Soluciones IBM® Client Security

Guía de instalación de Client Security Software Versión 5.4

Soluciones IBM® Client Security

Guía de instalación de Client Security Software Versión 5.4

Primera edición (octubre 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 35 y el Apéndice C, "**Avisos y marcas registradas**", en la página 43.

Esta publicación es la traducción del original inglés *IBM Client Security Solutions: Client Security Software Version 5.4 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, “Cómo bajar, instalar y configurar el 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 la *Guía del administrador y 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 y del usuario de Client Security Software*

En este documento se hacen referencias a la *Guía del administrador y del usuario de Client Security Software*. La *Guía del administrador y del usuario* 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 y del usuario* para configurar y mantener la política de seguridad para cada cliente.

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

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 TCG (Trusted Computing Group) definidas en la especificación principal de TCG versión 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. 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 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.
- **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 versión 5.1**

  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 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 4.8 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)
- Soporte de Lotus Notes mediante la protección de autenticación de inicio de sesión mejorada

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.

Los usuarios 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 del BIOS 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 Intro o F1 durante la secuencia de arranque del sistema. Esta contraseña se denomina *contraseña del administrador* en el programa Configuration/Setup Utility de ThinkCentre y *contraseña del supervisor* en el programa BIOS Setup Utility de ThinkPad.

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 soporte externo 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. Cómo bajar, instalar y configurar el 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 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. En el recuadro Resources (Recursos), pulse **Support and downloads** (Soporte y descargas).
3. En la sección Embedded Security Subsystem e IBM Client Security Software de la página Web, pulse **Software download** (Bajar software).
4. En el recuadro Select a system (Seleccione un sistema), 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. Entre su dirección de correo electrónico en el campo suministrado y seleccione su país/región en el menú desplegable.
6. Seleccione el recuadro de selección adecuado sobre si desea que se le envíe información sobre otras ofertas.
7. Revise el Acuerdo de licencia pulsando **View Licence** (Ver licencia); a continuación pulse **Accept Licence** (Aceptar licencia).

   Se le redirigirá automáticamente a la página para bajarse IBM Client Security.
8. Busque el enlace de Client Security Software 5.4 y pulse **Download Now** (Bajar ahora).

   Nota: Consulte el archivo `css54readme.html` para información específica sobre actualizaciones y limitaciones.
9. Pulse **Guardar** para guardar una copia del archivo ejecutable de instalación en el disco duro.

10. Especifique la ubicación de Guardar como y pulse **Guardar**. Para iniciar la instalación del software, pulse **Abrir** cuando se complete la descarga o efectúe una doble pulsación sobre el icono del archivo ejecutable.

    Se abre la ventana Bienvenido al Asistente de InstallShield para IBM Client Security Software.

Instalación del software

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

1. Efectúe una doble pulsación sobre el archivo ejecutable.

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

   Se muestra el Acuerdo de licencia de IBM Client Security Software.
3. Lea los términos del acuerdo de licencia, seleccione el botón de selección **Acepto los términos del acuerdo de licencia** y pulse **Siguiente**.

   Se muestra la pantalla Selección de producto.
4. Seleccione uno de los botones de selección siguientes y pulse **Siguiente**.
   - **IBM Client Security Software e IBM Password Manager.** Esta selección instalará o actualizará IBM Client Security Software, IBM Password Manager y todos los controladores de dispositivo necesarios.
   - **Sólo IBM Client Security Software.** Esta selección instalará o actualizará IBM Client Security Software y todos los controladores de dispositivo necesarios.

   Se muestra la pantalla Carpeta de destino.
5. Pulse **Siguiente** para aceptar la ubicación de instalación por omisión o pulse **Cambiar** para examinar la carpeta de destino deseada.

   Se muestra la pantalla Preparado para instalar el programa.
6. Pulse **Instalar** para iniciar la instalación o pulse **Atrás** para revisar o cambiar cualquiera de los valores de instalación.

   Una barra de estado muestra el progreso de la instalación y después se muestra la pantalla de finalización del asistente de InstallShield.
7. Pulse **Finalizar** para salir del asistente.

Debe reiniciar el sistema para que los cambios de la instalación realizados en el sistema entren en vigor.

Selección de una opción de configuración

La primera pantalla del Asistente de instalación de IBM Client Security le permite seleccionar una opción de configuración. Seleccionar la opción de configuración adecuada es muy importante. Revise cuidadosamente la información siguiente antes de selecciona una opción de configuración. Los usuarios de seguridad noveles deberían seleccionar la opción de *configuración típica*.

Configuración típica

Cuando se selecciona la configuración típica de IBM Client Security Software mediante el Asistente de instalación de Client Security, se configuran las siguientes características de Client Security:

- IBM Password Manager (si se ha seleccionado en la instalación)

- Cifrado de archivos con el botón derecho
- Autenticación de frase de paso y huella dactilar
- Soporte de firma digital

Si se utilizan las opciones recomendadas de la *configuración típica* en el Asistente de instalación de Client Security el proceso de configuración es sencillo. Sin embargo, algunas de las características avanzadas de Client Security Software están inhabilitadas cuando se selecciona esta configuración, quedando por tanto no disponibles.

Valores por omisión de la configuración típica

Los valores por omisión protegidos de la configuración típica son los siguientes:

- **Ubicación del archivador:** C:\documents and settings\all users\application data\ibm\security\archive
- **Ubicación del par de claves del administrador:** C:\documents and settings\all users\application data\ibm\security\keys

  La clave privada del administrador no se divide, y se cifra con la frase de paso del administrador de CSS.

Otros valores incluyen lo siguiente:

- El soporte de IBM Password Manager está habilitado
- La política de seguridad es media: cada método de autenticación disponible sólo será necesario la primera vez que se utilice una característica de CSS.
- La autenticación de la frase de paso siempre es necesaria.
- La autenticación de huellas dactilares es necesaria cuando se detecta un lector de huellas integrado en la instalación.
- La frase de paso del usuario que configure CSS es también la *contraseña del administrador*. Si se cambia la frase de paso de UVM, cambiará también la contraseña del administrador de CSS. La frase de paso del administrador de CSS nunca caduca.

Limitaciones de componentes de la configuración típica

Algunas características de Client Security Software que se habilitan después de una configuración avanzada se inhabilitan al seleccionar una configuración típica. Estas características no se pueden utilizar en la configuración típica de CSS. Para habilitar estas funciones, debe convertir la configuración a avanzada. Las diferencias funcionales después de una configuración típica son las siguientes:

- **Administrator Utility**

  Las acciones siguientes no se permiten en una configuración típica:

  – Restablecer usuario
  – Eliminar usuario
  – Cambiar la contraseña del administrador utilizando el botón Valores del chip
  – Configuración de claves

  Si un usuario intenta realizar una de las operaciones anteriores, se le pedirá que convierta CSS a la configuración avanzada. El proceso de conversión descifra el par de claves del administrador y en una ubicación especificada por el usuario.
- **Administrator Console**

  Las siguientes diferencias de utilización se aplican bajo una configuración típica:

  – El directorio del archivador, la ubicación de la clave privada y la ubicación de la clave pública están protegidos y no se pueden cambiar. El archivador sólo puede editarse en el sistema local.

- La opción para configurar la itinerancia de credenciales no está disponible en la configuración típica. Si selecciona una configuración típica y desea configurar la red de itinerancia de credenciales, debe convertir primero la configuración típica en una configuración avanzada.
- No se puede realizar una operación de cancelación de la frase de paso de UVM para el administrador de CSS.

- **User Configuration Utility**

  Las siguientes diferencias de utilización se aplican bajo una configuración típica:
  - La frase de paso del usuario que configure CSS es también la contraseña del administrador. Si se cambia la frase de paso de UVM, cambiará también la contraseña del administrador.
  - No se puede restablecer el administrador de CSS.
  - La opción para configurar la itinerancia de credenciales no está disponible en la configuración típica.

Conversión de una configuración típica en avanzada

Para convertir una configuración típica de Client Security Software en una configuración avanzada, siga este procedimiento:

1. Inicie Administrator Utility.
2. Entre la contraseña del administrador de CSS.
3. Pulse el botón **Configuración de claves**.
4. Pulse **Aceptar** para continuar.
5. Entre la ubicación donde desea almacenar el par de claves descifradas del administrador. El par de claves descifradas no debe almacenarse en la unidad de disco duro local. Se ha completado el proceso de conversión.
6. Cambie la ubicación del archivador. El archivador no debe almacenarse en la unidad de disco duro local.

Una vez convertido Client Security Software a una configuración avanzada, no se puede volver a una configuración típica.

Configuración avanzada

La *configuración avanzada* de IBM Client Security Software configura las siguientes características *adicionales* de Client Security:

- **Protección de inicio de sesión de UVM**
- **Selección de la ubicación de almacenamiento de claves**
- **Soporte de aplicaciones:** Entrust, Cifrado de archivos y carpetas, Lotus Notes

Utilización del Asistente de instalación de IBM Client Security

El Asistente de instalación de IBM Client Security proporciona una interfaz que ayuda a instalar Client Security Software y a habilitar el chip IBM Security Chip incorporado. Complete el procedimiento siguiente para permitir que el Asistente de instalación de IBM Client Security le guíe a través de las tareas necesarias relacionadas con la configuración de una política de seguridad en un cliente de IBM.

Estos son los pasos generales del Asistente de instalación de IBM Client Security. Los pasos específicos varían dependiendo de la opción de configuración seleccionada.

- **Establecer 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.

- **Crear 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.

- **Proteger 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.

- **Autorizar 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.

- **Seleccionar 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.

Utilización del Asistente de instalación para completar una configuración típica

Para utilizar el Asistente de instalación de IBM Client Security con el fin de completar una configuración típica, lleve a cabo el procedimiento siguiente:

1. Pulse **Inicio > Programas > Access IBM > IBM Client Security Software > Asistente de instalación de IBM Client Security**.

   La pantalla de bienvenida del Asistente de instalación de IBM Client Security le permite seleccionar una opción de configuración.

2. Seleccione el botón de selección Configuración típica (recomendada) y pulse **Siguiente**.

   Esta selección habilita IBM Password Manager y sólo requiere que se especifiquen muy pocos parámetros. Cuando se selecciona la configuración típica, CSS almacena la información de copia de seguridad y las claves de seguridad en la unidad de disco duro. Los usuarios de seguridad noveles deben utilizar la opción de configuración típica. Se trata del valor por omisión.

   Se muestra la pantalla Entrada de frase de paso.

3. Complete las tareas siguientes:

   a. Entre una frase de paso en el campo Entre la frase de paso. Si es necesario, pulse el botón **Ver requisitos de frase de paso** para ayudar a establecer una frase de paso válida.

      Nota: durante la instalación inicial o después de haber borrado la información del chip IBM Security Chip incorporado, se le solicitará

que confirme la frase de paso en el campo Confirmar frase de paso. También es posible que se le solicite que proporcione la contraseña del supervisor, si es aplicable.

b. Escriba una palabra o frase en el campo de la pista de la frase de paso.

c. Pulse **Siguiente**.

Si se detecta un lector de huellas dactilares en el sistema, se muestra la pantalla Almacenamiento de huellas dactilares. El recuadro de selección **Sí, deseo almacenar huellas dactilares ahora** aparece seleccionado por omisión.

4. Efectúe una de las acciones siguientes:
   - Quite la selección del recuadro de selección **Sí, deseo almacenar huellas dactilares ahora** y después pulse **Siguiente**.
   - Pulse **Siguiente** y siga las instrucciones que aparecen en pantalla para empezar a registrar las huellas dactilares ahora.

   Se muestra la pantalla Autorizar usuarios adicionales.
5. Efectúe una de las acciones siguientes:
   - Seleccione el recuadro de selección **Seleccionar usuarios adicionales para autorizarlos ahora (opcional)** y después pulse **Siguiente**.
   - Pulse **Omitir** para omitir esta tarea.

   Se muestra la pantalla Resumen de los valores y características de seguridad.
6. Pulse **Finalizar** para implementar los valores de seguridad que ha seleccionado. Este proceso podría llevarle unos minutos. Se muestra un mensaje indicando que el sistema está protegido ahora por IBM Client Security.
7. Pulse **Aceptar**.

Utilización del Asistente de instalación para completar una configuración avanzada

Para utilizar el Asistente de instalación de IBM Client Security con el fin de completar una configuración avanzada, lleve a cabo el procedimiento siguiente:

1. Pulse **Inicio > Programas > Access IBM > IBM Client Security Software > Asistente de instalación de IBM Client Security**.

   La pantalla de bienvenida del Asistente de instalación de IBM Client Security le permite seleccionar una opción de configuración.
2. Seleccione el botón de selección **Configuración avanzada** y pulse **Siguiente**.

   Esta selección requiere que se especifique información de configuración como la ubicación del almacenamiento de claves y el nivel de seguridad, y le permite habilitar la protección de inicio de sesión de CSS, la protección de Lotus Notes e IBM Password Manager.

   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 nuevas claves**.
  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 del archivador 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 la ubicación del archivador de claves donde 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.

   - **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 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.

   Se muestra la pantalla Se ha completado la instalación - Revise los valores de seguridad.
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**.

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**.

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

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 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 la última versión de Client Security Software y configúrelo utilizando el Asistente de instalación de IBM Client Security.

Actualización desde CSS 5.0 o posterior utilizando los datos de seguridad existentes

Si desea actualizar desde Client Security Software Versión 5.0 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. Actualice 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.

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 35.

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 instala o configura Client Security Software.

Funciones del administrador

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.

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 de dirección 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.

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 Security Feature** (Función de seguridad IBM TCPA) y pulse Intro.
5. Seleccione **Yes** (Sí).
6. Pulse Intro para confirmar la elección.
7. Pulse F10 para guardar los cambios y salir del programa Setup Utility.
8. Seleccione **Yes** (Sí) y 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 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 Security Chip** y pulse Intro.
5. Pulse Intro y seleccione **Disabled** (Inhabilitado).
6. Pulse Intro para confirmar la elección.
7. Pulse Intro para continuar.
8. Pulse F10 para guardar los cambios y salir del programa Setup Utility.
9. Seleccione **Yes** (Sí) y pulse Intro. Se reiniciará el sistema.

Limitaciones o problemas conocidos de CSS Versión 5.4

La información siguiente puede ser de ayuda cuando instale o configure Client Security Software Versión 5.4.

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 5.4 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.

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.

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.
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 elimínela. Después, reinicie el sistema 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.
Se muestra un mensaje de error al intentar realizar determinadas funciones 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 de ThinkPad o la contraseña del administrador del BIOS de ThinkCentre debe inhabilitarse para generar el par de claves de hardware en un sistema Crypto 1 (no TCG). El proceso de instalación de CSS no puede habilitar IBM Embedded Security Subsystem mientras no se inhabilite la contraseña adecuada.

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

La interfaz de Administrator Utility permite a los administradores de seguridad controlar los criterios de las contraseñas mediante una sencilla interfaz. Esta interfaz permite a los administradores establecer las normas de contraseñas del administrador siguientes:

Nota: el valor por omisión para cada criterio de las frases de paso aparece indicado abajo entre paréntesis. La contraseña del administrador nunca caduca.

- 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.

Las normas generales siguientes se aplican a la contraseña del administrador:

Longitud
La contraseña puede tener una longitud de hasta 256 caracteres.

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

Propiedades
La contraseña del administrador es diferente de una contraseña que pueda utilizarse para iniciar una sesión en un sistema operativo. La contraseña del administrador puede utilizarse junto con otros dispositivos de autenticación, como un sensor de huellas dactilares preparado para UVM.

Intentos incorrectos

Si escribe incorrectamente la contraseña del administrador varias veces durante una sesión, el sistema aplicará una serie de retardos para evitar que se fuerce el sistema.

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 que utilizan National TPM

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

Intentos	Retardo en el siguiente intento erróneo
7-13	4 segundos cada uno
14-20	8 segundos cada uno
21-27	16 segundos cada uno
28-34	32 segundos cada uno
35-41	64 segundos cada uno (1,07 minutos cada uno)
42-48	128 segundos cada uno (2,13 minutos cada uno)
49-55	256 segundos cada uno (4,27 minutos cada uno)
56-62	512 segundos cada uno (8,53 minutos cada uno)
63-69	1.024 segundos cada uno (17,07 minutos cada uno)
70-76	2.048 segundos cada uno (34,13 minutos cada uno)
77-83	68,26 minutos cada uno (1,14 horas cada uno)
84-90	136,52 minutos cada uno (2,28 horas cada uno)
91-97	273,04 minutos cada uno (4,55 horas cada uno)
98-104	546,08 minutos cada uno (9,1 horas cada uno)
105-111	1.092,16 minutos cada uno (18,2 horas cada uno)
112-118	2.184,32 minutos cada uno (36,4 horas cada uno)

Los sistemas National TPM 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. No existe un tiempo de espera máximo. Cada intento erróneo activa el retardo indicado anteriormente. Los retardos para evitar que se fuerce el sistema no terminan en el intento número 118; en su lugar, continúan indefinidamente de la forma ilustrada anteriormente.

Número de intentos erróneos en sistemas que utilizan Atmel TPM

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

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 Atmel TPM 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 Atmel no aplicarán un retardo superior a 4,7 horas.

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.