.

Información de resolución de problemas específicos de ThinkPad

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar Client Security Software en sistemas ThinkPad.

Síntoma del problema	Posible solución
Se muestra un mensaje de error al intentar efectuar una función del administrador de Client Security	**Acción**
Aparece un mensaje de error después de intentar efectuar una función del administrador de Client Security.	La contraseña del supervisor del ThinkPad debe estar inhabilitada para efectuar ciertas funciones del administrador de Client Security. Para inhabilitar la contraseña del supervisor, complete el procedimiento siguiente: 1. Pulse F1 para acceder a IBM BIOS Setup Utility. 2. Entre la contraseña actual del supervisor. 3. Entre una contraseña del supervisor en blanco y confirme una contraseña en blanco. 4. Pulse Intro. 5. Pulse F10 para guardar y salir.
Un sensor de huellas dactilares preparado para UVM diferente no funciona correctamente	**Acción**
El sistema IBM ThinkPad no soporta el intercambio de varios sensores de huellas dactilares preparados para UVM.	No intercambie los modelos de sensor de huellas dactilares. Utilice el mismo modelo cuando trabaje de forma remota y cuando trabaje desde una estación de acoplamiento.

Información de resolución de problemas de Microsoft

Las tablas de resolución de problemas siguientes contienen información que podría serle útil si experimenta problemas al utilizar Client Security Software con aplicaciones o sistemas operativos de Microsoft.

Síntoma del problema	Posible solución
El protector de pantalla sólo se muestra en la pantalla local	**Acción**

Síntoma del problema	Posible solución
Cuando se utiliza la función de escritorio extendido de Windows, el protector de pantalla de Client Security Software sólo se mostrará en la pantalla local aunque el acceso al sistema y al teclado estará protegido.	Si se está mostrando alguna información confidencial, minimice las ventanas en el escritorio extendido antes de invocar el protector de pantalla de Client Security.
Client Security no funciona correctamente para un usuario inscrito en UVM	**Acción**
Es posible que el usuario cliente inscrito en UVM haya cambiado su nombre de usuario de Windows. Si ocurre eso, se perderá toda la funcionalidad de Client Security.	Vuelva a inscribir el nombre de usuario nuevo en UVM y solicite todas las credenciales nuevas.
Nota: en Windows XP, los usuarios inscritos en UVM cuyo nombre de usuario de Windows se haya cambiado previamente, no serán reconocidos por UVM. Esta limitación se produce incluso si el nombre de usuario de Windows se cambió antes de instalar Client Security Software.	
Problemas al leer correo electrónico cifrado utilizando Outlook Express	**Acción**
El correo electrónico cifrado no puede descifrarse debido a las diferencias en los niveles de cifrado de los navegadores Web utilizados por el remitente y el destinatario.	Compruebe lo siguiente: 1. El nivel de cifrado para el navegador Web que utiliza el remitente es compatible con el nivel de cifrado del navegador Web que utiliza el destinatario. 2. El nivel de cifrado para el navegador Web es compatible con el nivel de cifrado proporcionado por el firmware de Client Security Software.
Problemas al utilizar un certificado desde una dirección que tiene asociados varios certificados	**Acción**
Outlook Express puede listar varios certificados asociados con una sola dirección de correo electrónico y algunos de esos certificados pueden quedar invalidados. Un certificado queda invalidado si la clave privada asociada con el certificado ya no existe en IBM Embedded Security Subsystem del sistema del remitente donde se generó el certificado.	Pida al destinatario que reenvíe su certificado digital; después seleccione ese certificado en la libreta de direcciones de Outlook Express.
Mensaje de anomalía al intentar firmar digitalmente un mensaje de correo electrónico	**Acción**
Si el redactor de un mensaje de correo electrónico intenta firmarlo digitalmente cuando el redactor aún no tiene un certificado asociado con su cuenta de correo electrónico, se muestra un mensaje de error.	Utilice los valores de seguridad en Outlook Express para especificar que se asocie un certificado con la cuenta de usuario. Consulte la documentación proporcionada para Outlook Express para obtener más información.
Outlook Express (128 bits) sólo cifra mensajes de correo electrónico con el algoritmo 3DES	**Acción**

Síntoma del problema	Posible solución
Cuando se envía correo electrónico cifrado entre clientes que utilicen Outlook Express con la versión de 128 bits de Internet Explorer 4.0 ó 5.0, sólo puede utilizarse el algoritmo 3DES.	Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con Outlook Express.
Los clientes Outlook Express devuelven mensajes de correo electrónico con un algoritmo diferente	**Acción**
Un mensaje de correo electrónico cifrado con el algoritmo RC2(40), RC2(64) o RC2(128) es enviado desde un cliente que utiliza Netscape Messenger a un cliente que utiliza Outlook Express (128 bits). Un mensaje de correo electrónico devuelto desde el cliente Outlook Express se cifra con el algoritmo RC2(40).	No se precisa ninguna acción. Una petición de cifrado RC2(40), RC2(64) o RC2(128) procedente de un cliente Netscape a un cliente Outlook Express (128 bits) siempre se devuelve al cliente Netscape con el algoritmo RC2(40). Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con su versión de Outlook Express.
Se muestra un mensaje de error al utilizar un certificado en Outlook Express después de una anomalía de una unidad de disco duro	**Acción**
Se pueden restaurar los certificados utilizando la característica de restauración de claves en Administrator Utility. Es posible que algunos certificados, como los certificados gratuitos proporcionados por VeriSign, no puedan ser restaurados después de una restauración de claves.	Después de restaurar las claves, efectúe una de las acciones siguientes: • obtenga nuevos certificados • registre la autoridad de certificados de nuevo en Outlook Express
Outlook Express no actualiza el nivel de cifrado asociado con un certificado	**Acción**
Cuando un remitente selecciona el nivel de cifrado en Netscape y envía un mensaje de correo electrónico firmado a un cliente utilizando Outlook Express con Internet Explorer 4.0 (128 bits), puede que no coincida el nivel de cifrado del correo electrónico devuelto.	Suprima el certificado asociado desde la libreta de direcciones de Outlook Express. Abra de nuevo el correo electrónico firmado y añada el certificado a la libreta de direcciones de Outlook Express.
Se muestra un mensaje de error de descifrado en Outlook Express	**Acción**
Puede abrir un mensaje en Outlook Express efectuando una doble pulsación en él. En algunos casos, cuando efectúa una doble pulsación demasiado rápido en un mensaje cifrado, aparece un mensaje de error de descifrado.	Cierre el mensaje y abra de nuevo el mensaje de correo electrónico cifrado.
Además, es posible que aparezca un mensaje de error de descifrado en el panel de vista previa cuando selecciona un mensaje cifrado.	Si aparece un mensaje de error en el panel de vista previa, no se precisa ninguna acción.
Se muestra un mensaje de error al pulsar el botón Enviar dos veces en correos electrónicos cifrados	**Acción**

Síntoma del problema	Posible solución
Cuando utiliza Outlook Express, si pulsa el botón Enviar dos veces para enviar un mensaje de correo electrónico cifrado, se muestra un mensaje de error indicando que no se ha podido enviar el mensaje.	Cierre el mensaje de error y después pulse el botón **Enviar** una vez.
Se muestra un mensaje de error al solicitar un certificado	**Acción**
Cuando utiliza Internet Explorer, es posible que reciba un mensaje de error si solicita un certificado que utiliza el CSP de IBM Embedded Security Subsystem.	Solicite el certificado digital de nuevo.

Información de resolución de problemas de Netscape

Las tablas de resolución de problemas siguientes contienen información que podría serle útil si experimenta problemas al utilizar Client Security Software con aplicaciones de Netscape.

Síntoma del problema	Posible solución
Problemas al leer correo electrónico cifrado	**Acción**
El correo electrónico cifrado no puede descifrarse debido a las diferencias en los niveles de cifrado de los navegadores Web utilizados por el remitente y el destinatario.	Compruebe lo siguiente: 1. El nivel de cifrado para el navegador Web que utiliza el remitente es compatible con el nivel de cifrado del navegador Web que utiliza el destinatario. 2. El nivel de cifrado para el navegador Web es compatible con el nivel de cifrado proporcionado por el firmware de Client Security Software.
Mensaje de anomalía al intentar firmar digitalmente un mensaje de correo electrónico	**Acción**
Si no se ha seleccionado el certificado de IBM Embedded Security Subsystem en Netscape Messenger y el redactor de un mensaje de correo electrónico intenta firmar el mensaje con el certificado, se muestra un mensaje de error.	Utilice los valores de seguridad de Netscape Messenger para seleccionar el certificado. Cuando se abra Netscape Messenger, pulse el icono de seguridad en la barra de herramientas. Se abre la ventana Información sobre seguridad. Pulse **Messenger** en el panel izquierdo y después seleccione el **Certificado del chip IBM Security Chip incorporado**. Consulte la documentación proporcionada por Netscape para obtener más información.
Se devuelve un mensaje de correo electrónico al cliente con un algoritmo diferente	**Acción**

Síntoma del problema	Posible solución
Un mensaje de correo electrónico cifrado con el algoritmo RC2(40), RC2(64) o RC2(128) es enviado desde un cliente que utiliza Netscape Messenger a un cliente que utiliza Outlook Express (128 bits). Un mensaje de correo electrónico devuelto desde el cliente Outlook Express se cifra con el algoritmo RC2(40).	No se precisa ninguna acción. Una petición de cifrado RC2(40), RC2(64) o RC2(128) procedente de un cliente Netscape a un cliente Outlook Express (128 bits) siempre se devuelve al cliente Netscape con el algoritmo RC2(40). Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con su versión de Outlook Express.
No se puede utilizar un certificado digital generado por IBM Embedded Security Subsystem	**Acción**
El certificado digital generado por IBM Embedded Security Subsystem no está disponible para utilizarlo.	Compruebe que se ha escrito la frase de paso de UVM correcta cuando se abrió Netscape. Si escribe la frase de paso de UVM incorrecta, se muestra un mensaje de error indicando una anomalía de autenticación. Si pulsa **Aceptar**, se abre Netscape, pero no podrá utilizar el certificado generado por IBM Embedded Security Subsystem. Debe salir y volver a abrir Netscape y después escribir la frase de paso de UVM correcta.
Los certificados digitales nuevos del mismo remitente no se sustituyen dentro de Netscape	**Acción**
Cuando se recibe más de una vez un correo electrónico firmado digitalmente por el mismo remitente, el primer certificado digital asociado con el correo electrónico no se sobrescribe.	Si recibe varios certificados de correo electrónico, sólo un certificado es el certificado por omisión. Utilice las características de seguridad de Netscape para suprimir el primer certificado y después vuelva a abrir el segundo certificado o pida al remitente que envíe otro correo electrónico firmado.
No se puede exportar el certificado de IBM Embedded Security Subsystem	**Acción**
El certificado de IBM Embedded Security Subsystem no puede exportarse en Netscape. La característica de exportación de Netscape puede utilizarse para hacer copias de seguridad de los certificados.	Vaya a Administrator Utility o User Configuration Utility para actualizar el archivador de claves. Cuando actualiza el archivador de claves, se crean copias de todos los certificados asociados con IBM Embedded Security Subsystem.
Se muestra un mensaje de error al intentar utilizar un certificado restaurado después de una anomalía de una unidad de disco duro	**Acción**
Se pueden restaurar los certificados utilizando la característica de restauración de claves en Administrator Utility. Es posible que algunos certificados, como los certificados gratuitos proporcionados por VeriSign, no puedan ser restaurados después de una restauración de claves.	Después de restaurar las claves, obtenga un certificado nuevo.
Se abre el agente de Netscape y produce un error en Netscape	**Acción**

Síntoma del problema	Posible solución
Se abre el agente de Netscape y se cierra Netscape.	Desactive el agente de Netscape.
Netscape se retarda si intenta abrirlo	**Acción**
Si añade el módulo PKCS#11 de IBM Embedded Security Subsystem y después abre Netscape, puede producirse un pequeño retardo antes de que se abra Netscape.	No se precisa ninguna acción. Este mensaje es sólo informativo.

Información de resolución de problemas de certificados digitales

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al obtener un certificado digital.

Síntoma del problema	Posible solución
La ventana de frase de paso de UVM o la ventana de autenticación de huellas dactilares se muestran varias veces durante la petición de un certificado digital	**Acción**
La política de seguridad de UVM define que un usuario debe proporcionar la frase de paso de UVM o la autenticación de huellas dactilares antes de que se pueda obtener un certificado digital. Si el usuario intenta obtener un certificado, la ventana de autenticación que solicita la frase de paso de UVM o la exploración de huellas dactilares se muestra más de una vez.	Escriba la frase de paso de UVM o explore su huella dactilar cada vez que se abra la ventana de autenticación.
Se muestra un mensaje de error de VBScript o JavaScript	**Acción**
Cuando solicita un certificado digital, puede mostrarse un mensaje de error relacionado con VBScript o JavaScript.	Reinicie el sistema y obtenga el certificado de nuevo.

Información de resolución de problemas de Tivoli Access Manager

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar Tivoli Access Manager con Client Security Software.

Síntoma del problema	Posible solución
Los valores de política local no se corresponden con los del servidor	**Acción**
Tivoli Access Manager permite ciertas configuraciones de bits que no son soportadas por UVM. En consecuencia, los requisitos de política local pueden prevalecer sobre los valores definidos por un administrador al configurar el servidor Tivoli Access Manager.	Se trata de una limitación conocida.
No se puede acceder a los valores de configuración de Tivoli Access Manager	**Acción**

Síntoma del problema	Posible solución
No se puede acceder a la configuración de Tivoli Access Manager ni a los valores de configuración de la antememoria local en la página Configuración de política en Administrator Utility.	Instale Tivoli Access Manager Runtime Environment. Si no está instalado Runtime Environment en el cliente de IBM, no se podrá acceder a los valores de Tivoli Access Manager en la página Configuración de política.
El control de un usuario es válido tanto para el usuario como para el grupo	**Acción**
Al configurar el servidor Tivoli Access Manager, si define un usuario en un grupo, el control del usuario es válido tanto para el usuario como para el grupo si está activo **Traverse bit** (Bit cruzado).	No se precisa ninguna acción.

Información de resolución de problemas de Lotus Notes

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar Lotus Notes con Client Security Software.

Síntoma del problema	Posible solución
Después de habilitar la protección de UVM para Lotus Notes, Notes no puede completar su configuración	**Acción**
Lotus Notes no puede completar la configuración después de habilitar la protección de UVM utilizando Administrator Utility.	Se trata de una limitación conocida. Lotus Notes debe estar configurado y en ejecución antes de habilitar el soporte de Lotus Notes en Administrator Utility.
Se muestra un mensaje de error al intentar cambiar la contraseña de Notes	**Acción**
Si se cambia la contraseña de Notes cuando se utiliza Client Security Software se puede mostrar un mensaje de error.	Vuelva a intentar cambiar la contraseña. Si no funciona, reinicie el cliente.
Se muestra un mensaje de error después de generar aleatoriamente una contraseña	**Acción**
Se puede mostrar un mensaje de error cuando hace lo siguiente: • Utiliza la herramienta Configuración de Lotus Notes para establecer la protección de UVM para un ID de Notes • Abre Notes y utiliza la función proporcionada por Notes para cambiar la contraseña para el archivo de ID de Notes • Cierra Notes inmediatamente después de cambiar la contraseña	Pulse **Aceptar** para cerrar el mensaje de error. No se precisa ninguna otra acción. Contrariamente al mensaje de error, la contraseña se ha cambiado. La contraseña nueva es una contraseña generada aleatoriamente creada por Client Security Software. El archivo de ID de Notes está cifrado ahora con la contraseña generada aleatoriamente y el usuario no necesita un archivo de ID de usuario nuevo. Si el usuario final cambia la contraseña de nuevo, UVM generará una nueva contraseña aleatoria para el ID de Notes.

Información de resolución de problemas de cifrado

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al cifrar archivos utilizando Client Security Software 3.0 o posterior.

Síntoma del problema	Posible solución
Los archivos cifrados previamente no se descifrarán	**Acción**
Los archivos cifrados con versiones anteriores de Client Security Software no se descifran después de actualizar a Client Security Software 3.0 o posterior.	Se trata de una limitación conocida. Debe descifrar todos los archivos que fueron cifrados utilizando versiones anteriores de Client Security Software *antes* de instalar Client Security Software 3.0 o posterior. Client Security Software 3.0 no puede descifrar los archivos que fueron cifrados utilizando versiones anteriores de Client Security Software debido a cambios en su implementación de cifrado de archivos.

Información de resolución de problemas de dispositivos preparados para UVM

La información de resolución de problemas siguiente podría serle útil si experimenta problemas al utilizar dispositivos preparados para UVM.

Síntoma del problema	Posible solución
Un dispositivo preparado para UVM deja de funcionar correctamente	**Acción**
Un dispositivo de seguridad preparado para UVM, como una smart card, un lector de smart cards o un lector de huellas dactilares, no está funcionando correctamente.	Confirme que el dispositivo esté configurado correctamente en el sistema. Después de configurar un dispositivo, es posible que necesite rearrancar el sistema para iniciar el servicio correctamente. Para obtener información sobre resolución de problemas con dispositivos, consulte la documentación del dispositivo o póngase en contacto con el proveedor del dispositivo.
Un dispositivo preparado para UVM deja de funcionar correctamente	**Acción**
Cuando desconecta un dispositivo preparado para UVM de un puerto USB (Bus serie universal) y después vuelve a conectarlo al puerto USB, es posible que el dispositivo no funcione correctamente.	Reinicie el sistema después de haber vuelto a conectar el dispositivo al puerto USB.

Apéndice A. Normativas de exportación de los EE.UU. para Client Security Software

El paquete de IBM Client Security Software ha sido revisado por la oficina de control de exportación de IBM (IBM Export Regulation Office - ERO) y según precisa la normativa de exportación del Gobierno de los EE.UU., IBM ha remitido la documentación adecuada y ha obtenido la aprobación de clasificación minorista para el soporte de cifrado de hasta 256 bits por parte del U.S. Department of Commerce (Departamento de comercio de los EE.UU.) para la distribución internacional excepto en aquellos países con embargos por parte del Gobierno de los EE.UU. La normativa de los EE.UU. y de otros países está sujeta a cambio por el gobierno del país en cuestión.

Si no puede bajarse el paquete de Client Security Software, por favor, póngase en contacto con la oficina de ventas de IBM local o consulte al coordinador de control de exportación del país de IBM (IBM Country Export Regulation Coordinator - ERC).

Apéndice B. Información sobre contraseñas y frases de paso

Este apéndice contiene información sobre contraseñas y frases de paso.

Normas para contraseñas y frases de paso

Cuando se trabaja con un sistema seguro, hay muchas contraseñas y frases de paso diferentes. Las diferentes contraseñas tienen normas distintas. Este apartado contiene información sobre la contraseña del administrador y la frase de paso de UVM.

Normas para contraseñas del administrador

Las normas que regulan la contraseña del administrador no pueden ser modificadas por un administrador de seguridad.

Las normas siguientes se aplican a la contraseña del administrador:

Longitud
La contraseña debe tener exactamente una longitud de ocho caracteres.

Caracteres
La contraseña sólo debe contener caracteres alfanuméricos. Se admite una combinación de letras y números. No se admiten caracteres especiales, como espacio, !, ?, %.

Propiedades
Establezca la contraseña del administrador para habilitar el chip IBM Security Chip incorporado en el sistema. Esta contraseña debe escribirse cada vez que se accede a Administrator Utility y a la Consola del administrador.

Intentos incorrectos
Si escribe la contraseña incorrectamente diez veces, el sistema se bloquea durante 1 hora y 17 minutos. Si después de que haya pasado este período de tiempo, escribe la contraseña incorrectamente diez veces más, el sistema se bloquea durante 2 horas y 34 minutos. El tiempo que está inhabilitado el sistema se duplica cada vez que se escribe la contraseña incorrectamente diez veces.

Normas para frases de paso de UVM

IBM Client Security Software permite a los administradores de seguridad establecer las normas que regulan la frase de paso de UVM de un usuario. Para mejorar la seguridad, la frase de paso de UVM es más larga y puede ser más exclusiva que una contraseña tradicional. La política de frases de paso de UVM es controlada por Administrator Utility.

La interfaz Política de frases de paso de UVM de Administrator Utility permite a los administradores de seguridad controlar los criterios de las frases de paso mediante una sencilla interfaz. La interfaz Política de frases de paso de UVM permite a los administradores establecer las normas para frases de paso siguientes:

Nota: el valor por omisión para cada criterio de las frases de paso aparece indicado abajo entre paréntesis.

- Establecer un número mínimo de caracteres alfanuméricos permitidos (sí, 6)

Por ejemplo, si se establece que son ″6″ los caracteres permitidos, 1234567xxx es una contraseña no válida.

- Establecer un número mínimo de caracteres numéricos permitidos (sí, 1)

  Por ejemplo, si se establece en ″1″, estaesmicontraseña es una contraseña no válida.
- Establecer el número mínimo de espacios permitidos (mínimo no definido)

  Por ejemplo, si se establece en ″2″, yo no estoy aquí es una contraseña no válida.
- Establecer si se permite que la frase de paso comience con un dígito (no)

  Por ejemplo, por omisión, 1contraseña es una contraseña no válida.
- Establecer si se permite que la frase de paso termine con un dígito (no)

  Por ejemplo, por omisión, contraseña8 es una contraseña no válida.
- Establecer si se permite que la frase de paso contenga un ID de usuario (no)

  Por ejemplo, por omisión, NombreUsuario es una contraseña no válida, donde NombreUsuario es un ID de usuario.
- Establecer si se comprueba que la nueva frase de paso sea diferente de las últimas x frases de paso, donde x es un campo editable (sí, 3)

  Por ejemplo, por omisión, micontraseña es una contraseña no válida si cualquiera de sus últimas tres contraseñas era micontraseña.
- Establecer si la frase de paso puede contener más de tres caracteres consecutivos idénticos a los de la contraseña anterior en cualquier posición (no)

  Por ejemplo, por omisión, contra es una contraseña no válida si su contraseña anterior era cont o tras.

La interfaz Política de frases de paso de UVM de Administrator Utility también permite a los administradores de seguridad controlar la caducidad de las frases de paso. La interfaz Política de frases de paso de UVM permite al administrador elegir entre las siguientes normas para la caducidad de las frases de paso:

- Establecer si desea hacer que la frase de paso caduque después de un número de días establecido (sí, 184)

  Por ejemplo, por omisión la frase de paso caducará en 184 días. La nueva frase de paso debe cumplir la política establecida para frases de paso.
- Establecer si la frase de paso caduca (sí)

  Cuando se selecciona esta opción, la frase de paso no caduca.

La política de frases de paso se comprueba en Administrator Utility cuando el usuario se inscribe y también se comprueba cuando el usuario cambia la frase de paso en User Configuration Utility. Los dos valores del usuario relacionados con la contraseña anterior se restablecerán y se eliminará el historial de frases de paso.

Las normas generales siguientes se aplican a la frase de paso de UVM:

Longitud
La frase de paso puede tener una longitud de hasta 256 caracteres.

Caracteres
La frase de paso puede contener cualquier combinación de caracteres que genere el teclado, incluidos espacios y caracteres alfanuméricos.

Propiedades
La frase de paso de UVM es diferente de una contraseña que pueda utilizarse para iniciar una sesión en un sistema operativo. La frase de paso

de UVM puede utilizarse junto con otros dispositivos de autenticación, como un sensor de huellas dactilares preparado para UVM.

Intentos incorrectos

Si escribe incorrectamente la frase de paso de UVM varias veces durante una sesión, el sistema aplicará una serie de retardos para evitar que se fuerce el sistema. Estos retardos se especifican en el apartado siguiente.

Número de intentos erróneos en sistemas TCPA y no TCPA

La tabla siguiente muestra los valores de retardos para evitar que se fuerce el sistema para un sistema TCPA:

Intentos	Retardo en el siguiente intento erróneo
15	1,1 minutos
31	2,2 minutos
47	4,4 minutos
63	8,8 minutos
79	17,6 minutos
95	35,2 minutos
111	1,2 horas
127	2,3 horas
143	4,7 horas

Los sistemas TCPA no distinguen entre frases de paso de usuarios y contraseña del administrador. Cualquier autenticación que se efectúe mediante el chip IBM Security Chip incorporado observa la misma política. El tiempo de espera máximo es de 4,7 horas. Los sistemas TCPA no aplicarán un retardo superior a 4,7 horas.

Los sistemas TCPA distinguen entre la contraseña del administrador y las frases de paso de usuarios. En los sistemas no TCPA, la contraseña del administrador tiene un retardo de 77 minutos después de 10 intentos erróneos; las contraseñas de usuarios sólo tienen un retardo de un minuto después de 32 intentos erróneos y después el tiempo de bloqueo se duplica cada 32 intentos erróneos.

Restablecimiento de una frase de paso

Si un usuario olvida su frase de paso, el administrador puede permitirle que restablezca su frase de paso.

Restablecimiento de una frase de paso de forma remota

Para restablecer una contraseña de forma remota, complete el procedimiento siguiente:

- **Administradores**

  Un administrador remoto debe hacer lo siguiente:

  1. Cree una contraseña de un solo uso y comuníquesela al usuario.
  2. Envíe un archivo de datos al usuario.

     El archivo de datos puede enviarse al usuario por correo electrónico, puede copiarse en un soporte de almacenamiento extraíble, como un disquete, o puede escribirse directamente en el archivador del usuario (siempre que el

usuario pueda acceder a este sistema). Este archivo cifrado se utiliza para confrontarlo con la nueva contraseña de un solo uso.

- **Usuarios**

  El usuario debe hacer lo siguiente:

  1. Iniciar una sesión en el sistema.
  2. Cuando se le solicite una frase de paso, seleccione el recuadro de selección ″He olvidado mi frase de paso″.
  3. Entre la contraseña de un solo uso que le ha comunicado el administrador remoto e indique la ubicación del archivo que le envío el administrador.

     Después de que UVM compruebe que la información del archivo se corresponde con la contraseña indicada, se otorga acceso al usuario. Inmediatamente después se solicita al usuario que cambie la frase de paso.

Esta es la forma recomendada para restablecer una frase de paso perdida.

Restablecimiento de una frase de paso de forma manual

Si el administrador puede ir físicamente al sistema del usuario que olvidó su frase de paso, podrá iniciar una sesión en el sistema del usuario como administrador, proporcionar la clave privada del administrador a Administrator Utility y cambiar manualmente la frase de paso del usuario. El administrador no tiene que conocer la frase de paso anterior del usuario para cambiar la frase de paso.

Apéndice C. Avisos y marcas registradas

Este apéndice ofrece avisos legales para los productos de IBM así como información de marcas registradas.

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en los Estados Unidos.

IBM quizá no ofrezca los productos, servicios o dispositivos mencionados en este documento, en otros países. Consulte al representante local de IBM para obtener información sobre los productos y servicios que actualmente pueden adquirirse en su zona geográfica. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni implicar que sólo pueda utilizarse este producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes en tramitación que hacen referencia a temas tratados en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede realizar consultas sobre licencias escribiendo a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN ″TAL CUAL″ SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no autorizan la exclusión de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que este aviso no sea aplicable en su caso.

La presente publicación puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación cuando lo considere oportuno y sin previo aviso.

Los usuarios con licencia de este programa que deseen obtener información sobre el mismo para poder: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar de forma mutua la información intercambiada, deben ponerse en contacto con IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, EE.UU. La disponibilidad de esta información, de acuerdo con los términos y condiciones correspondientes, podría incluir en algunos casos el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo es proporcionado por IBM bajo los términos que se especifican en IBM Customer Agreement, International Programming License Agreement o en cualquier otro acuerdo equivalente acordado entre las partes.

Marcas registradas

IBM y SecureWay son marcas registradas de IBM Corporation en los Estados Unidos y/o en otros países.

Tivoli es una marca registrada de Tivoli Systems Inc. en los Estados Unidos y/o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de otras empresas.