Soluciones IBM Client Security

Guía de instalación de Client Security Software Versión 5.1

Soluciones IBM Client Security

Guía de instalación de Client Security Software Versión 5.1

Primera edición (abril de 2003)

Esta publicación es la traducción del original inglés *Client Security Software Version 5.1 Installation Guide*.

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 45 y el Apéndice C, “**Avisos y marcas registradas**”, en la página 49.

© Copyright International Business Machines Corporation 2002. Reservados todos los derechos.

Contenido

Prefacio v
Acerca de esta guía v
A quién va dirigida esta guía v
Utilización de esta guía vi
Referencias a la *Guía del administrador de Client Security Software* vi
Referencias a la *Guía del usuario de Client Security Software* vi
Información adicional vi

Capítulo 1. Introducción a IBM Client Security Software 1
Aplicaciones y componentes de Client Security Software 1
Características PKI (Public Key Infrastructure) 2

Capítulo 2. Cómo empezar 5
Requisitos de hardware 5
El chip IBM Security Chip 5
Modelos de IBM soportados 5
Requisitos de software 5
Sistemas operativos 5
Productos preparados para UVM. 5
Navegadores Web 6
Cómo bajar el software 7

Capítulo 3. Antes de instalar el software 9
Antes de instalar el software 9
Instalación en clientes que ejecutan Windows XP y Windows 2000 9
Instalación para utilizarlo con Tivoli Access Manager 9
Consideraciones sobre las características de arranque 9
Información sobre actualizaciones del BIOS 10
Utilización del par de claves del archivador 10

Capítulo 4. Instalación, actualización y desinstalación del software 13
Cómo bajar e instalar el software 13
Utilización de asistente de instalación de IBM Client Security Software 14
Habilitación del chip IBM Security Chip 17
Instalación del software en otros clientes de IBM cuando está disponible la clave pública del administrador - sólo instalaciones desatendidas 18
Instalación desatendida. 18
Despliegue masivo 18
Instalación masiva 19
Configuración masiva 19
Actualización de la versión de Client Security Software 21
Actualización utilizando nuevos datos de seguridad 21
Actualización a Client Security Versión 5.1 utilizando los datos de seguridad existentes 21
Actualización desde el Release 5.1 a versiones posteriores utilizando datos de seguridad existentes 23
Desinstalación de Client Security Software. 24

Capítulo 5. Resolución de problemas 25
Funciones del administrador 25
Establecimiento de una contraseña del administrador (ThinkCentre) 25
Establecimiento de una contraseña del supervisor (ThinkPad) 26
Protección de la contraseña de hardware 27

© Copyright IBM Corp. 2002

Borrado de la información del chip IBM Security Chip incorporado (ThinkCentre) . . . 27
Borrado de la información del chip IBM Security Chip incorporado (ThinkPad) 27
Administrator Utility . . . 28
Supresión de usuarios . . . 28
Acceso denegado a objetos seleccionados con el control de Tivoli Access Manager . . . 28
Limitaciones conocidas . . . 29
Utilización de Client Security Software con sistemas operativos Windows 29
Utilización de Client Security Software con aplicaciones de Netscape . . . 29
El certificado del chip IBM Security Chip incorporado y los algoritmos de cifrado . . . 29
Utilización de la protección de UVM para un ID de usuario de Lotus Notes 30
Limitaciones de User Configuration Utility . . . 30
Mensajes de error . . . 31
Tablas de resolución de problemas . . . 31
Información de resolución de problemas de instalación . . . 31
Información de resolución de problemas de Administrator Utility . . . 32
Información de resolución de problemas de User Configuration Utility . . . 34
Información de resolución de problemas específicos de ThinkPad . . . 34
Información de resolución de problemas de Microsoft . . . 35
Información de resolución de problemas de Netscape . . . 38
Información de resolución de problemas de certificados digitales . . . 40
Información de resolución de problemas de Tivoli Access Manager . . . 41
Información de resolución de problemas de Lotus Notes . . . 41
Información de resolución de problemas de cifrado . . . 42
Información de resolución de problemas de dispositivos preparados para UVM . . . 43

Apéndice A. Normativas de exportación de los EE.UU. para Client Security Software . . . 45

Apéndice B. Normas para contraseñas y frases de paso . . . 47
Normas para contraseñas de hardware . . . 47
Normas para frases de paso de UVM . . . 47

Apéndice C. Avisos y marcas registradas . . . 49
Avisos . . . 49
Marcas registradas . . . 50

Prefacio

Esta sección proporciona información sobre el uso de esta guía.

Acerca de esta guía

Esta guía contiene información sobre la instalación de Client Security Software en sistemas de red de IBM, a los que también se hace referencia como clientes de IBM, que contienen chips IBM Security Chip incorporados. Esta guía también contiene instrucciones sobre cómo habilitar el chip IBM Security Chip incorporado y establecer la contraseña de hardware para el chip de seguridad.

La guía está organizada de la forma siguiente:

El ″Capítulo 1, “**Introducción a IBM Client Security Software**”″ contiene 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 Client Security Software.

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

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

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

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

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.

© Copyright IBM Corp. 2002

Utilización de esta guía

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

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

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

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

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

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

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

Información adicional

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

Capítulo 1. Introducción a IBM Client Security Software

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 clientes de IBM utilizar la seguridad para clientes a través de una red local, una corporación o Internet.

Aplicaciones y componentes de Client Security Software

Cuando instala Client Security Software, se instalan las aplicaciones y componentes de software siguientes:

- **Administrator Utility:** se trata de la interfaz que utiliza un administrador para activar o desactivar el chip IBM Security Chip 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.
- **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. El software UVM permite utilizar las características siguientes:
  - **Protección de política de cliente de UVM:** el software de UVM permite a un administrador establecer la política de seguridad del cliente, que define la forma en la que se autentica un usuario cliente en el sistema.

    Si la política indica que son necesarias las huellas dactilares para el inicio de sesión y el usuario no tiene huellas dactilares registradas, se le dará la opción de registrar las huellas dactilares como parte del inicio de sesión. Asimismo, si es necesaria la comprobación de huellas dactilares y no hay ningún escáner conectado, UVM informará de un error. Además, si no se ha registrado la contraseña de Windows o, se ha registrado de forma incorrecta, con UVM, el usuario tendrá la oportunidad de proporcionar la contraseña de Windows correcta como parte del inicio de sesión.
  - **Protección de inicio de sesión del sistema de UVM:** el software UVM permite a un administrador 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.
  - **Protección de protector de pantalla de Client Security de UVM:** el software UVM permite a los usuarios controlar el acceso al sistema mediante una interfaz de protector de pantalla de Client Security.
- **Administrator Console:** Client Security Software Administrator Console permite a un administrador de seguridad efectuar tareas específicas del administrador de forma remota.
- **User Configuration Utility:** permite a un usuario cliente cambiar la frase de paso de UVM. En Windows 2000 o Windows XP, User Configuration Utility permite a los usuarios cambiar las contraseñas de inicio de sesión de Windows para que las reconozca UVM y actualizar los archivadores de claves. Un usuario también puede crear copias de seguridad de los certificados digitales creados con el chip IBM Security Chip incorporado.

© Copyright IBM Corp. 2002

Características PKI (Public Key Infrastructure)

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 el chip IBM Security Chip incorporado 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 almacena en el chip IBM Security Chip incorporado. Además, los usuarios de Netscape puede elegir los chips IBM Security Chip incorporados como los generadores 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 el chip IBM Security Chip incorporado.
- **Posibilidad de transferir certificados digitales al chip IBM Security Chip incorporado.** 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 IBM embedded Security Subsystem CSP. Esto aumenta enormemente la protección ofrecida a las claves privadas asociadas con los certificados porque éstos se almacenarán de forma segura en el chip IBM Security Chip incorporado, en lugar de en un software vulnerable.
- **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. Client Security Software proporciona una interfaz que permite definir un archivador para las claves y certificados digitales creados con el chip IBM Security Chip incorporado 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 de forma rápida y sencilla. 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 ahora 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 para UVM utilice cualquier sistema de la red, como si estuviese en su propia estación de trabajo. Si un usuario está autorizado para utilizar UVM en cualquier cliente registrado en CSS, podrá importar sus datos personales en cualquier otro cliente registrado de la red. Sus datos personales se actualizarán y mantendrán 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, estarán disponibles inmediatamente en todos los demás sistemas.
- **Certificación en FIPS 140-1.** Client Security Software soporta bibliotecas criptográficas certificadas en FIPS 140-1. Las bibliotecas RSA BSAFE certificadas en FIPS se utilizan en sistemas TCPA.
- **Caducidad de las frases de paso.** Client Security Software establece una frase de paso y una política de caducidad de frases de paso específica para cada usuario cuando éste se añade a UVM.
- **Protección automática de carpetas seleccionadas.** La función Protección automática de carpetas permite al administrador de Client Security Software designar que se proteja automáticamente la carpeta Mis documentos de todos los usuarios autorizados para UVM, sin precisar ninguna acción por parte de los usuarios.

Capítulo 2. Cómo empezar

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

Requisitos de hardware

Antes de bajar e instalar el software, asegúrese de que el hardware del sistema es compatible con 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/ww/security/secdownload.html.

El chip IBM Security Chip

El chip IBM Security Chip incorporado 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 chips IBM Security Chip incorporados soportan Client Security Software. Si intenta bajar e instalar el software en un sistema que no contenga un chip IBM Security Chip incorporado, 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/ww/resources/security/secdownload.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 Client Security Software.

Sistemas operativos

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 máquina 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**

© Copyright IBM Corp. 2002

UVM proporciona una interfaz conectar y listo para dispositivos biométricos. Debe instalar 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 Client Security Software y después reinstalar el sensor preparado para UVM.

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

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

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

- **Lotus Notes versión 4.5 o posterior**

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

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

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

- **RSA SecurID Software Token**

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

- **Lector de huellas dactilares Targus**

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

- **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

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

- Internet Explorer 5.0 o posterior
- Netscape 4.51 a Netscape 7

Información del nivel cifrado del navegador Web

Si está instalado el soporte para un cifrado fuerte, utilice la versión de 128 bits del navegador Web. En caso contrario, utilice la versión de 40 bits del navegador Web. Para comprobar el nivel cifrado del navegador Web, consulte el sistema de ayuda proporcionado con el navegador.

Servicios criptográficos

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, Client Security Software permite utilizar las operaciones criptográficas del chip IBM Security Chip incorporado 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 del chip IBM Security Chip incorporado, puede utilizar el chip IBM Security Chip incorporado para generar certificados digitales para Netscape, Entrust, RSA y otras aplicaciones que utilicen PKCS#11.

Aplicaciones de correo electrónico

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

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

Cómo bajar el software

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

Formulario de registro

Cuando baja el software, debe completar un formulario de registro y un cuestionario, y aceptar los términos de la licencia. Siga las instrucciones proporcionadas en el sitio Web para bajar el software.

Los archivos de instalación de Client Security Software están incluidos dentro del archivo autoextraíble denominado csec51.exe.

Normativas de exportación

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 Client Security Software. Para obtener más información sobre las normativas de exportación que regulan Client Security Software, consulte el Apéndice A, “Normativas de exportación de los EE.UU. para Client Security Software”, en la página 45.

Capítulo 3. Antes de instalar el software

Esta sección contiene instrucciones sobre los requisitos previos para ejecutar el programa de instalación y configurar Client Security Software en clientes de IBM. Todos los archivos necesarios para la instalación se proporcionan dentro del archivo csec51.exe que puede bajarse del sitio Web de IBM.

Antes de instalar el software

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

Instalación en clientes que ejecutan Windows XP y Windows 2000

Los usuarios de Windows XP y Windows 2000 deben iniciar una sesión con derechos de administrador para instalar 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 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 el subsistema de seguridad (Security Chip incorporado) y se generan las claves de cifrado de hardware. Estas características son la contraseña del administrador y Seguridad ampliada.

La contraseña del administrador (NetVista)

Las contraseñas del administrador evitan que las personas no autorizadas cambien los valores de configuración de un sistema de IBM. Estas contraseñas se establecen utilizando el programa Configuration/Setup Utility, al que se accede pulsando F1 durante la secuencia de arranque del sistema.

Contraseña del supervisor (ThinkPad)

Las contraseñas del supervisor evitan que las personas no autorizadas cambien los valores de configuración de un sistema ThinkPad de IBM. Estas contraseñas se establecen utilizando el programa IBM BIOS Setup Utility, al que se accede pulsando F1 durante la secuencia de arranque del sistema.

Seguridad ampliada

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

© Copyright IBM Corp. 2002

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 los modelos NetVista (6059, 6569, 6579, 6649, 6646 y todos los modelos Q1x), debe abrir Administrator Utility para habilitar el chip y generar las claves de hardware.

Si Seguridad ampliada está habilitada en estos modelos NetVista, debe utilizar Administrator Utility para habilitar el chip Security Chip incorporado y generar las claves de cifrado de hardware después de instalar 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 el chip y generar las claves de hardware.

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 el chip de seguridad. Después de haber habilitado el chip, puede utilizar Administrator Utility para generar las claves de hardware.

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 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 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 NetVista adecuado y siga las instrucciones de la página Web.

Utilización del par de claves del archivador

El par de claves del archivador, que incluye la clave pública del administrador y la clave privada del administrador, permite generar las claves de cifrado de hardware para un cliente de IBM y mantener copias de los datos de claves en otro sitio para su restauración.

Ya que para crear el par de claves del archivador se utiliza Client Security Administrator Utility, debe instalar Client Security Software en un cliente de IBM

inicial y después crear el par de claves del archivador. Más adelante se proporcionan instrucciones para instalar y configurar el software en el primer cliente de IBM.

Nota: si tiene previsto utilizar una política de UVM que pueda usarse en clientes remotos, debe utilizar el mismo par de claves del archivador para instalar el software en esos clientes.

Capítulo 4. Instalación, actualización y desinstalación del software

Esta sección contiene instrucciones para bajar, instalar y configurar Client Security Software en clientes de IBM. Esta sección 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 Client Security Software 5.0, debe descifrar todos los archivos cifrados antes de instalar Client Security Software 5.1. Client Security Software 5.1 no puede descifrar los archivos que fueron cifrados utilizando versiones anteriores a Client Security Software 5.0, debido a cambios en su implementación de cifrado de archivos.

Cómo bajar e instalar el software

Todos los archivos necesarios para la instalación de Client Security Software se proporcionan dentro del archivo csec51.exe que puede bajarse del sitio Web de IBM en http://www.pc.ibm.com/ww/security/secdownload.html. El sitio Web proporciona información que ayuda a comprobar que su sistema tiene el chip IBM Security Chip incorporado y que le permite seleccionar la oferta de 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/ww/security/secdownload.html
2. Utilizando la información del sitio Web, compruebe si su máquina tiene instalado el chip IBM Security Chip incorporado; para ello busque su número de modelo en la tabla de requisitos del sistema; después pulse **Continue** (Continuar).
3. Seleccione el botón de selección que se corresponda con su tipo de máquina y pulse **Continue** (Continuar).
4. Cree un ID de usuario, regístrese con IBM rellenando el formulario en línea y revise el Acuerdo de licencia; después pulse **Accept Licence** (Acepto la licencia).

   Se le redirigirá automáticamente a la página para bajarse Client Security.
5. Siga los pasos de esta página para bajarse todos los controladores de dispositivo necesarios, los archivos readme, el software, los documentos de referencia y los programas de utilidad adicionales que constituyen IBM Client Security Software. Siga la secuencia para bajarlo especificada en el sitio Web.
6. En el escritorio de Windows, pulse **Inicio > Ejecutar**.
7. En el campo Ejecutar, escriba `d:\directorio\csec51.exe`, donde d:\directorio\ es la letra de la unidad y el directorio donde se encuentra el archivo.
8. Pulse **Aceptar**.

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

© Copyright IBM Corp. 2002

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

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

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

Utilización de asistente de instalación de IBM Client Security Software

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

Estos pasos son los siguientes:

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

  La contraseña del administrador de seguridad se utiliza para controlar el acceso a IBM Client Security Administrator Utility, que se utiliza para cambiar los valores de seguridad para este sistema.

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

  Las claves de seguridad del administrador son un conjunto de claves digitales que se almacenan en un archivo del sistema. Es aconsejable que guarde estas claves de seguridad en un disco o unidad extraíble. Cuando se hace un cambio en la política de seguridad en Security Administrator Utility, se le solicitará este archivo para comprobar que el cambio de política está autorizado.

  También se guarda información de seguridad de copia de de seguridad por si necesita alguna vez sustituir la placa del sistema o la unidad de disco duro del sistema. Esta información de copia de seguridad debería almacenarse en algún sitio fuera del sistema.

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

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

- **Autorización de los usuarios**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   - **Utilizar una clave de seguridad existente**

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

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

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

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

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

6. Pulse **Siguiente**.

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

7. Habilite la protección de IBM Client Security; para ello seleccione los recuadros de selección adecuados para que aparezca una marca de selección en cada recuadro seleccionado y pulse **Siguiente**. Las selecciones disponibles de Client Security son las siguientes:
   - **Proteger el acceso al sistema mediante la sustitución del inicio de sesión de Windows normal por el inicio de sesión seguro de Client Security**

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

- **Habilitar el cifrado de archivos y carpetas**

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

- **Habilitar el soporte de IBM Client Security Password Manager**

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

- **Sustituir el inicio de sesión de Lotus Notes por el inicio de sesión de IBM Client Security**

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

- **Habilitar el soporte de Entrust**

  Seleccione este recuadro si desea habilitar la integración con los productos de software de seguridad de Entrust.

- **Proteger Microsoft Internet Explorer**

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

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

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

   Se muestra la pantalla Seleccionar el nivel de seguridad del sistema.
9. Seleccione un nivel de seguridad del sistema mediante el procedimiento siguiente:

a. Seleccione los requisitos de autenticación que va a utilizar pulsando los recuadros de selección adecuados. Puede seleccionar más de un requisito de autenticación.
b. 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 de IBM Client Security.

10. Revise los valores de seguridad y efectúe una de las acciones siguientes:
    - Para aceptar los valores, pulse **Finalizar**.
    - Para cambiar los valores, pulse **Atrás** y haga los cambios apropiados; después vuelva a esta pantalla y pulse **Finalizar**.

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

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

Habilitación del chip IBM Security Chip

El chip IBM Security Chip 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 la sección anterior.

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

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

   Aparece una pantalla que muestra un mensaje indicando que el chip IBM Security Chip 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, debe inhabilitarla en la configuración del BIOS 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 Client Security Subsystem** para abrir Administrator Utility.

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

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

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

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

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

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

Instalación desatendida

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

Antes de iniciar una instalación desatendida, lea el Capítulo 3, “Antes de instalar el software”, en la página 9. No se muestra ningún mensaje de error durante las instalaciones desatendidas. Si una instalación desatendida termina de forma prematura, debe efectuar una instalación atendida para ver los mensajes de error que pudieran aparecer.

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

Para obtener información completa sobre cómo efectuar una instalación desatendida, complete el procedimiento siguiente, consulte el archivo css51readme disponible en el sitio Web de IBM en http://www.pc.ibm.com/ww/security/secdownload.html.

Despliegue masivo

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

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

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

Hay dos pasos principales para efectuar un despliegue masivo:

- Instalación masiva

- Configuración masiva

Instalación masiva

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

Para iniciar una instalación masiva, complete el procedimiento siguiente:

1. Cree un archivo CSS.ini.

   Este paso sólo es necesario si desea efectuar una configuración masiva.
2. Extraiga el contenido del paquete de instalación de CSS con Winzip utilizando los nombres de carpeta.
3. Edite las entradas `szIniPath` y `szDir`, que son necesarias para una configuración masiva, en el archivo setup.iss.

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

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

A continuación se lista el contenido completo de archivo setup.iss con algunas descripciones: [InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csssetup.ini (El parámetro anterior es el nombre y la ubicación del archivo .ini, que es necesario para la configuración masiva. Si es una unidad de red, debe estar correlacionada. Cuando no se vaya a utilizar una configuración masiva con una instalación silenciosa, elimine esta entrada). [File Transfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0] Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0] szDir=C:\Archivos de programa\IBM\Security (El parámetro anterior es el directorio usado para instalar Client Security. Debe ser un directorio local del sistema). Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client Security Software (El parámetro anterior es el grupo de programas de Client Security). Result=1 [Application] Name=Client Security Version=5.00.002f Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0] Result=6 BootOption=3

Configuración masiva

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

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

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

[CSSSetup]	Cabecera de la sección para la configuración de CSS.
suppw=arranque	Contraseña del administrador/supervisor. Déjela en blanco si no es necesaria.
hwpw=11111111	Contraseña de hardware de CSS. Debe tener ocho caracteres. Es siempre necesaria. Debe ser correcta si ya se ha establecido una contraseña de hardware.
newkp=1	1 para generar un par de claves del administrador nuevo 0 para utilizar un par de claves del administrador existente.
keysplit=1	Cuando newkp es 1, este parámetro determina el número de componentes de clave privada. **Nota:** si el par de claves existente utiliza varias partes de clave privada, todas las partes de clave privada deben almacenarse en el mismo directorio.
kpl=c:\jgk	Ubicación del par de claves del administrador cuando newkp es 1, si es una unidad de red debe estar correlacionada.
kal=c:\jgk\archive	Ubicación del archivador de claves de usuario, si es una unidad de red debe estar correlacionada.
pub=c:\jk\admin.key	Ubicación de la clave pública del administrador cuando se utiliza un par de claves del administrador existente, si es una unidad de red debe estar correlacionada.
pri=c:\jk\private1.key	Ubicación de la clave privada del administrador cuando se utiliza un par de claves del administrador existente, si es una unidad de red debe estar correlacionada.
clean=0	1 para suprimir el archivo .ini después de la inicialización. 0 para dejar el archivo .ini después de la inicialización.
[UVMEnrollment]	Cabecera de la sección para la inscripción de usuarios.
enrollall=0	1 para inscribir todas las cuentas de usuarios locales en UVM, 0 para inscribir cuentas de usuarios específicos en UVM.
defaultuvmpw=arriba	Cuando enrollall es 1, esta es la frase de paso de UVM para todos los usuarios.
defaultwinpw=abajo	Cuando enrollall es 1, esta es la contraseña de Windows registrada con UVM para todos los usuarios.
enrollusers=2	Cuando enrollall es 0, este es el número de usuarios que se inscribirán en UVM.
user1=juan	Enumere el número de usuarios que se van a inscribir, empezando por 1; los nombres de usuario deben ser los nombres de las cuentas. Para obtener el nombre real de la cuenta en XP, haga lo siguiente: 1. Inicie Administración de equipos (Administrador de dispositivos). 2. Expanda el nodo Usuarios locales y grupos. 3. Abra la carpeta Usuarios. Los elementos listados en la columna Nombre son los nombres de las cuentas.
user1uvmpw=cromo	Enumere la frase de paso de UVM del número de usuarios que se van a inscribir, empezando por 1.
user1winpw=redondo	Enumere la contraseña de Windows registrada con UVM del número de usuarios que se va a inscribir, empezando por 1.
user1domain=0	0 para indicar que esta cuenta es local. 1 para indicar que esta cuenta está en el dominio.
user2=elena user2uvmpw=izda user2winpw=dcha user2domain=0	

[UVMAppConfig]	Cabecera de la sección para la configuración de aplicaciones y módulos preparados para UVM.
uvmlogon=0	1 para utilizar la protección de inicio de sesión de UVM, 0 para utilizar el inicio de sesión de Windows.
entrust=0	1 para utilizar UVM para la autenticación de Entrust, 0 para utilizar la autenticación de Entrust.
notes=0	1 para utilizar la protección de UVM para Lotus Notes, 0 para utilizar la protección mediante contraseña de Notes.
passman=0	1 para utilizar Password Manager, 0 para no utilizar Password Manager
folderprotect=0	1 para utilizar Cifrado de archivos y carpetas, 0 para no utilizar Cifrado de archivos y carpetas.

Actualización de la versión de Client Security Software

Los clientes que tengan instaladas versiones de Client Security anteriores a la Versión 5.0 deberían actualizar su software a Client Security Software Versión 5.1 para aprovechar las nuevas características de Client Security.

Importante: los sistemas TCPA que tuvieran instalado IBM Client Security Software Versión 4.0x deben borrar la información del chip antes de instalar IBM Client Security Software Versión 5.1. 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 de utilidad del BIOS.
4. Rearranque el sistema.
5. Instale Client Security Software Release 5.1 y configúrelo utilizando el Asistente de instalación de IBM Client Security Software.

Actualización a Client Security Versión 5.1 utilizando los datos de seguridad existentes

Si desea actualizar desde un release de Client Security Software anterior a la Versión 5.0 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 > Client Utility**.
   b. Pulse el botón **Actualizar archivador** para asegurar que la información de copia de seguridad se actualiza.

      Anote el directorio del archivador.
   c. Salga de IBM Client Security Software User Configuration Utility.
2. Elimine la versión existente de Client Security Software completando los pasos siguientes:

a. Localice las claves pública y privada del administrador que se crearon cuando configuró la versión anterior de Client Security Software.
b. Pulse **Inicio > Configuración > Panel de control > Agregar o quitar programas** y seleccione eliminar IBM Client Security Software.
c. Seleccione **No** cuando se le solicite rearrancar.
d. Concluya el sistema.

3. Borre la información del chip IBM Security Chip incorporado completando los pasos siguientes:
   a. Encienda el sistema.
   b. Pulse F1 para entrar en el programa BIOS Setup Utility.
   c. Vaya a los valores del chip de seguridad y borre su información.
   d. Salga del programa BIOS Setup Utility.

      El sistema continuará con el rearranque.
4. Ejecute el programa de instalación de Client Security Software Versión 5.0.
5. Rearranque el sistema cuando se le solicite.

   Después de rearrancar, el Asistente de instalación de Client Security Software se iniciará automáticamente. NO ejecute el Asistente de instalación.
6. Pulse **Cancelar** para salir del Asistente de instalación.
7. Efectúe una copia de seguridad temporal de la política de seguridad por omisión completando los pasos siguientes:
   a. Mediante el Explorador de Windows, vaya al directorio de instalación de IBM Client Security Software (por omisión es c:\Archivos de programa\ibm\security).
   b. Pulse el botón derecho del ratón en la carpeta UVM_Policy y seleccione **Copiar**.
   c. Pulse el botón derecho del ratón en el escritorio de Windows y pulse **Pegar**.

      Esto creará una copia de seguridad temporal en el escritorio de Windows.

      Nota: los valores de política de seguridad existentes serán sustituidos por los nuevos valores por omisión.
8. Restaure los valores de IBM Client Security Software Versión 4.0x completando los pasos siguientes:
   a. Pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

      Se muestra la pantalla principal de IBM Client Security Software Administrator Utility.
   b. Pulse el botón **Configuración de claves**.
   c. Seleccione **Sí** para restaurar las claves desde el archivador de claves.
9. Proporcione la ubicación del directorio del archivador anterior.
10. Proporcione la ubicación de los archivos de claves pública y privada del administrador que creó en el release anterior.

    Se le notificará que el archivador se va a actualizar para el nuevo release.
11. Pulse **Aceptar**.
12. Proporcione la ubicación para crear las nuevas claves del administrador. Asegúrese de crear las claves en una ubicación diferente de la ubicación de las claves del administrador existentes. Si tiene claves del administrador que ya había creado para el Release 5.0 en otro sistema, puede seleccionar **Utilizar un par de claves existente del archivador de CSS** y proporcionar la ubicación de las claves existentes.

13. Pulse **Siguiente**.

    El archivador se convertirá y restaurará.
14. Salga de la aplicación cuando haya terminado.
15. Restaure los valores de política completando los pasos siguientes:
    a. Mediante el Explorador de Windows, vaya al directorio de instalación de IBM Client Security Software (por omisión es c:\Archivos de programa\ibm\security).
    b. Con el botón izquierdo del ratón, arrastre la carpeta UVM_Policy desde el escritorio al directorio de instalación de IBM Client Security Software.
    c. Pulse **Sí** en todos los mensajes de aviso.

    Sus datos de seguridad se han migrado a Client Security Software Release 5.0.

Nota: si cambió previamente la política de seguridad en Client Security Software Versión 4.0x, es posible que quiera volver a someter los valores de política de seguridad completando los pasos siguientes:

1. Pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.
2. Pulse el botón **Configurar soporte de aplicaciones y políticas**.
3. Pulse el botón **Política de aplicaciones**.
4. Pulse el botón **Editar política**.

Actualización desde el Release 5.1 a versiones posteriores utilizando 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** para asegurar que la información de copia de seguridad se actualiza.

       Anote el directorio del archivador.
    c. Salga de IBM Client Security Software User Configuration Utility.
2. Elimine la versión existente de Client Security Software completando los pasos siguientes:
    a. Localice las claves pública y privada del administrador que se crearon cuando configuró la versión anterior de Client Security Software.
    b. Ejecute csec51.exe.
    c. Seleccione **Actualizar**.
    d. Rearranque el sistema.

Desinstalación de Client Security Software

Asegúrese de desinstalar los distintos programas de utilidad 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.

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 **Sí** para desinstalar el software.
8. 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.
9. Pulse **Aceptar** 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. No obstante, el archivador de claves no se ve afectado cuando se desinstala Client Security Software.

Capítulo 5. Resolución de problemas

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

Funciones del administrador

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

Establecimiento de una contraseña del administrador (ThinkCentre)

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

- Cambiar la contraseña de hardware del chip IBM Security Chip incorporado
- Habilitar o inhabilitar el chip IBM Security Chip incorporado
- Borrar la información del chip IBM Security Chip incorporado

Atención:

- No borre la información ni inhabilite el chip IBM Security Chip incorporado si está habilitada la protección de UVM. Si lo hace, el contenido del disco duro queda inutilizable y debe volver a formatear la unidad de disco duro y reinstalar todo el software.

  Para inhabilitar la protección de UVM, abra Administrator Utility, pulse **Configurar soporte de aplicaciones y políticas** y quite la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**. Debe reiniciar el sistema para que se inhabilite la protección de UVM.
- No borre la información ni inhabilite el chip IBM Security Chip incorporado si está habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema.
- Cuando se borra la información del chip IBM Security Chip incorporado, se pierden todas las claves de cifrado y los certificados almacenados en el chip.

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:

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.

© Copyright IBM Corp. 2002

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

Importante: conserve un registro de la contraseña del administrador en un lugar seguro. Si pierde u olvida la contraseña del administrador, no podrá acceder al programa Configuration/Setup Utility y no podrá cambiar o suprimir la contraseña 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 el chip IBM Security Chip incorporado
- Borrar la información del chip IBM Security Chip incorporado

Atención:

- No borre la información ni inhabilite el chip IBM Security Chip incorporado si está habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema.

  Para inhabilitar la protección de UVM, abra Administrator Utility, pulse **Configurar soporte de aplicaciones y políticas** y quite la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**. Debe reiniciar el sistema para que se inhabilite la protección de UVM.

  Cuando se borra la información del chip IBM Security Chip incorporado, se pierden todas las claves de cifrado y los certificados almacenados en el chip.
- 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 el procedimiento siguiente:

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

   Se abre el menú principal del programa IBM BIOS 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.

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

Importante: conserve un registro de la contraseña del supervisor en un lugar seguro. Si pierde u olvida la contraseña del supervisor, no podrá acceder al

programa IBM BIOS Setup Utility y no podrá cambiar o suprimir la contraseña. Consulte la documentación del hardware incluida con el sistema para obtener más información.

Protección de la contraseña de hardware

Establezca la contraseña del chip de seguridad para habilitar el chip IBM Security Chip incorporado para un cliente. Después de establecer una contraseña del chip de seguridad, el acceso a Administrator Utility está protegido por esta contraseña. Debería proteger la contraseña del chip de seguridad para impedir que los usuarios no autorizados cambien valores en Administrator Utility.

Borrado de la información del chip IBM Security Chip incorporado (ThinkCentre)

Si desea borrar todas las claves de cifrado del usuario del chip IBM Security Chip incorporado y borrar la contraseña de hardware para el chip, debe borrar la información del chip. Lea la información bajo Atención antes de borrar la información del chip IBM Security Chip incorporado.

Atención:

- No borre la información ni inhabilite el chip IBM Security Chip incorporado si está habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema.

  Para inhabilitar la protección de UVM, abra Administrator Utility, pulse **Configurar soporte de aplicaciones y políticas** y quite la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**. Debe reiniciar el sistema para que se inhabilite la protección de UVM.
- Cuando se borra la información del chip IBM Security Chip incorporado, se pierden todas las claves de cifrado y los certificados almacenados en el chip.

Para borrar la información del chip IBM Security Chip incorporado, complete el procedimiento siguiente:

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 **Security** (Seguridad).
4. Seleccione **IBM TCPA Feature Setup** (Configuración de la función IBM TCPA).
5. Seleccione **Clear IBM TCPA Security Feature** (Borrar la función de seguridad IBM TCPA).
6. Seleccione **Yes** (Sí).
7. Pulse Esc para continuar.
8. Pulse Esc para salir y guardar los valores.

Borrado de la información del chip IBM Security Chip incorporado (ThinkPad)

Si desea borrar todas las claves de cifrado del usuario del chip IBM Security Chip incorporado y borrar la contraseña de hardware para el chip, debe borrar la información del chip. Lea la información bajo Atención antes de borrar la información del chip IBM Security Chip incorporado.

Atención:

- No borre la información ni inhabilite el chip IBM Security Chip incorporado si está habilitada la protección de UVM. Si lo hace, el contenido del disco duro queda inutilizable y debe volver a formatear la unidad de disco duro y reinstalar todo el software.

  Para inhabilitar la protección de UVM, abra Administrator Utility, pulse **Configurar soporte de aplicaciones y políticas** y quite la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**. Debe reiniciar el sistema para que se inhabilite la protección de UVM.
- Cuando se borra la información del chip IBM Security Chip incorporado, se pierden todas las claves de cifrado y los certificados almacenados en el chip.

Para borrar la información del chip IBM Security Chip incorporado, complete el procedimiento siguiente:

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

   Nota: en algunos modelos de ThinkPad, es posible que necesite pulsar la tecla F1 durante el encendido para acceder al programa IBM BIOS Setup Utility. Consulte el mensaje de ayuda en el programa IBM BIOS Setup Utility para obtener detalles.

   Se abre el menú principal del programa IBM BIOS Setup Utility.
3. Seleccione **Config** (Configurar).
4. Seleccione **IBM Security Chip**.
5. Seleccione **Clear IBM Security Chip** (Borrar el chip IBM Security Chip).
6. Seleccione **Yes** (Sí).
7. Pulse Intro para continuar.
8. Pulse F10 para guardar y salir.

Administrator Utility

La sección siguiente contiene información que debe tenerse en cuenta a la hora de utilizar Administrator Utility.

Supresión de usuarios

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

Acceso denegado a objetos seleccionados con el control de Tivoli Access Manager

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

Limitaciones conocidas

Esta sección contiene información sobre las limitaciones conocidas en relación con Client Security Software.

Utilización de Client Security Software con sistemas operativos Windows

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

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

Utilización de Client Security Software con aplicaciones de Netscape

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

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

- SHA-1
- MD5

El certificado del chip IBM Security Chip incorporado y los algoritmos de cifrado

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

Cuando se envía correo electrónico desde un cliente Outlook Express (128 bits) a otro cliente Outlook Express (128 bits): si utiliza Outlook Express con la versión de 128 bits de Internet Explorer 4.0 ó 5.0 para enviar correo electrónico cifrado a otros clientes que utilicen Outlook Express (128 bits), los mensajes de correo electrónico cifrados con el certificado del chip IBM Security Chip incorporado sólo pueden utilizar el algoritmo 3DES.

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

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

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

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

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

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

Limitaciones de User Configuration Utility

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

Windows XP Professional

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

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

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

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

Estas limitaciones desaparecen después de que un administrador inicie y salga de Administrator Utility.

Windows XP Home

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

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

Mensajes de error

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

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

Tablas de resolución de problemas

La sección 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 ya hay instalada una versión anterior de Client Security Software.	Pulse **Aceptar** para salir de la ventana. Haga lo siguiente: 1. Desinstale el software. 2. Reinstale el software. **Nota:** si tiene previsto utilizar la misma contraseña de hardware para proteger el chip IBM Security Chip incorporado, no tiene que borrar la información del chip ni restablecer la contraseña.

Síntoma del problema	Posible solución
El acceso de instalación se ha denegado debido a una contraseña de hardware desconocida	**Acción**
Al instalar el software en un cliente de IBM con un chip IBM Security Chip incorporado habilitado, la contraseña de hardware para el chip IBM Security Chip incorporado es desconocida.	Borre la información del chip para continuar con la instalación.
El archivo setup.exe no responde adecuadamente (CSS versión 4.0x)	**Acción**
Si extrae todos los archivos del archivo csec4_0.exe en un directorio común, el archivo setup.exe no funcionará correctamente.	Ejecute el archivo smbus.exe para instalar el controlador de dispositivo SMBus y después ejecute el archivo csec4_0.exe para instalar el código de Client Security Software.

Información de resolución de problemas de Administrator Utility

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

Síntoma del problema	Posible solución
No se cumple la política de frases de paso de UVM	**Acción**
El recuadro de selección **no contener más de 2 caracteres repetidos** no funciona en IBM Client Security Software Versión 5.0	Se trata de una limitación conocida con IBM Client Security Software Versión 5.0.
El botón Siguiente no está disponible después de entrar y confirmar la frase de paso de UVM en Administrator Utility	**Acción**
Cuando se añaden usuarios a UVM, puede que el botón **Siguiente** no esté disponible después de entrar y confirmar la frase de paso de UVM en Administrator Utility.	Pulse el elemento **Información** en la barra de tareas de Windows y continúe el procedimiento.
Se muestra un mensaje de error al intentar editar la política local de UVM	**Acción**
Cuando edita la política local de UVM, puede que aparezca un mensaje de error si no hay ningún usuario inscrito en UVM.	Añada un usuario a UVM antes de intentar editar el archivo de políticas.
Se muestra un mensaje de error al cambiar la clave pública del administrador	**Acción**
Cuando borra la información del chip IBM Security Chip incorporado y después restaura el archivador de claves, puede que aparezca un mensaje de error si cambia la clave pública del administrador.	Añada los usuarios a UVM y solicite nuevos certificados, si procede.

Síntoma del problema	Posible solución
Se muestra un mensaje de error al intentar recuperar una frase de paso de UVM	**Acción**
Cuando cambia la clave pública del administrador y después intenta recuperar una frase de paso de UVM para un usuario, puede que aparezca un mensaje de error.	Haga una de las cosas siguientes: • Si no se necesita la frase de paso de UVM para el usuario, no se precisa ninguna acción. • Si se necesita la frase de paso de UVM para el usuario, debe añadir el usuario a UVM y solicitar nuevos certificados, si procede.
Se muestra un mensaje de error al intentar guardar el archivo de políticas de UVM	**Acción**
Cuando intenta guardar un archivo de políticas de UVM (globalpolicy.gvm) pulsando **Aplicar** o **Guardar**, se muestra un mensaje de error.	Salga del mensaje de error, edite el archivo de políticas de UVM de nuevo para hacer los cambios que desee y después guarde el archivo.
Se muestra un mensaje de error al intentar abrir el editor de política de UVM	**Acción**
Si el usuario actual (que tiene iniciada una sesión en el sistema operativo) no se ha añadido a UVM, no se abrirá el editor de política de UVM.	Añada el usuario a UVM y abra el editor de política de UVM.
Se muestra un mensaje de error al utilizar Administrator Utility	**Acción**
Mientras utiliza Administrator Utility, puede mostrarse el mensaje de error siguiente: Se ha producido un error de E/S del almacenamiento intermedio al intentar acceder al chip de Client Security. Esto podría resolverse mediante un rearranque.	Salga del mensaje de error y reinicie el sistema.
Se muestra un mensaje de inhabilitar chip cuando se cambia la contraseña del chip de seguridad	**Acción**
Cuando intenta cambiar la contraseña del chip de seguridad y pulsa Intro o Tab > Intro después de escribir la contraseña de confirmación, el botón Inhabilitar chip se habilitará y aparecerá un mensaje de confirmación para inhabilitar el chip.	Haga lo siguiente: 1. Salga de la ventana de confirmación para inhabilitar el chip. 2. Para cambiar la contraseña del chip de seguridad, escriba la contraseña nueva, escriba la contraseña de confirmación y después pulse **Cambiar**. No pulse Intro ni Tab > Intro después de escribir la contraseña de confirmación.

Información de resolución de problemas de User Configuration Utility

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

Síntoma del problema	**Posible solución**
Los usuarios limitados no pueden realizar ciertas funciones de User Configuration Utility en Windows XP Professional	**Acción**
Es posible que los usuarios limitados de Windows XP Professional no puedan efectuar las siguientes tareas de User Configuration Utility: • Cambiar sus frases de paso de UVM • Actualizar la contraseña de Windows registrada con UVM • Actualizar el archivador de claves	Estas limitaciones desaparecen después de que un administrador inicie y salga de Administrator Utility.
Los usuarios limitados no pueden utilizar User Configuration Utility en Windows XP Home	**Acción**
Los usuarios limitados de Windows XP Home no podrán utilizar User Configuration Utility en ninguna de las situaciones siguientes: • Client Security Software está instalado en una partición con formato NTFS • La carpeta de Windows está en una partición con formato NTFS • La carpeta del archivador está en una partición con formato NTFS	Se trata de una limitación conocida con Windows XP Home. No hay ninguna solución para este problema.

Información de resolución de problemas específicos de ThinkPad

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

Síntoma del problema	**Posible solución**
Se muestra un mensaje de error al intentar efectuar una función del administrador de Client Security	**Acción**
El mensaje de error siguiente se muestra después de intentar efectuar una función del administrador de Client Security: ERROR 0197: Se ha solicitado un cambio remoto no válido. Pulse <F1> para abrir la configuración	La contraseña del supervisor del ThinkPad debe estar inhabilitada para efectuar ciertas funciones del administrador de Client Security. Para inhabilitar la contraseña del supervisor, complete el procedimiento siguiente: 1. Pulse F1 para acceder a IBM BIOS Setup Utility. 2. Entre la contraseña actual del supervisor. 3. Entre una contraseña del supervisor en blanco y confirme una contraseña en blanco. 4. Pulse Intro. 5. Pulse F10 para guardar y salir.

Síntoma del problema	Posible solución
Un sensor de huellas dactilares preparado para UVM diferente no funciona correctamente	**Acción**
El sistema IBM ThinkPad no soporta el intercambio de varios sensores de huellas dactilares preparados para UVM.	No intercambie los modelos de sensor de huellas dactilares. Utilice el mismo modelo cuando trabaje de forma remota y cuando trabaje desde una estación de acoplamiento.

Información de resolución de problemas de Microsoft

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

Síntoma del problema	Posible solución
El protector de pantalla sólo se muestra en la pantalla local	**Acción**
Cuando se utiliza la función de escritorio extendido de Windows, el protector de pantalla de Client Security Software sólo se mostrará en la pantalla local aunque el acceso al sistema y al teclado estará protegido.	Si se está mostrando alguna información confidencial, minimice las ventanas en el escritorio extendido antes de invocar el protector de pantalla de Client Security.
Los archivos del Reproductor de Windows Media se cifran en lugar de ejecutarse en Windows XP	**Acción**
En Windows XP, cuando abre una carpeta y pulsa **Reproducir todo**, el contenido del archivo se cifrará en lugar de reproducirse mediante el Reproductor de Windows Media.	Para hacer que el Reproductor de Windows Media reproduzca los archivos, complete el procedimiento siguiente: 1. Inicie el Reproductor de Windows Media. 2. Seleccione todos los archivos en la carpeta adecuada. 3. Arrastre los archivos al área de la lista de reproducción del Reproductor de Windows Media.
Client Security no funciona correctamente para un usuario inscrito en UVM	**Acción**
Es posible que el usuario cliente inscrito en UVM haya cambiado su nombre de usuario de Windows. Si ocurre eso, se perderá toda la funcionalidad de Client Security.	Vuelva a inscribir el nombre de usuario nuevo en UVM y solicite todas las credenciales nuevas.
Nota: en Windows XP, los usuarios inscritos en UVM cuyo nombre de usuario de Windows se haya cambiado previamente, no serán reconocidos por UVM. Esta limitación se produce incluso si el nombre de usuario de Windows se cambió antes de instalar Client Security Software.	

Síntoma del problema	Posible solución
Problemas al leer correo electrónico cifrado utilizando Outlook Express	**Acción**
El correo electrónico cifrado no puede descifrarse debido a las diferencias en los niveles de cifrado de los navegadores Web utilizados por el remitente y el destinatario. **Nota:** para utilizar navegadores Web de 128 bits con Client Security Software, el chip IBM Security Chip incorporado debe soportar el cifrado de 256 bits. Si el chip IBM Security Chip incorporado soporta el cifrado de 256 bits, debe utilizar un navegador Web de 40 bits. Puede averiguar el nivel de cifrado proporcionado por Client Security Software en Administrator Utility.	Compruebe lo siguiente: 1. El nivel de cifrado para el navegador Web que utiliza el remitente es compatible con el nivel de cifrado del navegador Web que utiliza el destinatario. 2. El nivel de cifrado para el navegador Web es compatible con el nivel de cifrado proporcionado por el firmware de Client Security Software.
Problemas al utilizar un certificado desde una dirección que tiene asociados varios certificados	**Acción**
Outlook Express puede listar varios certificados asociados con una sola dirección de correo electrónico y algunos de esos certificados pueden quedar invalidados. Un certificado queda invalidado si la clave privada asociada con el certificado ya no existe en el chip IBM Security Chip incorporado del sistema del remitente donde se generó el certificado.	Pida al destinatario que reenvíe su certificado digital; después seleccione ese certificado en la libreta de direcciones de Outlook Express.
Mensaje de anomalía al intentar firmar digitalmente un mensaje de correo electrónico	**Acción**
Si el redactor de un mensaje de correo electrónico intenta firmarlo digitalmente cuando el redactor aún no tiene un certificado asociado con su cuenta de correo electrónico, se muestra un mensaje de error.	Utilice los valores de seguridad en Outlook Express para especificar que se asocie un certificado con la cuenta de usuario. Consulte la documentación proporcionada para Outlook Express para obtener más información.
Outlook Express (128 bits) sólo cifra mensajes de correo electrónico con el algoritmo 3DES	**Acción**
Cuando se envía correo electrónico cifrado entre clientes que utilicen Outlook Express con la versión de 128 bits de Internet Explorer 4.0 ó 5.0, sólo puede utilizarse el algoritmo 3DES.	Para utilizar navegadores de 128 bits con Client Security Software, el chip IBM Security Chip incorporado debe soportar el cifrado de 256 bits. Si el chip IBM Security Chip incorporado soporta el cifrado de 256 bits, debe utilizar un navegador Web de 40 bits. Puede averiguar el nivel de cifrado proporcionado por Client Security Software en Administrator Utility. Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con Outlook Express.

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

Síntoma del problema	Posible solución
Se muestra un mensaje de error al solicitar un certificado	**Acción**
Cuando utiliza Internet Explorer, es posible que reciba un mensaje de error si solicita un certificado que utiliza el CSP del chip IBM Security Chip incorporado.	Solicite el certificado digital de nuevo.

Información de resolución de problemas de Netscape

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

Síntoma del problema	Posible solución
Problemas al leer correo electrónico cifrado	**Acción**
El correo electrónico cifrado no puede descifrarse debido a las diferencias en los niveles de cifrado de los navegadores Web utilizados por el remitente y el destinatario. **Nota:** para utilizar navegadores de 128 bits con Client Security Software, el chip IBM Security Chip incorporado debe soportar el cifrado de 256 bits. Si el chip IBM Security Chip incorporado soporta el cifrado de 256 bits, debe utilizar un navegador Web de 40 bits. Puede averiguar el nivel de cifrado proporcionado por Client Security Software en Administrator Utility.	Compruebe lo siguiente: 1. El nivel de cifrado para el navegador Web que utiliza el remitente es compatible con el nivel de cifrado del navegador Web que utiliza el destinatario. 2. El nivel de cifrado para el navegador Web es compatible con el nivel de cifrado proporcionado por el firmware de Client Security Software.
Mensaje de anomalía al intentar firmar digitalmente un mensaje de correo electrónico	**Acción**
Si no se ha seleccionado el certificado del chip IBM Security Chip incorporado en Netscape Messenger y el redactor de un mensaje de correo electrónico intenta firmar el mensaje con el certificado, se muestra un mensaje de error.	Utilice los valores de seguridad de Netscape Messenger para seleccionar el certificado. Cuando se abra Netscape Messenger, pulse el icono de seguridad en la barra de herramientas. Se abre la ventana Información sobre seguridad. Pulse **Messenger** en el panel izquierdo y después seleccione el **Certificado del chip IBM Security Chip incorporado**. Consulte la documentación proporcionada por Netscape para obtener más información.

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

Síntoma del problema	Posible solución
Se muestra un mensaje de error al intentar utilizar un certificado restaurado después de una anomalía de una unidad de disco duro	**Acción**
Se pueden restaurar los certificados utilizando la característica de restauración de claves en Administrator Utility. Es posible que algunos certificados, como los certificados gratuitos proporcionados por VeriSign, no puedan ser restaurados después de una restauración de claves.	Después de restaurar las claves, obtenga un certificado nuevo.
Se abre el agente de Netscape y produce un error en Netscape	**Acción**
Se abre el agente de Netscape y se cierra Netscape.	Desactive el agente de Netscape.
Netscape se retarda si intenta abrirlo	**Acción**
Si añade el módulo PKCS#11 del chip IBM Security Chip incorporado y después abre Netscape, puede producirse un pequeño retardo antes de que se abra Netscape.	No se precisa ninguna acción. Este mensaje es sólo informativo.

Información de resolución de problemas de certificados digitales

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

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

Información de resolución de problemas de Tivoli Access Manager

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

Síntoma del problema	**Posible solución**
Los valores de política local no se corresponden con los del servidor	**Acción**
Tivoli Access Manager permite ciertas configuraciones de bits que no son soportadas por UVM. En consecuencia, los requisitos de política local pueden prevalecer sobre los valores definidos por un administrador al configurar el servidor Tivoli Access Manager.	Se trata de una limitación conocida.
No se puede acceder a los valores de configuración de Tivoli Access Manager	**Acción**
No se puede acceder a la configuración de Tivoli Access Manager ni a los valores de configuración de la antememoria local en la página Configuración de política en Administrator Utility.	Instale Tivoli Access Manager Runtime Environment. Si no está instalado Runtime Environment en el cliente de IBM, no se podrá acceder a los valores de Tivoli Access Manager en la página Configuración de política.
El control de un usuario es válido tanto para el usuario como para el grupo	**Acción**
Al configurar el servidor Tivoli Access Manager, si define un usuario en un grupo, el control del usuario es válido tanto para el usuario como para el grupo si está activo **Traverse bit** (Bit cruzado).	No se precisa ninguna acción.

Información de resolución de problemas de Lotus Notes

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

Síntoma del problema	**Posible solución**
Después de habilitar la protección de UVM para Lotus Notes, Notes no puede completar su configuración	**Acción**
Lotus Notes no puede completar la configuración después de habilitar la protección de UVM utilizando Administrator Utility.	Se trata de una limitación conocida. Lotus Notes debe estar configurado y en ejecución antes de habilitar el soporte de Lotus Notes en Administrator Utility.
Se muestra un mensaje de error al intentar cambiar la contraseña de Notes	**Acción**
Si se cambia la contraseña de Notes cuando se utiliza Client Security Software se puede mostrar un mensaje de error.	Vuelva a intentar cambiar la contraseña. Si no funciona, reinicie el cliente.

Síntoma del problema	Posible solución
Se muestra un mensaje de error después de generar aleatoriamente una contraseña	**Acción**
Se puede mostrar un mensaje de error cuando hace lo siguiente: • Utiliza la herramienta Configuración de Lotus Notes para establecer la protección de UVM para un ID de Notes • Abre Notes y utiliza la función proporcionada por Notes para cambiar la contraseña para el archivo de ID de Notes • Cierra Notes inmediatamente después de cambiar la contraseña	Pulse **Aceptar** para cerrar el mensaje de error. No se precisa ninguna otra acción. Contrariamente al mensaje de error, la contraseña se ha cambiado. La contraseña nueva es una contraseña generada aleatoriamente creada por Client Security Software. El archivo de ID de Notes está cifrado ahora con la contraseña generada aleatoriamente y el usuario no necesita un archivo de ID de usuario nuevo. Si el usuario final cambia la contraseña de nuevo, UVM generará una nueva contraseña aleatoria para el ID de Notes.

Información de resolución de problemas de cifrado

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

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

Información de resolución de problemas de dispositivos preparados para UVM

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

Síntoma del problema	Posible solución
Un dispositivo preparado para UVM deja de funcionar correctamente	**Acción**
Cuando desconecta un dispositivo preparado para UVM de un puerto USB (Bus serie universal) y después vuelve a conectarlo al puerto USB, es posible que el dispositivo no funcione correctamente.	Reinicie el sistema después de haber vuelto a conectar el dispositivo al puerto USB.

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

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

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

© Copyright IBM Corp. 2002

Apéndice B. Normas para contraseñas y frases de paso

Este apéndice contiene información sobre las normas relacionadas con distintas contraseñas del sistema.

Normas para contraseñas de hardware

Las normas siguientes se aplican a la contraseña de hardware:

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

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

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

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

Normas para frases de paso de UVM

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 IBM Client Security 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 permiten más de dos caracteres repetidos (no)

© Copyright IBM Corp. 2002

Por ejemplo, cuando está establecido, `aaabcdefghijk` 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 que la frase de paso no caduca

  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 no se bloqueará. No hay ningún límite en el número de intentos incorrectos.

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

© Copyright IBM Corp. 2002

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.

Número Pieza: 59P7649

(1P) P/N: 59P7649