Soluciones IBM Client Security

Guía del administrador de Client Security Software Versión 5.1

Soluciones IBM Client Security

Guía del administrador 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 Administrator's 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 65 y el Apéndice D, "**Avisos y marcas registradas**", en la página 71.

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

Contenido

Prefacio vii
A quién va dirigida esta guía viii
Utilización de esta guía viii
Referencias a la *Guía de instalación de Client Security Software* viii
Referencias a *Utilización de Client Security con Tivoli Access Manager* . . . viii
Referencias a la *Guía del usuario de Client Security* viii
Información adicional ix

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. Cifrado de archivos y carpetas 5
Protección de archivos mediante el botón derecho 5
Protección de carpetas mediante el botón derecho 5
Estado de cifrado de las carpetas 5
Consejos sobre el programa de utilidad Cifrado de archivos y carpetas (FFE) 7
Protección en otras letras de unidad 7
Supresión de archivos y carpetas protegidos 7
Antes de actualizar desde una versión anterior del programa de utilidad IBM FFE 7
Antes de desinstalar el programa de utilidad IBM FFE 7
Limitaciones del programa de utilidad Cifrado de archivos y carpetas (FFE) . . . 7
Limitaciones al mover archivos y carpetas protegidos 7
Limitaciones al ejecutar aplicaciones 8
Limitaciones en la longitud de los nombres de vía de acceso 8
Problemas al proteger una carpeta 8

Capítulo 3. Cómo utilizar Client Security Software 9
Ejemplo 1 - Un cliente Windows 2000 y otro Windows XP que utilizan los dos Outlook Express 9
Ejemplo 2 - Dos clientes de IBM con Windows 2000 que utilizan Lotus Notes y el protector de pantalla de Client Security 10
Ejemplo 3 - Varios clientes de IBM con Windows 2000 gestionados por Tivoli Access Manager y que utilizan Netscape para el correo electrónico. 11

Capítulo 4. Autorización de los usuarios 13
Autenticación de usuarios cliente 13
Elementos de autenticación 13
Antes de autorizar usuarios 13
Autorización de los usuarios 14
Eliminación de usuarios 15
Creación de usuarios nuevos 16

Capítulo 5. Después de haber autorizado a los usuarios con UVM 17
Protección de inicio de sesión del sistema operativo de UVM 17
Protección de inicio de sesión del sistema operativo de UVM 17
Configuración de la protección de inicio de sesión del sistema operativo de UVM 18
Registro de las huellas dactilares de los usuarios con UVM 18
Utilización de la protección de UVM para Lotus Notes 19
Habilitación y configuración de la protección de UVM para un ID de usuario de Lotus Notes 19

© Copyright IBM Corp. 2002

Utilización de la protección de UVM dentro de Lotus Notes 19
Inhabilitación de la protección de UVM para un ID de usuario de Lotus Notes 20
Configuración de la protección de UVM para un ID de usuario de Lotus Notes cambiado 21
Utilización de Client Security Software con aplicaciones de Netscape 21
Instalación del módulo PKCS#11 del chip IBM Security Chip incorporado para aplicaciones de Netscape 21
Utilización de la protección de inicio de sesión de PKCS#11 para aplicaciones de Netscape 22
Selección del chip IBM Security Chip incorporado para generar un certificado digital para las aplicaciones de Netscape 22
Actualización del archivador de claves para aplicaciones de Netscape . . . 22
Utilización del certificado digital para aplicaciones de Netscape 22

Capítulo 6. Trabajo con la política de UVM 23
Edición de una política local de UVM. 23
Selección de objetos. 24
Elementos de autenticación 25
Utilización del editor de política de UVM 26
Edición y utilización de la política de UVM para clientes remotos 26

Capítulo 7. Otras funciones para el administrador de seguridad 29
Utilización de Administrator Console 29
Registro de un cliente en una red de itinerancia de credenciales 30
Cambio de la ubicación del archivador de claves 32
Cambio del par de claves del archivador 32
Restauración de las claves desde el archivador. 33
Restablecimiento del contador de errores de autenticación. 34
Cambio de la información de configuración de Tivoli Access Manager. 35
Acceso al archivo de configuración de Tivoli Access Manager 35
Renovación de la antememoria local 35
Recuperación de frases de paso de UVM 35
Cambio de la contraseña del chip IBM Security Chip 36
Consulta de información sobre Client Security Software 37
Inhabilitación del chip IBM Security Chip incorporado. 37
Habilitación del chip IBM Security Chip incorporado y establecimiento de la contraseña del chip de seguridad 37
Habilitación del soporte de Entrust. 38

Capítulo 8. Instrucciones para el usuario cliente 39
Utilización de la protección de UVM para el inicio de sesión del sistema. . . . 39
Desbloqueo del cliente 39
El protector de pantalla de Client Security 40
Configuración del protector de pantalla de Client Security 40
Comportamiento del protector de pantalla de Client Security 40
User Configuration Utility 40
Características de User Configuration Utility 41
Limitaciones de User Configuration Utility en Windows XP 41
Utilización de User Configuration Utility 42
Utilización de correo electrónico y navegación en la Web seguros 42
Utilización de Client Security Software con aplicaciones de Microsoft 43
Obtención de un certificado digital para aplicaciones de Microsoft 43
Transferencia de certificados desde el CSP de Microsoft 43
Actualización del archivador de claves para aplicaciones de Microsoft . . . 44
Utilización del certificado digital para aplicaciones de Microsoft 44
Configuración de las preferencias de sonido de UVM. 44

Capítulo 9. Resolución de problemas 45
Funciones del administrador 45
Establecimiento de una contraseña del administrador (ThinkCentre) 45
Establecimiento de una contraseña del supervisor (ThinkPad) 46
Protección de la contraseña de hardware 47
Borrado de la información del chip IBM Security Chip incorporado (ThinkCentre) 47
Borrado de la información del chip IBM Security Chip incorporado (ThinkPad) 47
Administrator Utility 48
Supresión de usuarios 48
Acceso denegado a objetos seleccionados con el control de Tivoli Access Manager 48
Limitaciones conocidas 49
Utilización de Client Security Software con sistemas operativos Windows 49
Utilización de Client Security Software con aplicaciones de Netscape 49
El certificado del chip IBM Security Chip incorporado y los algoritmos de cifrado 49
Utilización de la protección de UVM para un ID de usuario de Lotus Notes 50
Limitaciones de User Configuration Utility 50
Mensajes de error. 51
Tablas de resolución de problemas 51
Información de resolución de problemas de instalación 51
Información de resolución de problemas de Administrator Utility 52
Información de resolución de problemas de User Configuration Utility. . . . 54
Información de resolución de problemas específicos de ThinkPad 54
Información de resolución de problemas de Microsoft. 55
Información de resolución de problemas de Netscape 58
Información de resolución de problemas de certificados digitales 60
Información de resolución de problemas de Tivoli Access Manager. 61
Información de resolución de problemas de Lotus Notes 61
Información de resolución de problemas de cifrado 62
Información de resolución de problemas de dispositivos preparados para UVM 63

Apéndice A. Normativas de exportación de los EE.UU. para Client Security Software 65

Apéndice B. Normas para contraseñas y frases de paso 67
Normas para contraseñas de hardware 67
Normas para frases de paso de UVM 67

Apéndice C. Normas para la utilización de la protección de UVM para el inicio de sesión del sistema 69

Apéndice D. Avisos y marcas registradas 71
Avisos 71
Marcas registradas 72

Prefacio

Esta guía contiene información sobre la configuración y utilización de las características de seguridad proporcionadas con Client Security Software.

Esta 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, “Cifrado de archivos y carpetas”″ contiene información sobre cómo utilizar IBM Client Security Software para proteger los archivos y carpetas confidenciales.

El ″Capítulo 3, “Cómo utilizar Client Security Software”″ contiene ejemplos sobre cómo utilizar los componentes proporcionados por Client Security Software para configurar las características de seguridad que necesitan los usuarios clientes de IBM.

El ″Capítulo 4, “Autorización de los usuarios”″ contiene información sobre la autenticación de usuarios cliente, incluido cómo autorizar y eliminar usuarios en User Verification Manager (UVM).

El ″Capítulo 5, “Después de haber autorizado a los usuarios con UVM”″ contiene instrucciones informativas sobre cómo configurar la protección de UVM para el inicio de sesión del sistema operativo, cómo utilizar la protección de UVM para Lotus Notes y cómo utilizar Client Security Software con aplicaciones de Netscape.

El ″Capítulo 6, “Trabajo con la política de UVM”″ contiene instrucciones sobre cómo editar una política local de UVM, utilizar la política de UVM para un cliente remoto y cambiar la contraseña para un archivo de políticas de UVM.

El ″Capítulo 7, “Otras funciones para el administrador de seguridad”″ contiene instrucciones sobre cómo utilizar Administrator Utility para cambiar la ubicación del archivador de claves, restaurar las claves desde el archivador, recuperar una frase de paso de UVM y habilitar o inhabilitar el chip IBM Security Chip incorporado.

El ″Capítulo 8, “Instrucciones para el usuario cliente”″ contiene instrucciones sobre las diferentes tareas que efectúa el usuario cliente con Client Security Software. Esta capítulo incluye instrucciones sobre cómo utilizar la protección de inicio de sesión de UVM, el protector de pantalla de Client Security, el correo electrónico seguro y User Configuration Utility.

El ″Capítulo 9, “Resolución de problemas”″ contiene información útil para superar limitaciones y problemas conocidos 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.

© Copyright IBM Corp. 2002

El ″Apéndice C, “**Normas para la utilización de la protección de UVM para el inicio de sesión del sistema**”″ contiene información sobre la utilización de la protección de UVM para el inicio de sesión del sistema operativo.

El ″Apéndice D, “**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 seguridad que vayan a:

- Configurar la autenticación de usuarios para el cliente de IBM
- Configurar y editar la política de seguridad de UVM para los clientes de IBM
- Utilizar Administrator Utility para gestionar el subsistema de seguridad (chip IBM Security Chip incorporado) y los valores asociados para los clientes de IBM

Esta guía también va dirigida a los administradores de Tivoli Access Manager que vayan a utilizar IBM Tivoli Access Manager para gestionar los objetos de autenticación proporcionados en la política de UVM. Los administradores de Tivoli Access Manager deben poder gestionar lo siguiente:

- El espacio de objetos de Tivoli Access Manager
- Los procesos de autenticación, autorización y obtención de credenciales
- IBM Distributed Computing Environment (DCE)
- IBM SecureWay Directory LDAP (Lightweight Directory Access Protocol)

Utilización de esta guía

Utilice esta guía para configurar la autenticación de usuarios y la política de seguridad de UVM para los clientes de IBM. Esta guía acompaña a los manuales *Guía de instalación 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 del sitio Web de IBM en http://www.pc.ibm.com/ww/security/secdownload.html.

Referencias a la *Guía de instalación de Client Security Software*

En este documento se hacen referencias a la *Guía de instalación de Client Security Software*. Debe instalar Client Security Software en un cliente de IBM antes de poder utilizar esta guía. Se proporcionan instrucciones para instalar el software en la *Guía de instalación de Client Security Software*.

Referencias a *Utilización de Client Security con Tivoli Access Manager*

En este documento se hacen referencias a *Utilización de Client Security con Tivoli Access Manager*. Los administradores de seguridad que vayan a utilizar Tivoli Access Manager para gestionar objetos de autenticación para la política de UVM deberían leer *Utilización de Client Security con Tivoli Access Manager*.

Referencias a la *Guía del usuario de Client Security*

En este documento se hacen referencias a la *Guía del usuario de Client Security*. Los administradores pueden utilizar esta guía para configurar y mantener la política de UVM en los clientes de IBM que utilicen Client Security Software. Después de que un administrador haya configurado la autenticación de usuarios y la política de seguridad de UVM, un usuario cliente puede leer la *Guía del usuario de Client Security* para aprender a utilizar Client Security Software.

La Guía del usuario contiene información sobre cómo efectuar tareas de Client Security Software, como la utilización de la protección de inicio de sesión de UVM, la configuración del protector de pantalla de Client Security, 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. Cifrado de archivos y carpetas

El programa de utilidad Cifrado de archivos y carpetas de IBM, que puede bajarse del sitio Web de IBM Client Security, permite a los usuarios de Client Security Software proteger los archivos y carpetas confidenciales utilizando el ratón derecho del ratón. La forma en la que el programa de utilidad protege un archivo y una carpeta difiere en función del modo en el que el archivo o carpeta se cifre inicialmente. Lea la información siguiente para determinar la técnica de cifrado que debería utilizar para proteger sus datos. Debe instalarse Client Security Software *antes* de instalar el programa de utilidad Cifrado de archivos y carpetas de IBM.

Es posible que se ejecute el programa de utilidad de verificación del disco cuando se reinicia el sistema operativo después de proteger o desproteger las carpetas. Espere a que se verifique el sistema antes de utilizar el equipo.

Protección de archivos mediante el botón derecho

Los archivos pueden cifrarse y descifrarse manualmente mediante el menú del botón derecho. Cuando los archivos se cifran de este modo, la operación de cifrado añade una extensión .enc a los archivos. Estos archivos cifrados pueden almacenarse de forma segura en los servidores remotos. Permanecerán cifrados y no estarán disponibles para que los utilicen las aplicaciones hasta que se utilice de nuevo el recurso del botón derecho para descifrarlos.

Protección de carpetas mediante el botón derecho

Un usuario inscrito en UVM puede seleccionar una carpeta para protegerla o desprotegerla mediante la interfaz del botón derecho. Esto cifrará todos los archivos contenidos en la carpeta o todas sus subcarpetas. Cuando se protegen los archivos de este modo, no se añade ninguna extensión al nombre del archivo. Cuando una aplicación intente acceder a un archivo en una carpeta cifrada, el archivo se descifrará en memoria y se volverá a cifrar antes de guardarlo en el disco duro.

Cualquier operación de Windows que intente acceder a un archivo en una carpeta protegida obtendrá acceso a los datos en formato descifrado. Esta característica ofrece facilidad de uso ya que no hay que descifrar un archivo antes de utilizarlo ni volver a cifrarlo después de que un programa haya terminado de utilizarlo.

Estado de cifrado de las carpetas

IBM Client Security Software permite a los usuarios proteger los archivos y carpetas confidenciales utilizando el botón derecho del ratón. La forma en la que el software protege un archivo y una carpeta difiere en función del modo en el que el archivo o carpeta se cifre inicialmente.

Una carpeta puede estar en uno de los estados siguientes; cada estado es gestionado de forma distinta por la opción de protección de carpetas mediante el botón derecho:

- **Una carpeta desprotegida**

  Ni esta carpeta ni sus subcarpeta ni ninguno de sus padres han sido designados como protegidos. Se ofrece al usuario la opción de proteger esta carpeta.
- **Una carpeta protegida**

  Una carpeta protegida puede estar en uno de estos tres estados:

© Copyright IBM Corp. 2002

- **Protegida por el usuario actual**

  El usuario actual ha designado esta carpeta como protegida. Todos los archivos están cifrados, incluidos los archivos de todas las subcarpetas. Se ofrece al usuario la opción de desproteger la carpeta.
- **Una subcarpeta de una carpeta protegida por el usuario actual**

  El usuario actual ha designado uno de los padres de esta carpeta como protegido. Todos los archivos están cifrados. El usuario actual no tiene opciones de botón derecho.
- **Protegida por un usuario diferente**

  Un usuario diferente ha designado esta carpeta como protegida. Todos los archivos están cifrados, incluidos los archivos de todas las subcarpetas y no están disponibles para el usuario actual. El usuario actual no tiene opciones de botón derecho.

• **Un padre de una carpeta protegida**

  Un padre de una carpeta protegida puede estar en uno de estos tres estados:
- **Puede contener una o más subcarpetas protegidas por el usuario actual**

  El usuario actual ha designado una o más subcarpetas como protegidas. Todos los archivos en las subcarpetas protegidas están cifrados. Se ofrece al usuario la opción de proteger la carpeta padre.
- **Puede contener una o más subcarpetas protegidas por uno o más usuarios diferentes**

  Un usuario o usuarios diferentes han designado una o más subcarpetas como protegidas. Todos los archivos en las subcarpetas protegidas están cifrados y no están disponibles para el usuario actual. El usuario actual no tiene opciones de botón derecho.
- **Puede contener subcarpetas protegidas por el usuario actual y uno o más usuarios diferentes**

  Tanto el usuario actual como uno o más usuarios diferentes han designado las subcarpetas como protegidas. El usuario actual no tiene opciones de botón derecho.

• **Una carpeta crítica**

  Una carpeta crítica es una carpeta que está en una vía de acceso crítica y, por lo tanto, no puede protegerse. Hay dos vías de acceso críticas: la vía de acceso de Windows y la de Client Security.

Cada estado es gestionado de forma diferente por la opción de protección de carpetas mediante el botón derecho.

Consejos sobre el programa de utilidad Cifrado de archivos y carpetas (FFE)

La información siguiente podría ser útil a la hora de efectuar ciertas operaciones de cifrado de archivos y carpetas.

Protección en otras letras de unidad

Sólo puede utilizarse el programa de utilidad IBM FFE para cifrar los archivos y carpetas de la unidad C. Este programa de utilidad no soporta el cifrado en ninguna otra partición del disco duro ni unidad física.

Supresión de archivos y carpetas protegidos

Para asegurarse de que no quedan desprotegidos archivos o carpetas delicados en la Papelera de reciclaje, debe utilizar la combinación de teclas Mayús+Supr para suprimir los archivos y carpetas protegidos. La combinación de teclas Mayús+Supr efectúa una operación de supresión incondicional y no intenta poner los archivos suprimidos en la Papelera de reciclaje.

Antes de actualizar desde una versión anterior del programa de utilidad IBM FFE

Si va a actualizar sobre una versión anterior del programa de utilidad IBM FFE (versión 1.04 o anterior) y tiene carpetas protegidas en unidades que no sean la unidad C, desproteja esas carpetas antes de instalar la versión 1.05 del programa de utilidad IBM FFE. Si necesita volver a proteger esas carpetas después de instalar la versión 1.05, debe moverlas antes a la unidad C y después protegerlas.

Antes de desinstalar el programa de utilidad IBM FFE

Antes de desinstalar el programa de utilidad IBM FFE, utilícelo para desproteger todos los archivos o carpetas que estén protegidos actualmente.

Limitaciones del programa de utilidad Cifrado de archivos y carpetas (FFE)

El programa de utilidad IBM FFE tiene las limitaciones siguientes:

Limitaciones al mover archivos y carpetas protegidos

El programa de utilidad IBM FFE no soporta las acciones siguientes:

- El traslado de archivos y carpetas dentro de carpetas protegidas
- El traslado de archivos o carpetas entre carpetas protegidas y desprotegidas

Si intenta efectuar cualquiera de estas operaciones de traslado no soportadas, el sistema operativo mostrará un mensaje de ″Acceso denegado″. Este mensaje es normal. Sólo proporciona la notificación de que esta operación de traslado no está soportada. Como alternativa a la utilización de una operación de traslado, haga lo siguiente:

1. Copie los archivos o carpetas protegidos en la nueva ubicación.
2. Suprima los archivos o carpetas originales utilizando la combinación de teclas Mayús+Supr.

Limitaciones al ejecutar aplicaciones

El programa de utilidad IBM FFE no soporta la ejecución de aplicaciones desde una carpeta protegida. Por ejemplo, si tiene un ejecutable denominado PROGRAMA.EXE, no puede ejecutar esa aplicación desde una carpeta protegida.

Limitaciones en la longitud de los nombres de vía de acceso

Mientras intenta proteger una carpeta utilizando el programa de utilidad IBM FFE o intenta copiar o mover un archivo o carpeta desde una carpeta desprotegida a una protegida, es posible que reciba un mensaje ″Los nombres de una o más vías de acceso son demasiado largos″ del sistema operativo. Si recibe este mensaje, quiere decir que tiene uno o más archivos o carpetas que tienen una vía de acceso que supera la longitud máxima de caracteres permitida. Para corregir el problema, reorganice la estructura de la carpeta para reducir los niveles de profundidad o acorte los nombres de alguna carpeta o archivo.

Problemas al proteger una carpeta

Si intenta proteger una carpeta y recibe un mensaje indicando que "La carpeta no puede protegerse. Puede que haya uno o más archivos en uso", compruebe lo siguiente:

- Compruebe que ninguno de los archivos contenidos en la carpeta está actualmente en uso.
- Si el Explorador de Windows muestra una o más subcarpetas dentro de una carpeta que está intentando proteger, asegúrese de que la carpeta que está intentando proteger está resaltada y activa, y no alguna de las subcarpetas.

Capítulo 3. Cómo utilizar Client Security Software

Los administradores pueden utilizar varios componentes proporcionados por Client Security Software para configurar las características de seguridad que requieren los usuarios clientes de IBM. Utilice los ejemplos siguientes como apoyo para planificar la política y configuración de Client Security. Por ejemplo, los usuarios de Windows NT pueden establecer la protección de UVM para el inicio de sesión del sistema que prohíbe a los usuarios no autorizados el inicio de sesión en el cliente de IBM.

Ejemplo 1 - Un cliente Windows 2000 y otro Windows XP que utilizan los dos Outlook Express

En este ejemplo, un cliente de IBM (cliente 1) tiene instalado Windows 2000 y Outlook Express, el otro cliente (cliente 2) tiene instalado Windows XP y Outlook Express. Hay tres usuarios que necesitarán configurar la autenticación con UVM en el cliente 1; un usuario cliente necesitará configurar la autenticación con UVM en el cliente 2. Todos los usuarios clientes registrarán sus huellas dactilares con objeto de poder utilizarlas en la autenticación. Se instalará un sensor de huellas dactilares preparado para UVM durante este ejemplo. También se ha establecido que los dos clientes necesitarán protección de UVM para iniciar la sesión de Windows. El administrador ha decidido que la política local de UVM se editará y utilizará en cada cliente.

Para configurar la seguridad del cliente, complete el procedimiento siguiente:

1. Instale el software en el cliente 1 y el 2. Consulte la *Guía de instalación de Client Security Software* para obtener detalles.
2. Instale en cada cliente los sensores de huellas dactilares preparados para UVM y los productos de software asociados.

   Para obtener información sobre los productos preparados para UVM, vaya a la página http://www.pc.ibm.com/ww/security/secdownload.html en la World Wide Web.
3. Configure la autenticación de usuarios con UVM para cada cliente. Haga lo siguiente:
   a. Añada usuarios a UVM asignándolos una frase de paso de UVM. Dado que el cliente 1 tiene tres usuarios, debe repetir el proceso para añadir usuarios a UVM hasta que haya añadido todos los usuarios.
   b. Configure la protección de UVM para el inicio de sesión de Windows en cada cliente.
   c. Registre las huellas dactilares de los usuarios. Dado que la política se establecerá indicando que tres usuarios utilizarán el cliente 1, los tres usuarios deben registrar sus huellas dactilares.

      Nota: si establece las huellas dactilares como un requisito de autenticación que forma parte de la política de UVM para un cliente, cada usuario deberá registrar sus huellas dactilares.
4. Edite y guarde una política local de UVM en cada cliente que requiere autenticación para lo siguiente:
   - Iniciar la sesión en el sistema operativo
   - Obtener un certificado digital
   - Utilizar una firma digital para mensajes de correo electrónico

© Copyright IBM Corp. 2002

5. Reinicie cada cliente con objeto de habilitar la protección de UVM para el inicio de sesión de Windows.
6. Informe a los usuarios de las frases de paso de UVM que ha establecido para ellos y de los requisitos de autenticación que ha establecido en la política de UVM para el cliente de IBM.

Los usuarios cliente pueden efectuar ahora las tareas siguientes:

- Utilizar la protección de UVM para bloquear y desbloquear el sistema operativo.
- Solicitar un certificado digital y seleccionar el chip IBM Security Chip incorporado como el suministrador de servicio criptográfico asociado al certificado.
- Utilizar el certificado digital para cifrar mensajes de correo electrónico creados con Outlook Express.

Ejemplo 2 - Dos clientes de IBM con Windows 2000 que utilizan Lotus Notes y el protector de pantalla de Client Security

En este ejemplo, los dos clientes de IBM (cliente 1 y 2) tienen los dos instalado Windows 2000 y Lotus Notes. Dos usuarios requerirán establecer la autenticación con UVM en el cliente 1; un usuario requerirá establecer la autenticación con UVM en el cliente 2. Los dos clientes requerirán la protección de UVM para el inicio de sesión del sistema y utilizarán el protector de pantalla de Client Security y la protección de UVM para Lotus Notes. El administrador ha decidido que se editará en el cliente 1 una política de UVM para clientes remotos y luego se copiará en el cliente 2.

Para configurar la seguridad del cliente, complete el procedimiento siguiente:

1. Instale el software en el cliente 1 y el 2. Dado que se utilizará una política de UVM para clientes remotos, deberá utilizar la misma clave pública del administrador cuando instale el software en los dos clientes, el 1 y el 2. Lea el manual *Guía de instalación de Client Security Software* para obtener detalles sobre la instalación del software.
2. Configure la autenticación de usuarios con UVM para cada cliente. A continuación, efectúe lo siguiente:
   a. Añada usuarios a UVM asignándolos una frase de paso de UVM. Dado que el cliente 1 tiene dos usuarios, debe repetir el proceso para añadir usuarios a UVM hasta que haya añadido los dos usuarios.
   b. Configure la protección de UVM para el inicio de sesión de Windows en cada cliente.
3. Habilite la protección de UVM para Lotus Notes en los dos clientes. Para obtener más información, consulte “Utilización de la protección de UVM para Lotus Notes” en la página 19.
4. Edite y guarde una política de UVM para clientes remotos en el cliente 1 y, a continuación, cópiela en el cliente 2. La política de UVM requerirá la autenticación del usuario para borrar el protector de pantalla e iniciar la sesión de Lotus Notes y el sistema operativo. Para obtener más detalles, consulte “Edición y utilización de la política de UVM para clientes remotos” en la página 26.
5. Reinicie cada cliente con objeto de habilitar la protección de UVM para el inicio de sesión del sistema.
6. Informe a los usuarios cliente de las frases de paso de UVM y de la política que se ha establecido para cada cliente.

Los usuarios pueden leer ahora el manual *Guía del usuario de Client Security Software* para aprender a efectuar las tareas siguientes:

- Habilitar el protector de pantalla de Client Security
- Utilizar la protección de UVM para Windows 2000

Ejemplo 3 - Varios clientes de IBM con Windows 2000 gestionados por Tivoli Access Manager y que utilizan Netscape para el correo electrónico

El ejemplo siguiente va dirigido a administradores corporativos que tienen planificado utilizar Tivoli Access Manager para gestionar los objetos de autenticación establecidos por la política de UVM. En este ejemplo, varios clientes de IBM tienen instalado Windows 2000 y Netscape. Todos los clientes disponen de un cliente NetSEAT instalado, un componente de Tivoli Access Manager. Todos los clientes que utilizan un servidor LDAP tienen instalado el cliente LDAP. Se instalará en todos los clientes la política de UVM para clientes remotos. La política de UVM habilitará Tivoli Access Manager para controlar los objetos de autenticación seleccionados para los clientes.

En este ejemplo, un usuario requerirá la configuración de autenticación con UVM en cada cliente. Todos los usuarios registrarán sus huellas dactilares para que se puedan utilizar en la autenticación. Se instalará durante este ejemplo un sensor de huellas dactilares preparado para UVM y todos los clientes necesitarán protección de UVM para el inicio de sesión de Windows.

Para configurar la seguridad del cliente, complete el procedimiento siguiente:

1. Instale el componente Client Security en el servidor Tivoli Access Manager. Para obtener detalles, consulte el manual *Utilización de Client Security con Tivoli Access Manager*.
2. Instale Client Security Software en todos los clientes. Dado que se utilizará una política de UVM para clientes remotos, deberá utilizar la misma clave pública del administrador cuando instale el software en todos los clientes. Lea el manual *Guía de instalación de Client Security Software* para obtener detalles sobre la instalación del software.
3. Instale en cada cliente los sensores de huellas dactilares preparados para UVM y los productos de software asociados. Para obtener información sobre los productos preparados para UVM disponibles, vaya a la página http://www.pc.ibm.com/ww/security/secdownload.html en la World Wide Web.
4. Configure la autenticación de usuarios con UVM en cada cliente. Consulte “Eliminación de usuarios” en la página 15 para obtener detalles. A continuación, efectúe lo siguiente:
   a. Añada usuarios a UVM asignándolos una frase de paso de UVM.
   b. Configure la protección de UVM para el inicio de sesión de Windows en cada cliente.
   c. Registre las huellas dactilares para cada usuario cliente. Si es necesaria la autenticación en clientes de IBM, todos los usuarios de ese cliente deberán registrar sus huellas dactilares.
5. Configure la información de configuración de Tivoli Access Manager en cada cliente. Para obtener detalles, consulte el manual *Utilización de Client Security con Tivoli Access Manager*.

6. Edite y guarde una política de UVM para clientes remotos en uno de los clientes y a continuación cópiela en los otros clientes. Establezca la política de UVM de modo que Tivoli Access Manager pueda controlar los objetos de autenticación siguientes:
   - Iniciar la sesión en el sistema operativo
   - Obtener un certificado digital
   - Utilizar una firma digital para mensajes de correo electrónico

   Para obtener más detalles, consulte “Edición y utilización de la política de UVM para clientes remotos” en la página 26.
7. Reinicie cada cliente con objeto de habilitar la protección de UVM para el inicio de sesión de Windows.
8. Instale el módulo PKCS#11 del chip IBM Security Chip incorporado en cada cliente. Este módulo proporciona soporte criptográfico en clientes que utilizan Netscape para enviar y recibir mensajes de correo electrónico y el chip IBM Security Chip incorporado para obtener certificados digitales. Para obtener más información, consulte la *Guía de instalación de Client Security Software*.
9. Habilite Tivoli Access Manager para controlar los objetos de IBM Client Security Software que aparecen en Tivoli Access Manager Management Console.
10. Informe a los usuarios cliente de las frases de paso de UVM que se han establecido y de la política que se ha establecido para cada cliente.
11. Sugiera a los usuarios que lean el manual *Guía del usuario de Client Security Software* para aprender a efectuar las tareas siguientes:
    - Utilizar la protección de UVM para bloquear y desbloquear el sistema operativo
    - Utilizar User Configuration Utility
    - Solicitar un certificado digital que utiliza el chip IBM Security Chip incorporado como el suministrador de servicio criptográfico asociado al certificado
    - Utilizar el certificado digital para cifrar mensajes de correo electrónico creados con Netscape

Capítulo 4. Autorización de los usuarios

La información siguiente es útil a la ahora de autorizar usuarios de Windows para que utilicen User Verification Manager (UVM).

Autenticación de usuarios cliente

La autenticación de los usuarios finales en el nivel del cliente es una cuestión importante de la seguridad del sistema. 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.

La política de seguridad de UVM para un cliente de IBM puede gestionarse de dos formas:

- Localmente, utilizando un editor de política que esté en el cliente de IBM
- En toda una corporación, utilizando Tivoli Access Manager

Cuando añade el primer usuario, se generan claves de cifrado de hardware.

Elementos de autenticación

Los elementos de autenticación (como las frases de paso de UVM o las huellas dactilares del usuario) se utilizan para autorizar a los usuarios en el cliente de IBM. Cuando autoriza a un usuario de Windows para utilizar UVM, asigna una frase de paso de UVM para el usuario cliente. La frase de paso de UVM, que puede tener hasta 256 caracteres de longitud, es el elemento principal de la autenticación que se utiliza en UVM. Cuando asigna una frase de paso de UVM, se crean las claves de cifrado para ese usuario cliente y se almacenan en un archivo que gestiona el chip IBM Security Chip incorporado. Si el cliente de IBM utiliza para la autenticación un dispositivo preparado para UVM, debe registrarse también con UVM el elemento de autenticación, por ejemplo, las huellas dactilares del usuario.

Durante la configuración de la autenticación del usuario, puede seleccionar las siguientes características de seguridad que se proporcionan en Client Security Software:

- **Protección de UVM para el inicio de sesión del sistema operativo.** La protección de UVM asegura que sólo los usuarios reconocidos por UVM pueden acceder al sistema. Antes de habilitar la protección de UVM para el inicio de sesión del sistema, consulte Configuración de la protección de inicio de sesión del sistema operativo de UVM para obtener información importante.
- **Protector de pantalla de Client Security.** Después de añadir usuarios cliente, el usuario puede configurar y utilizar el protector de pantalla de Client Security. El protector de pantalla de Client Security se configura mediante la opción Pantalla en el software del sistema operativo.

Antes de autorizar usuarios

Importante: autorice únicamente cuentas de usuario que puedan utilizarse para iniciar una sesión en el sistema operativo. Si se autoriza una cuenta de usuario que *no se puede* utilizar para iniciar la sesión en el sistema operativo, se bloquearán **todos** los usuarios del sistema cuando se habilite la protección de inicio de sesión de UVM.

© Copyright IBM Corp. 2002

Cuando autoriza un usuario cliente, Administrator Utility le proporciona una lista de nombres de usuario que puede seleccionar. Los nombres de esa lista son las cuentas de usuario que se han añadido mediante el sistema operativo. Antes de añadir usuarios cliente a UVM, utilice el software del sistema operativo para crear para esos usuarios cuentas y perfiles de usuario. Client Security Software funciona junto con las características de seguridad que proporciona el sistema operativo.

Windows XP y Windows 2000.

Utilice el programa Usuarios y contraseñas para crear nuevas cuentas de usuario y gestionar cuentas de usuario o grupos. Consulte la documentación del sistema operativo para obtener más información.

En Windows XP, no se renueva el campo Seleccionar usuarios de Windows para autorizarlos cuando pulsa el botón **Crear nuevos usuarios de Windows**. Debe salir y reiniciar Administrator Utility para renovar este campo.

Notas:

1. Cuando utiliza el software del sistema operativo para crear usuarios nuevos, la contraseña de dominio de cada usuario nuevo debe ser la misma.
2. No autorice un usuario que tuviera antes un nombre de usuario de Windows cambiado. UVM señalará al nombre de usuario anterior mientras que Windows sólo reconocerá el nombre de usuario nuevo.
3. Cuando se suprime de Windows una cuenta de usuario que se había autorizado, la interfaz de protección de inicio de sesión de UVM sigue listando incorrectamente la cuenta como si se pudiera utilizar para iniciar la sesión en Windows. Esta cuenta *no se puede* utilizar para iniciar la sesión en Windows.
4. Después de haber autorizado un usuario, no modifique su nombre de usuario de Windows. Si lo hace, tendrá que volver a autorizar el nombre de usuario nuevo en UVM y solicitar todas las credenciales nuevas.

Autorización de los usuarios

Los usuarios deben iniciar una sesión con derechos de administrador para utilizar Administrator Utility.

Para autorizar usuarios con UVM, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se muestra el mensaje Entre la contraseña del administrador.
2. Escriba la contraseña del administrador y pulse **Aceptar**.

   Se abrirá la ventana principal de IBM Security Subsystem Administrator Utility.
3. En el área Seleccionar usuarios de Windows para autorizarlos, seleccione un nombre de usuario en la lista.

   Nota: los nombres de usuario de la lista se definen en las cuentas de usuario creadas en el sistema operativo o la red.
4. Pulse **Autorizar**.

   Se muestra la pantalla Configuración de autenticación del usuario.
5. Entre y confirme una frase de paso inicial de User Verification Manager para el usuario recién autorizado y pulse **Siguiente**.

   Si la frase de paso no cumple los requisitos de la política de seguridad, se muestra una pantalla indicando que la frase de paso entrada no es válida. Si

ocurre esto, pulse **Aceptar** y después pulse **Ver requisitos de la frase de paso** para ver los parámetros que debe cumplir una frase de paso válida.

Cuando se acepte la frase de paso, aparecerá un mensaje indicando que la operación se ha completado satisfactoriamente.

6. Pulse **Aceptar** para continuar.

   Se muestra la pantalla Contraseña de inicio de sesión de Windows. Si está habilitado el inicio de sesión seguro de UVM, la contraseña actual de Windows del usuario debe almacenarse para que el usuario pueda iniciar una sesión en el sistema. Esta pantalla permite al administrador efectuar una de estas acciones:

   - **Almacenar ahora la contraseña actual de Windows del usuario.** Para almacenar ahora la contraseña actual de Windows del usuario, entre y confirme la contraseña del usuario en los campos proporcionados y pulse **Siguiente**.

     Nota: la contraseña entrada aquí debe coincidir con la contraseña actual de Windows del usuario. Este valor no afecta a la contraseña almacenada con el sistema operativo.

   - **Hacer que el usuario almacene la contraseña de Windows más tarde utilizando User Configuration Utility.** Para hacer que el usuario almacene su contraseña de Windows más tarde utilizando User Configuration Utility, seleccione el botón de selección adecuado y pulse **Siguiente**.

   Aparecerá un mensaje que indica que la operación se ha completado satisfactoriamente.

7. Pulse **Finalizar**.

Eliminación de usuarios

Los usuarios deben iniciar una sesión con derechos de administrador para utilizar Administrator Utility.

Para desautorizar usuarios con UVM, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se muestra el mensaje Entre la contraseña del administrador.

2. Escriba la contraseña del administrador y pulse **Aceptar**.

   Se abrirá la ventana principal de IBM Security Subsystem Administrator Utility.

3. En el área Usuarios de Windows autorizados para usar UVM, seleccione un nombre de usuario en la lista.
4. Pulse **Eliminar usuario**.

   Se muestra un mensaje advirtiendo que se perderá la información de seguridad del usuario seleccionado, incluidas todas las claves existentes, certificados, huellas dactilares registradas y contraseñas almacenadas del usuario.

5. Pulse **Sí** para continuar.

   Se muestra un mensaje preguntando si desea eliminar la información archivada del usuario. Si elimina esta información el usuario no podrá restaurar ninguno de los valores guardados previamente en cualquier sistema.

6. Pulse **Sí** para completar la operación.

Creación de usuarios nuevos

Los usuarios deben iniciar una sesión con derechos de administrador para utilizar Administrator Utility.

Para crear usuarios nuevos, utilice el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se muestra el mensaje Entre la contraseña del administrador.
2. Escriba la contraseña del administrador y pulse **Aceptar**.

   Se abrirá la ventana principal de IBM Security Subsystem Administrator Utility.
3. En el área Seleccionar usuarios de Windows para autorizarlos, pulse **Crear nuevos usuarios de Windows**.

   Se muestra la pantalla Cuentas de usuario de Windows.
4. Pulse **Crear una cuenta nueva**.
5. Dé un nombre a la cuenta nueva escribiendo un nombre en el campo proporcionado; después pulse **Siguiente**.
6. Elija un tipo de cuenta seleccionando el botón de selección adecuado.
7. Pulse **Crear cuenta**.
8. Vuelva a IBM Client Security Subsystem Administrator Utility.

   La cuenta de usuario nueva se muestra en el área Seleccionar usuarios de Windows para autorizarlos.

Capítulo 5. Después de haber autorizado a los usuarios con UVM

Después de haber autorizado a los usuarios, se pueden utilizar funciones adicionales de Client Security, como las siguientes:

- **Configuración de la protección de UVM para el inicio de sesión del sistema operativo.** Consulte “Protección de inicio de sesión del sistema operativo de UVM” para obtener más información.
- **Archivo de claves de cifrado de usuarios.** Consulte “Cambio de la ubicación del archivador de claves” en la página 32 para obtener más información.
- **Configuración del protector de pantalla de Client Security.** Consulte el Capítulo 8, “Instrucciones para el usuario cliente”, en la página 39 para obtener más información.
- **Registro de las huellas dactilares de los usuarios con UVM.** Consulte “Registro de las huellas dactilares de los usuarios con UVM” en la página 18 para obtener más información.

  Si ha instalado un sensor de huellas dactilares preparado para UVM antes de añadir usuarios a UVM, se puede efectuar en ese momento el registro de huella dactilar.

Protección de inicio de sesión del sistema operativo de UVM

La protección del inicio de sesión del sistema de UVM amplía la característica de contraseña proporcionada con el sistema operativo. La interfaz de inicio de sesión de UVM sustituye al inicio de sesión del sistema operativo, de modo que la ventana de inicio de sesión de UVM se abre cada vez que un usuario intenta iniciar una sesión en el sistema.

Protección de inicio de sesión del sistema operativo de UVM

Lea la información siguientes antes de establecer y utilizar la protección de UVM para el inicio del sesión del sistema:

- Si la política de UVM indica que es necesaria la autenticación de huellas dactilares para el inicio de sesión del sistema y el usuario no tiene registradas las huellas dactilares, deberá registrarlas para iniciar la sesión.

  Además, si no se ha registrado la contraseña de Windows (o se ha registrado de forma incorrecta) con UVM, el usuario deberá proporcionar la contraseña de Windows correcta para iniciar la sesión.
- No borre la información del chip IBM Security Chip incorporado mientras esté habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema. Para obtener más información, consulte “Funciones del administrador” en el Capítulo 9, “Resolución de problemas”, en la página 45.
- Si quita la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM** en Administrator Utility, el sistema vuelve al proceso de inicio de sesión de Windows sin utilizar la protección de inicio de sesión de UVM.
- Si sustituye el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM y habilita la función LEAP de Cisco, debe reinstalar Cisco Aironet Client Utility (ACU).

© Copyright IBM Corp. 2002

Configuración de la protección de inicio de sesión del sistema operativo de UVM

Para configurar la protección de UVM para el sistema operativo, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se abrirá la ventana principal de Administrator Utility.
2. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
3. Pulse el recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**.
4. Pulse **Aceptar**.
5. Reinicie el sistema.

Cuando se reinicia el sistema, se le solicitará que inicie la sesión del sistema. Para obtener más información sobre la protección de UVM, consulte “Protección de inicio de sesión del sistema operativo de UVM” en la página 17.

Registro de las huellas dactilares de los usuarios con UVM

Cuando se ha editado una política de UVM para incluir autenticación de huellas dactilares, todos los usuarios deberán registrar sus huellas dactilares con UVM.

Nota: Windows XP no ofrece soporte a sensores de huellas dactilares DigitalPersona U.are.U Pro.

Para registrar huellas dactilares de usuario con UVM, complete el procedimiento de Administrator Utility siguiente:

1. En el área Usuarios de Windows autorizados para usar UVM, seleccione un nombre de usuario en la lista.
2. Pulse **Editar usuario**.

   Se muestra la ventana Modificar la configuración de claves de Client Security-Editar los atributos del usuario de UVM.
3. Seleccione el recuadro de selección **Registrar con dispositivo preparado para UVM** y pulse **Siguiente**.

   Se muestra la ventana Modificar la configuración de claves de Client Security-Dispositivos de UVM habilitados.
4. Pulse **Registrar huellas dactilares del usuario**.
5. En el área Seleccionar una mano, pulse **Izquierda** o **Derecha**.
6. En el área Seleccionar un dedo, pulse para seleccionar el dedo del que va a explorar la huella y a continuación pulse **Iniciar registro**.
7. Sitúe el dedo en un sensor de huellas dactilares preparado para UVM y siga las instrucciones que aparecen en pantalla.

   En función del modelo de escáner, es posible que necesite explorar cada huella dactilar cuatro veces. Pulse **Cancelar este dedo** para cancelar la exploración de huellas dactilares.
8. Especifique otro dedo para registrarlo o, pulse **Salir** para finalizar.

Utilización de la protección de UVM para Lotus Notes

UVM proporciona protección de seguridad ampliada para los usuarios de Lotus Notes.

Habilitación y configuración de la protección de UVM para un ID de usuario de Lotus Notes

Antes de poder habilitar la protección de UVM para Lotus Notes, debe instalar Notes en el cliente de IBM, establecer un ID de usuario y una contraseña de Notes y debe autorizarse al usuario de Notes para utilizar UVM.

Para configurar la protección de UVM para Lotus Notes, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se abrirá la ventana principal de Administrator Utility.
2. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
3. Pulse el recuadro de selección **Habilitar soporte de Lotus Notes**.

   Ahora está habilitada la protección de UVM para el ID de usuario de Lotus Notes. Si es necesario continúe con los pasos opcionales siguientes para configurar la política de inicio de sesión de Lotus Notes.
4. Pulse **Política de aplicaciones**.

   Se mostrará la pantalla Modificar la configuración de políticas de Client Security.
5. Pulse **Editar política**.
6. Entre la contraseña del administrador y pulse **Aceptar**. Se muestra la pantalla Política de IBM UVM: Inicio de sesión de Lotus Notes.
7. En la pestaña Selección de objetos, seleccione Inicio de sesión de Lotus Notes en el menú desplegable Acción.
8. En la pestaña Elementos de autenticación, seleccione los elementos de autenticación que desee que se soliciten para el Inicio de sesión de Lotus Notes.
9. Pulse **Aplicar** para guardar las selecciones.

   Se muestra la pantalla Clave privada del administrador necesaria.
10. 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.
11. Pulse **Aceptar**.

    La pantalla IBM User Verification Manager: Resumen de políticas muestra un resumen de los objetos controlados por la política local del cliente.
12. Inicie Lotus Notes.

    El registro de contraseña de UVM estará completo cuando se inicia Lotus Notes.

Utilización de la protección de UVM dentro de Lotus Notes

Antes de poder utilizar la protección de UVM para Lotus Notes, debe seguir los pasos en “Configuración de la protección de UVM dentro de Lotus Notes” en la página 20.

Configuración de la protección de UVM dentro de Lotus Notes

Para configurar la protección de UVM en Lotus Notes, efectúe lo siguiente:

1. Inicie una sesión de Lotus Notes.

   Se mostrará la ventana IBM User Verification Manager.
2. Entre y verifique la contraseña de Lotus Notes en los campos disponibles.

   Ahora la contraseña de Lotus Notes se ha registrado con UVM.

Restablecimiento de la contraseña de Lotus Notes

Para restablecer la contraseña de Lotus Notes, efectúe lo siguiente:

1. Inicie una sesión de Lotus Notes.
2. En la barra de menús de Lotus Notes, pulse **Archivo > Herramientas > ID de usuario**.

   Se mostrará la ventana IBM User Verification Manager.
3. Entre la frase de paso de UVM y pulse **Aceptar**.

   Se mostrará la ventana ID de usuario.
4. Pulse **Establecer contraseña**.

   Se mostrará la ventana IBM User Verification Manager.
5. Pulse el botón de selección **Crear su propia contraseña**.
6. Entre y verifique la nueva contraseña de Lotus Notes en los campos disponibles y pulse **Aceptar**.

Nota: cuando cambia la contraseña en Lotus Notes con un valor que ha utilizado antes, Notes rechaza el cambio de contraseña, pero no informa a Client Security Software. Como consecuencia, UVM almacena la contraseña que Notes ha rechazado.

Si recibe un mensaje que indica que se ha utilizado la contraseña antes cuando cambia la contraseña en Lotus Notes, tendrá que salir de Lotus Notes, iniciar User Configuration Utility y restaurar la contraseña de Lotus Notes con el valor que tenía antes.

Si la contraseña de Lotus Notes se ha generado aleatoriamente y recibe este error, no hay forma de saber qué contraseña era y, por lo tanto, no puede restablecerla manualmente. Deberá solicitar un nuevo archivo de identificadores al administrador o restaurar una copia previamente guardada del archivo de identificadores.

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

Si desea inhabilitar la protección de UVM para un ID de usuario de Lotus Notes, efectúe lo siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Después de que entre su contraseña, se mostrará la ventana principal de Administrator Utility.
2. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
3. Quite la selección del recuadro de selección **Habilitar soporte de Lotus Notes**.
4. Pulse **Aceptar**.

Se mostrará la pantalla Acciones de soporte de aplicaciones con un mensaje que indica que está habilitado el soporte de Lotus Notes.

Configuración de la protección de UVM para un ID de usuario de Lotus Notes cambiado

Para cambiar de un ID de usuario que tenga habilitada la protección de UVM a otro ID de usuario, haga lo siguiente:

1. Salga de Lotus Notes.
2. Inhabilite la protección de UVM para el ID de usuario actual. Consulte “Inhabilitación de la protección de UVM para un ID de usuario de Lotus Notes” en la página 20 para obtener detalles.
3. Entre en Lotus Notes y cambie el ID de usuario. Consulte la documentación de Lotus Notes para obtener información sobre el cambio de ID de usuario.
4. Para configurar la protección de UVM para el ID de usuario al que ha cambiado, entre en la herramienta Configuración de Lotus Notes (proporcionada por Client Security Software) y configure la protección de UVM. Consulte “Utilización de la protección de UVM dentro de Lotus Notes” en la página 19.

Utilización de Client Security Software con aplicaciones de Netscape

Las instrucciones proporcionadas en esta sección son específicas para el uso de Client Security Software en lo que se refiere generalmente a la obtención y utilización de certificados digitales con aplicaciones que soporten PKCS#11, específicamente aplicaciones de Netscape.

Para obtener detalles sobre cómo utilizar los valores de seguridad para aplicaciones de Netscape, consulte la documentación proporcionada con Netscape. IBM Client Security Software sólo soporta Netscape Versión 4.7x.

Nota: para utilizar navegadores de 128 bits con Client Security Software, el chip IBM Security Chip incorporado debe soportar el cifrado de 256 bits. El nivel de cifrado proporcionado por Client Security Software se encuentra en Administrator Utility al pulsar el botón **Valores del chip**.

Instalación del módulo PKCS#11 del chip IBM Security Chip incorporado para aplicaciones de Netscape

Antes de poder utilizar un certificado digital, debe instalar el módulo PKCS#11 del chip IBM Security Chip incorporado en el sistema. Dado que la instalación de dicho módulo requiere una frase de paso de UVM, debe añadir al menos un usuario a la política de seguridad del sistema.

Para instalar el módulo PKCS#11 del chip IBM Security Chip incorporado, complete los pasos siguientes:

1. Abra Netscape y pulse **Archivo > Abrir página**.
2. Localice el archivo de instalación IBMPKCSINSTALL.HTML.

   Si aceptó el directorio por omisión cuando instaló el software, el archivo se encuentra en C:\Archivos de programa\IBM\Security.
3. Abra el archivo de instalación IBMPKCSINSTALL.HTML en Netscape.

   Cuando abra el archivo en Netscape, la secuencia de instalación comienza y se abre la ventana Frase de paso de UVM.
4. Escriba la frase de paso de UVM y pulse **Aceptar**.

Se muestra un mensaje preguntando si está seguro de que desea instalar este módulo de seguridad.

5. Pulse **Aceptar**.

   Se mostrará un mensaje que notifica que el módulo se ha instalado.

6. Pulse **Aceptar**.

Utilización de la protección de inicio de sesión de PKCS#11 para aplicaciones de Netscape

Cuando se ha establecido en el sistema la protección de inicio de sesión de PKCS#11, debe cumplir los requisitos de autenticación cada vez que inicia la sesión en Netscape. Es posible que tenga que escribir la frase de paso de UVM, explorar sus huellas dactilares o hacer ambas cosas para cumplir los requisitos de autenticación. Los requisitos de autenticación están definidos en la política de UVM para el sistema.

Selección del chip IBM Security Chip incorporado para generar un certificado digital para las aplicaciones de Netscape

Durante la creación de certificados digitales, se le solicitará que seleccione la tarjeta o la base de datos donde desea generar la clave, seleccione **IBM embedded Security Subsystem**.

Para obtener más información sobre cómo generar certificados digitales y utilizarlos con Netscape, consulte la documentación proporcionada con Netscape.

Actualización del archivador de claves para aplicaciones de Netscape

Después de crear un certificado digital, efectúe una copia de seguridad del certificado mediante la actualización del archivador de claves. Puede actualizar el archivador de claves utilizando User Configuration Utility.

Utilización del certificado digital para aplicaciones de Netscape

Utilice los valores de seguridad de las aplicaciones de Netscape para ver, seleccionar y utilizar certificados digitales. Por ejemplo, en los valores de seguridad de Netscape Messenger, debe seleccionar el certificado antes de poder utilizarlo para firmar digitalmente o cifrar mensajes de correo electrónico. Consulte la documentación proporcionada por Netscape para obtener más información.

Después de haber instalado el módulo PKCS#11 del chip IBM Security Chip incorporado, UVM le solicitará los requisitos de autenticación cada vez que utilice el certificado digital. Es posible que tenga que escribir la frase de paso de UVM, explorar sus huellas dactilares o hacer ambas cosas para cumplir los requisitos de autenticación. Los requisitos de autenticación están definidos en la política de UVM para el sistema.

Si no cumple los requisitos de autenticación establecidos mediante la política de UVM, se mostrará un mensaje de error. Cuando pulse **Aceptar** en este mensaje, se abrirá Netscape, pero no podrá utilizar el certificado digital generado por el chip IBM Security Chip incorporado hasta que no reinicie Netscape y proporcione la frase de paso de UVM o las huellas dactilares correctas o ambas cosas.

Capítulo 6. Trabajo con la política de UVM

Antes de intentar editar la política de UVM para el cliente local, asegúrese de que hay al menos un usuario autorizado para utilizar UVM. De lo contrario, se mostrará un mensaje de error cuando el editor de política intente abrir el archivo de políticas locales.

Después de haber autorizado a los usuarios para utilizar UVM, debe editar y guardar una política de seguridad para cada cliente de IBM. La política de seguridad proporcionada por Client Security Software se llama política de UVM, que combina los valores proporcionados en "Autorización de los usuarios" con los requisitos de autenticación de clientes. La política de UVM puede utilizarse para controlar la política de seguridad de un cliente local o puede copiarse a clientes remotos a través de una red.

El programa Administrator Utility tiene un editor de política de UVM incorporado que puede utilizar para editar y guardar políticas de UVM para un cliente local. Las tareas realizadas en el cliente de IBM, como iniciar la sesión en el sistema operativo o quitar el protector de pantalla, se llaman objetos de autenticación y estos objetos tienen asignados requisitos de autenticación dentro de la política de UVM. Por ejemplo, puede establecer la política de UVM para que requiera lo que se detalla a continuación:

- Todos los usuarios deben escribir una frase de paso de UVM y utilizar una autenticación de tarjeta de identificación por contacto para iniciar la sesión en el sistema operativo.
- Todos los usuarios deben escribir una frase de paso de UVM cada vez que se obtiene un certificado digital.

También puede utilizar Tivoli Access Manager para controlar objetos de autenticación específicos tal como está establecido en la política de UVM.

La política de UVM establece los requisitos de objetos de autenticación para el cliente de IBM, no para el usuario individual. Por lo tanto, si establece que la política de UVM requiera la autenticación de huellas dactilares para un objeto (como el inicio de sesión del sistema operativo), cada usuario que se autorice para utilizar UVM debe registrar una huella dactilar para utilizar ese objeto. Para obtener detalles, consulte "Eliminación de usuarios" en la página 15.

La política de UVM se guarda en un archivo llamado `globalpolicy.gvm`. Para utilizar UVM en clientes remotos, debe guardarse la política de UVM en un cliente de IBM y a continuación copiarse en clientes remotos. La copia del archivo de política de UVM en los clientes remotos puede ahorrarle tiempo en la configuración de la política de UVM en los clientes remotos.

Edición de una política local de UVM

Cuando se edita la política local de UVM sólo se utiliza en el cliente para el que se ha editado. Si ha instalado Client Security en su ubicación por omisión, la política local de UVM está almacenada como \Archivos de programa\IBM\Security\UVM_Policy\globalpolicy.gvm. Utilice el editor de política de UVM para editar y guardar políticas locales de UVM. Sólo los usuarios que se hayan añadido a UVM pueden utilizar el editor de política de UVM. Se proporciona en Administrator Utility la interfaz del editor de política de UVM.

© Copyright IBM Corp. 2002

Cuando guarda cambios en la política de UVM, se muestra un mensaje que le solicita la clave privada del administrador. Escriba la clave privada del administrador y pulse **Aceptar** para guardar los cambios. Si proporciona una clave privada del administrador incorrecta, no se guardarán los cambios.

La autenticación se produce basándose en la selección que ha efectuado en el editor de política. Por ejemplo, si selecciona “No se necesita una frase de paso después de 1ª vez usada así” para el inicio de sesión de Lotus Notes, entonces siempre que inicie la sesión en Lotus Notes se le solicitará la autenticación de UVM. Cada vez que accede a Lotus Notes después de eso, hasta que rearranca o finaliza la sesión, no es necesaria la frase de paso.

Cuando establece que la política de UVM requiera huellas dactilares para objetos de autenticación (como el inicio de sesión del sistema operativo), los usuarios que se añadan a UVM deben tener registradas sus huellas dactilares para utilizar ese objeto.

Mientras edita la política de UVM, puede ver información sobre el resumen de políticas pulsando Resumen de políticas de UVM. Además, puede pulsar **Aplicar** para guardar los cambios. Cuando pulsa **Aplicar**, se muestra un mensaje que le solicita la clave privada del administrador. Escriba la clave privada del administrador y pulse **Aceptar** para guardar los cambios. Si proporciona una clave privada del administrador incorrecta, no se guardarán los cambios.

Selección de objetos

Los objetos de la política de UVM permiten establecer distintas políticas de seguridad para las diversas acciones de usuario. Los objetos de UVM válidos están especificados en la pestaña **Selección de objetos** de la pantalla Política de IBM UVM en Administrator Utility.

Los objetos de política de UVM válidos incluyen los siguientes:

Inicio de sesión del sistema
Este objeto controla los requisitos de autenticación necesarios para iniciar una sesión en el sistema.

Desbloqueo del sistema
Este objeto controla los requisitos de autenticación necesarios para quitar el protector de pantalla de Client Security.

Inicio de sesión de Lotus Notes
Este objeto controla los requisitos de autenticación necesarios para iniciar una sesión en Lotus Notes.

Cambio de contraseña de Lotus Notes
Este objeto controla los requisitos de autenticación necesarios para utilizar UVM para generar una contraseña aleatoria de Lotus Notes.

Firma digital (correo electrónico)
Este objeto controla los requisitos de autenticación necesarios cuando se pulsa el botón Firmar en Microsoft Outlook o Outlook Express.

Descifrado (correo electrónico)
Este objeto controla los requisitos de autenticación necesarios cuando se pulsa el botón Descifrar en Microsoft Outlook o Outlook Express.

Protección de archivos y carpetas
Este objeto controla los requisitos de autenticación necesarios cuando se ha seleccionado el cifrado y descifrado con el botón derecho.

Password Manager

Este objeto controla los requisitos de autenticación necesarios cuando se utiliza IBM Password Manager, que está disponible en el sitio Web de IBM. Cuando está activado, la mayoría de los usuarios deberían dejar este valor en ″No se necesita una frase de paso después de 1ª vez usada así″.

Inicio de sesión de Netscape - PKCS#11

Este objeto controla los requisitos de autenticación necesarios cuando el módulo PKCS#11 recibe una llamada C_OpenSession de PKCS#11. La mayoría de los usuarios deberían dejar este valor en “No se necesita una frase de paso después de 1ª vez usada así”.

Inicio de sesión de Entrust

Este objeto controla los requisitos de autenticación necesarios cuando Entrust emite una llamada C_OpenSession de PKCS#11 para que la reciba el módulo PKCS#11. La mayoría de los usuarios deberían dejar este valor en “No se necesita una frase de paso después de 1ª vez usada así”.

Cambio de contraseña de inicio de sesión de Entrust

Este objeto controla los requisitos de autenticación necesarios para cambiar la contraseña de inicio de sesión de Entrust. Entrust hace esto emitiendo una llamada C_OpenSession de PKCS#11 para que la reciba el módulo PKCS#11. La mayoría de los usuarios deberían dejar este valor en “No se necesita una frase de paso después de 1ª vez usada así”.

Elementos de autenticación

La política de UVM establece los elementos de autenticación disponibles que van a ser necesarios para cada objeto que se habilite. Esto permite establecer distintas políticas de seguridad para las diversas acciones de usuario.

Los elementos de autenticación que pueden seleccionarse en la pestaña **Elementos de autenticación** en la pantalla Política de IBM UVM en Administrator Utility incluyen los siguientes:

Selección de frase de paso

Esta selección permite al administrador establecer la frase de paso de UVM que se va a utilizar para autenticar un usuario de cualquiera de las tres formas siguientes:

- Se precisa una frase de paso nueva siempre.
- No se necesita una frase de paso después de 1ª vez usada así.
- No se necesita una frase de paso si se da en inicio de sesión sistema.

Selección de huella dactilar

Esta selección permite al administrador establecer que se utilice la exploración de una huella dactilar para autenticar un usuario de cualquiera de las tres formas siguientes:

- Se precisa una huella dactilar nueva siempre.
- No se necesita una huella dactilar después de 1ª vez usada así.
- No se necesita una huella dactilar si se da en inicio de sesión sistema.

Valores globales de huellas dactilares

Esta selección permite al administrador establecer un número máximo de reintentos de autenticación antes de que el sistema bloquee a un usuario. Esta área también permite al administrador dejar que la protección mediante autenticación de huellas dactilares se sobrescriba con la frase de paso de UVM.

Selección de Smart Card
Esta selección permite al administrador solicitar que se proporcione una smart card como un dispositivo de autenticación adicional.

Valores globales de Smart Card
Esta selección permite al administrador establecer la política para permitir la sobrescritura cuando se proporcione la frase de paso de UVM.

Utilización del editor de política de UVM

Para utilizar el editor de política de UVM, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
2. Pulse el botón **Política de aplicaciones**.

   Se mostrará la pantalla Modificar la configuración de políticas de Client Security.
3. Pulse el botón **Editar política**.

   Se muestra la pantalla Entre la contraseña del administrador.
4. Entre la contraseña del administrador y pulse **Aceptar**.

   Se muestra la pantalla Política de IBM UVM.
5. En la pestaña Selección de objetos, pulse **Acción** o **Tipo de objeto** y seleccione el objeto al que desea asignar requisitos de autenticación.

   Entre las acciones se incluyen Inicio de sesión del sistema, Desbloqueo del sistema, Descifrado de correo electrónico; un ejemplo de un tipo de objeto es Obtener un certificado digital.
6. Para cada objeto que seleccione, efectúe una de las acciones siguientes:
   - Pulse la pestaña **Elementos de autenticación** y edite los valores de los elementos de autenticación disponibles que desea asignar al objeto.
   - Seleccione **Tivoli Access Manager controla el objeto seleccionado** para habilitar Tivoli Access Manager para que controle el objeto seleccionado. Seleccione esta opción sólo si desea que Tivoli Access Manager controle los elementos de autenticación del cliente de IBM. Para obtener más información, consulte *Utilización de Client Security con Tivoli Access Manager*.

     Importante: si se habilita Tivoli Access Manager para que controle el objeto, se da el control del objeto al espacio de objetos de Tivoli Access Manager. Si lo hace, deberá reinstalar Client Security Software para volver a establecer el control local sobre ese objeto.
   - Seleccione **Denegar todo acceso al objeto seleccionado** para denegar el acceso para el objeto seleccionado.
7. Pulse **Aceptar** para guardar los cambios y salir.

Edición y utilización de la política de UVM para clientes remotos

Para utilizar la política de UVM en varios clientes de IBM, edite y guarde la política de UVM para clientes remotos y después copie el archivo de políticas de UVM en otros clientes de IBM. Si instala Client Security en la ubicación por omisión, se almacenará el archivo de políticas de UVM como \Archivos de programa\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copie los archivos siguientes en los otros clientes de IBM remotos que vayan a utilizar esta política de UVM:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Si ha instalado Client Security Software en la ubicación por omisión, el directorio raíz de las vías de acceso anteriores es \Archivos de programa. Copie ambos archivos en la vía de acceso del directorio \IBM\Security\UVM_Policy\ de los clientes remotos.

Capítulo 7. Otras funciones para el administrador de seguridad

Cuando se configura Client Security Software en clientes de IBM, se utiliza Administrator Utility para habilitar el chip IBM Security Chip incorporado, establecer una contraseña del chip de seguridad, generar las claves de hardware y configurar la política de seguridad. Esta sección proporciona instrucciones para utilizar otras funciones de Administrator Utility.

Para abrir Administrator Utility, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Dado que el acceso a Administrator Utility está protegido por la contraseña del chip de seguridad, se mostrará un mensaje que le solicitará que escriba la contraseña del chip de seguridad.
2. Escriba la contraseña del chip de seguridad y pulse **Aceptar**.

Utilización de Administrator Console

Client Security Software Administrator Console permite a un administrador de seguridad efectuar tareas específicas del administrador de forma remota de su sistema.

La aplicación Administrator Console (console.exe) debe instalarse y ejecutarse desde el directorio `\Archivos de programa\ibm\security`.

Administrator Console permite que un administrador de seguridad utilice las funciones siguientes:

- **Cancelar o sobrescribir los elementos de autenticación.** Las funciones de cancelación o sobrescritura que puede efectuar el administrador incluyen las siguientes:
  - **Cancelación de la frase de paso de UVM.** Esta función permite al administrador pasar por alto la frase de paso de UVM. Cuando se utiliza esta función, se crea una frase de paso aleatoria temporal, junto con un archivo de contraseña. El administrador envía el archivo de contraseña al usuario y le comunica la contraseña por algún otro medio. Esto garantiza la seguridad de la nueva frase de paso.
  - **Mostrar/Cambiar la contraseña de sobrescritura de huellas dactilares/smart card.** Esta función permite al administrador sobrescribir la política de seguridad incluso si está establecido NO permitir que se sobrescriba la frase de paso para huellas dactilares o smart card. Esto podría ser necesario si se rompe o no está disponible el lector de huellas dactilares de un usuario o su smart card. El administrador puede leer o enviar por correo electrónico la contraseña de sobrescritura al usuario.
- **Acceder a información de la clave de archivador.** La información a la que puede acceder el administrador incluye la siguiente:
  - **Directorio del archivador.** Este campo permite al administrador localizar la información de la clave del archivador desde una ubicación remota.
  - **Ubicación de la clave privada del administrador.** Este campo permite al administrador localizar la clave privada del administrador.

© Copyright IBM Corp. 2002

- **Otras funciones remotas del administrador.** Administrator Console permite a los administradores de seguridad realizar las funciones siguientes de forma remota:
  - **Crear archivo de configuración del administrador.** Esta función permite al administrador generar el archivo de configuración del administrador, lo que se necesario cuando un usuario desea inscribirse o restablecer su configuración utilizando User Configuration Utility. El administrador suele enviar el archivo por correo electrónico al usuario.
  - **Cifrar/Descifrar archivo de configuración.** Esta función permite el cifrado del archivo de configuración para mayor seguridad. También descifrará el archivo para que pueda editarse.
  - **Configurar itinerancia de credenciales.** Esta función registra este sistema como un servidor de itinerancia CSS. Una vez registrados, todos los usuarios autorizados para UVM en la red podrán acceder a sus datos personales (frases de paso, certificado, etc.) en este sistema.

Registro de un cliente en una red de itinerancia de credenciales

Para efectuar el registro silencioso de un cliente en una red de itinerancia de credenciales, complete el procedimiento siguiente:

1. Mediante el programa de utilidad de la consola, descifre un archivo CSEC.INI generado previamente. Este archivo ya contendrá la contraseña de hardware y los usuarios que hay que inscribir.
2. En la sección csssetup del archivo, añada `"enableroaming=1"`. Esto indica que el sistema debe registrarse como un cliente itinerante.
3. En la misma sección, añada la entrada `"username=OPCIÓN"`. Hay tres opciones posibles para este valor:
   a. **La serie `"[promptcurrent]"` - incluidos los corchetes.** Esta designación debería utilizarse si se ha generado en el servidor de itinerancia un archivo .dat para el usuario que tiene iniciada la sesión actualmente y el usuario actual conoce la contraseña de registro del sistema. Esta opción hará que aparezca un recuadro emergente que solicita la usuario que entre la contraseña de registro del sistema (`sysregpwd`). Obviamente, si se trata de una instalación totalmente silenciosa, el administrador preferirá evitar este valor ya que requiere que haya un usuario en el teclado.
   b. **La serie `"[current]"` - incluidos los corchetes.** Esta designación debería utilizarse si se ha generado en el servidor un archivo .dat para el usuario que tiene iniciada la sesión actualmente. La contraseña de registro del sistema (`sysregpwd`) se gestionará del modo que se describe en el punto siguiente.
   c. **Un nombre de usuario real como `"juan"`.** Si se utiliza un nombre de usuario específico, el servidor de itinerancia debe haber generado previamente `"juan.dat"`. La `sysregpwd` para este caso también se gestionará como se describe en el punto siguiente.
4. Finalmente, si se utilizan las opciones dos o tres anteriores, debe indicarse otra entrada `"sysregpwd=SYSREGPW"`. Es la contraseña de ocho dígitos asociada al usuario actual (si se ha implementado la opción dos) o el usuario específico (si se ha implementado la opción tres).
5. Para completar el registro del cliente, conecte el sistema a la ubicación del archivador configurada por el servidor de itinerancia. La ubicación del archivador se definirá en el archivo CSEC.INI.

Ejemplos del archivo CSEC.INI

Los ejemplos siguientes muestran un archivo CSEC.INI de ejemplo y cómo cambiaría en función de la opción de itinerancia de credenciales que se seleccione. Estas opciones son las siguientes:

- **Sin valores de itinerancia.** Este archivo base no tiene habilitada la itinerancia de credenciales.
- **Opción de itinerancia 1.** Este archivo tiene habilitada la itinerancia con la opción 1 para el registro de clientes. El usuario actual debe indicar la contraseña de registro del sistema.
- **Opción de itinerancia 2.** Este archivo tiene habilitada la itinerancia con la opción 2 para el registro de clientes. El usuario actual debe indicar su ID de usuario y la contraseña de registro del sistema.
- **Opción de itinerancia 3.** Este archivo tiene habilitada la itinerancia con la opción 3 para el registro de clientes. Se especifica un usuario. El usuario específico debe indicar la contraseña de registro del sistema.

Estos son los ejemplos de cuatro archivos CSEC.INI distintos:

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
clean=0

[UVMEnrollment]
enrollall=0
user1=juan
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
enableroaming=1
username=
[promptcurrent]
clean=0

[UVMEnrollment]
enrollall=0
user1=juan
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
enableroaming=1
username=[current]

sysregpwd=12345678
clean=0

[UVMEnrollment]
enrollall=0
user1=juan
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
enableroaming=1
username=juan

sysregpwd=12345678
clean=0

[UVMEnrollment]
enrollall=0
user1=juan
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

Cambio de la ubicación del archivador de claves

Cuando se crea por primera vez el archivador de claves, se crean copias de todas las claves de cifrado y se guardan en la ubicación especificada en la instalación.

Nota: el usuario cliente también puede cambiar la ubicación del archivador de claves mediante User Configuration Utility. Para obtener más información, consulte el Capítulo 8, “Instrucciones para el usuario cliente”, en la página 39.

Para cambiar la ubicación del archivador de claves, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Configuración de claves**.

   Se muestra la pantalla Modificar la configuración de claves de Client Security-Configurar claves.
2. Pulse el botón de selección **Cambiar la ubicación del archivador** y pulse **Siguiente**.

   Se muestra la pantalla Modificar la configuración de claves de Client Security-Nueva ubicación del archivador de claves.
3. Escriba la nueva vía de acceso o pulse **Examinar** para seleccionar la vía de acceso.
4. Pulse **Aceptar**.

   Aparece un mensaje que indica que la operación se ha completado.
5. Pulse **Finalizar**.

Cambio del par de claves del archivador

Cuando se crea por primera vez el par de claves del archivador, se suele almacenar en un disquete o un directorio de red. Si se dañara el par de claves del archivador, podría cambiar a otro par de claves del archivador.

Nota: asegúrese de actualizar el archivador antes de cambiar el par de claves del archivador.

Para cambiar el par de claves del archivador, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Configuración de claves**.

   Se muestra la pantalla Modificar la configuración de claves de Client Security-Configurar claves.
2. Pulse el botón de selección **Cambiar el par de claves del archivador de IBM Security Subsystem** y pulse **Siguiente**.

   Se muestra la pantalla Modificar la configuración de claves de Client Security - Nuevo archivo de claves públicas del administrador de UVM.
3. En el área Clave nueva del archivador de CSS, escriba el nombre de archivo de la clave pública nueva del archivador en el campo Archivo de claves públicas. También puede pulsar **Examinar** para buscar el archivo nuevo o pulsar **Crear** para generar una clave pública nueva del archivador.

   Nota: asegúrese de crear la clave pública nueva en una ubicación distinta a la que contiene los archivos de claves del archivador antiguos.
4. En el área Clave nueva del archivador de CSS, escriba el nombre de archivo de la clave privada nueva del archivador en el campo Archivo de claves

privadas. También puede pulsar **Examinar** para buscar el archivo nuevo o pulsar **Crear** para generar un par de claves nuevo del archivador.

Nota: asegúrese de crear el par de claves nuevo en una ubicación distinta a la que contiene los archivos de claves del archivador antiguos.

5. En el área Clave antigua del archivador de CSS, escriba el nombre de archivo de la clave pública antigua del archivador en el campo Archivo de claves públicas o pulse **Examinar** para buscar el archivo.
6. En el área Clave antigua del archivador de CSS, escriba el nombre de archivo de la clave privada antigua del archivador en el campo Archivo de claves privadas o pulse **Examinar** para buscar el archivo.
7. En el área Ubicación del archivador, escriba la vía de acceso donde está almacenado el archivador de claves o pulse **Examinar** para seleccionar la vía de acceso.
8. Pulse **Siguiente**.

   Nota: si se ha dividido el par de claves del archivador en varios archivos, se mostrará un mensaje que le solicitará que escriba la ubicación y el nombre de cada archivo. Pulse **Leer siguiente** después de escribir todos los nombres de archivo en el campo Archivo de claves.

   Aparece un mensaje que indica que la operación se ha completado satisfactoriamente.
9. Pulse **Aceptar**.

   Aparece un mensaje que indica que la operación se ha completado.
10. Pulse **Finalizar**.

Restauración de las claves desde el archivador

Si ha sustituido la placa del sistema o se ha producido una anomalía en la unidad de disco duro es posible que tenga que restaurar las claves. Cuando restaura claves, se copian los últimos archivos de claves de usuario del archivador de claves y se almacenan en el chip IBM Security Chip incorporado. Estos archivos de claves de usuario copiados aparecen en el directorio donde se habían almacenado anteriormente en el sistema, como un directorio de red o un disquete.

Si una anomalía en la unidad de disco duro del sistema compromete la integridad de las claves de usuario, puede restaurar las claves del archivador de claves. La restauración de las claves escribirá encima de cualquier clave que se haya almacenado.

Si sustituye la placa del sistema por otra que contiene el chip IBM Security Chip incorporado y aún son válidas las claves de cifrado en la unidad de disco duro, puede restaurar las claves de cifrado que se han asociado previamente al sistema "volviendo a cifrarlas" con el chip IBM Security Chip incorporado en la placa del sistema nueva.

Puede realizar una restauración de claves después de habilitar el chip nuevo y establecer una contraseña del chip de seguridad. Para obtener detalles, consulte "Habilitación del chip IBM Security Chip incorporado y establecimiento de la contraseña del chip de seguridad" en la página 37.

Nota: se habilita automáticamente el inicio de sesión de UVM después de una restauración de claves. Como consecuencia, si era necesaria la

autenticación de huellas dactilares para el inicio de sesión de UVM, DEBERÁ instalar el software de huellas dactilares antes de rearrancar después de la restauración para evitar que se bloquee el sistema.

En las instrucciones siguientes se supone que Administrator Utility no se ha dañado por una anomalía en la unidad de disco duro. Si la anomalía en la unidad de disco duro ha dañado los archivos de seguridad del cliente, es posible que tenga que volver a instalar Client Security Software.

Para restaurar las claves de cifrado desde el archivador de claves, complete el procedimiento siguiente de Administrator Utility:

Nota: si cambia el par de claves del administrador después de restaurar el archivador, se mostrará un mensaje de error. Si se produjera este error, deberá añadir los usuarios a UVM y solicitar certificados nuevos.

1. Pulse el botón **Configuración de claves**.

   Se muestra la pantalla Modificar la configuración de claves de Client Security-Configurar claves.
2. Pulse el botón de selección **Restaurar las claves de IBM Security Subsystem desde el archivador** y a continuación pulse **Siguiente**.

   Se muestra la pantalla Modificar la configuración de claves de Client Security-Restaurar todas las claves de IBM Security Subsystem.
3. En el campo Directorio del archivador (vía de acceso), escriba la vía de acceso al directorio del archivador o pulse **Examinar** para buscar el directorio.
4. En el campo Archivo de claves públicas del archivador de CSS, escriba la vía de acceso y el nombre de archivo de la clave pública del administrador o pulse **Examinar** para buscar el archivo.
5. En el campo Archivo de claves privadas del archivador de CSS, escriba la vía de acceso y el nombre de archivo de la clave privada del administrador o pulse **Examinar** para buscar el archivo.
6. Pulse **Siguiente**.

   Aparecerá un mensaje que indica que la operación se ha completado satisfactoriamente.

   Nota: si se ha dividido la clave privada del administrador en varios archivos, se mostrará un mensaje que le solicitará que escriba la ubicación y el nombre de cada archivo. Pulse **Leer siguiente** después de escribir todos los nombres de archivo en el campo Archivo de claves.
7. Pulse **Aceptar**.
8. Pulse **Finalizar**.

Restablecimiento del contador de errores de autenticación

Para restablecer el contador de errores de autenticación para un usuario, complete el procedimiento siguiente en Administrator Utility:

1. En el área Usuarios de Windows autorizados para usar UVM, seleccione un usuario.
2. Pulse **Restablecer nº errores**.

   Se muestra la pantalla Restablecer nº de errores para el usuario.
3. Escriba la frase de paso de UVM del usuario seleccionado y pulse **Aceptar**.

   Se mostrará un mensaje que notifica que la operación se ha completado satisfactoriamente.

4. Pulse **Aceptar**.

Cambio de la información de configuración de Tivoli Access Manager

La información siguiente va dirigida a los administradores de seguridad que desean utilizar Tivoli Access Manager para gestionar objetos de autenticación para la política de seguridad de UVM. Para obtener más información, consulte *Utilización de Client Security con Tivoli Access Manager*.

Acceso al archivo de configuración de Tivoli Access Manager

Para definir la información de configuración de Tivoli Access Manager en el cliente de IBM, Client Security Software utiliza un archivo de configuración. Este archivo de configuración se utiliza para enlazar Tivoli Access Manager con los objetos que la política de UVM cede para ser controlados por él. Para acceder a la configuración de Tivoli Access Manager, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
2. En el área Información de configuración de Tivoli Access Manager, escriba la vía de acceso y el nombre de archivo del archivo de configuración o pulse **Examinar** para buscar el archivo.
3. Pulse el botón **Editar política**.
4. Continúe con el procedimiento de edición de política.

Renovación de la antememoria local

En el cliente de IBM se mantiene una duplicación local de la información de política de seguridad gestionada por Tivoli Access Manager. Puede establecer la cadencia de renovación de la antememoria local en incrementos de meses y días o, puede pulsar un botón para actualizar inmediatamente la antememoria local.

Para establecer o renovar la antememoria local, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
2. En el área Intervalo de renovación de la antememoria local, efectúe una de las acciones siguientes:
   - Para renovar la antememoria local ahora, pulse **Renovar antememoria local**.
   - Para establecer la cadencia de renovación, escriba el número de meses y días en los campos proporcionados. El valor de meses y días representa la cantidad de tiempo entre renovaciones planificadas.

Recuperación de frases de paso de UVM

Para cada usuario que se autoriza mediante la política de seguridad del cliente de IBM se crea una frase de paso de UVM. Dado que se pueden perder u olvidar las frases de paso o el usuario cliente puede cambiarlas, Administrator Utility permite a un administrador recuperar una frase de paso perdida u olvidada.

Para recuperar una frase de paso, complete el procedimiento de Administrator Utility siguiente:

1. Seleccione un usuario en el campo Usuarios de Windows autorizados para usar UVM.
2. Pulse el botón **Cambiar frase de paso**.

   Se abrirá la pantalla Cambiar frase de paso.
3. En el campo Ubicación del archivador de IBM Security Subsystem, escriba la vía de acceso y el nombre de directorio del archivador de claves o pulse **Examinar** para localizar el directorio.
4. En el área Clave del archivador de IBM Security Subsystem, escriba la vía de acceso y el nombre de archivo de la clave privada del administrador en el campo Archivo de claves privadas o pulse **Examinar** para localizar el archivo.
5. En el área Clave del archivador de IBM Security Subsystem, escriba la vía de acceso y el nombre de archivo de la clave pública del administrador en el campo Archivo de claves públicas o pulse **Examinar** para localizar el archivo.
6. Pulse **Aceptar**.

   Se mostrará un mensaje que le indicará la frase de paso de UVM del usuario.
7. Pulse **Aceptar**.

   Si se ha dividido la clave privada del administrador en varios archivos, se mostrará un mensaje que le solicitará que escriba la ubicación y el nombre de cada archivo. Pulse **Leer siguiente** después de escribir todos los nombres de archivo en el campo Archivo de claves privadas.

   Este procedimiento generará una contraseña aleatoria temporal y un archivo de contraseña. Ambos elementos son necesarios para volver a obtener acceso al sistema bloqueado.
8. Envíe el archivo al usuario y comuníquele la contraseña temporal por algún otro medio.

Cambio de la contraseña del chip IBM Security Chip

Debe establecer 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. Para mejorar la seguridad, debería cambiar periódicamente la contraseña del chip de seguridad. Las contraseñas que permanecen si cambiar durante un largo período de tiempo pueden ser más vulnerables a ataques externos. Proteja con contraseña el chip de seguridad para impedir que los usuarios no autorizados cambien valores en Administrator Utility. Para obtener información sobre las normas para la contraseña del chip de seguridad, consulte el Apéndice B, “Normas para contraseñas y frases de paso”, en la página 67.

Para cambiar la contraseña del chip de seguridad, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Valores del chip**.

   Se mostrará la pantalla Modificar valores del chip IBM Security Chip.
2. Pulse **Cambiar contraseña del chip**.

   Se muestra la pantalla Cambiar contraseña del chip IBM Security Chip.
3. En el campo Contraseña nueva, escriba la contraseña nueva.
4. En el campo Confirmación, escriba de nuevo la contraseña.
5. Pulse **Aceptar**.

   Se mostrará un mensaje que notifica que la operación se ha completado satisfactoriamente.

Atención: no pulse Intro ni Tab > Intro para guardar los cambios. Si lo hace, se mostrará la pantalla Inhabilitar chip. Si se abre dicha ventana, no inhabilite el chip; en lugar de eso, salga de la pantalla.

6. Pulse **Aceptar**.

Consulta de información sobre Client Security Software

La información que se detalla a continuación sobre el chip IBM Security Chip incorporado y Client Security Software está disponible pulsando el botón **Valores del chip** de Administrator Utility:

- El número de versión del firmware utilizado con Client Security Software
- El estado de cifrado del chip de seguridad incorporado
- La validez de las claves de cifrado del hardware
- El estado del chip IBM Security Chip incorporado

Inhabilitación del chip IBM Security Chip incorporado

Administrator Utility proporciona un modo de inhabilitar el chip IBM Security Chip incorporado. Dado que es necesaria la contraseña del chip de seguridad para iniciar Administrator Utility e inhabilitar el chip, proteja la contraseña del chip de seguridad para prohibir a los usuarios no autorizados que inhabiliten el chip.

Importante: no borre la información del chip IBM Security Chip incorporado mientras esté habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema. Para borrar la protección de UVM, abra Administrator Utility 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 para el inicio de sesión del sistema.

Para inhabilitar el chip de seguridad incorporado, complete el procedimiento siguiente de Administrator Utility:

1. Pulse el botón **Valores del chip**.
2. Pulse el botón **Inhabilitar chip** y siga las instrucciones que aparecen en pantalla.
3. Si el sistema tiene habilitada la seguridad ampliada, es posible que tenga que escribir la contraseña del administrador que se ha establecido en el programa Configuration/Setup Utility para inhabilitar el chip.

Para utilizar el chip IBM Security Chip incorporado y las claves de cifrado de hardware después de que se inhabilita el chip, deber volver a habilitar el chip.

Habilitación del chip IBM Security Chip incorporado y establecimiento de la contraseña del chip de seguridad

Si tiene que habilitar el chip IBM Security Chip incorporado después de instalar el software, puede utilizar Administrator Utility para restablecer la contraseña del chip de seguridad así como para configurar nuevas claves de cifrado.

Es posible que necesite habilitar el chip IBM Security Chip incorporado para restaurar el archivo de claves después de una sustitución de la placa del sistema o si ha inhabilitado el chip.

Para habilitar el chip y establecer la contraseña del chip de seguridad, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se mostrará un mensaje que le solicita que habilite el chip IBM Security Chip incorporado para el cliente de IBM.
2. Pulse **Sí**.

   Se mostrará un mensaje que le solicitará que reinicie el sistema. Debe reiniciar el sistema antes de habilitar el chip IBM Security Chip incorporado. Si el sistema tiene habilitada la seguridad ampliada, es posible que tenga que escribir la contraseña del administrador que se ha establecido en el programa Configuration/Setup Utility para habilitar el chip.
3. Pulse **Aceptar** para reiniciar el sistema.
4. En el escritorio de Windows, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Dado que el acceso a Administrator Utility está protegido por la contraseña del chip de seguridad, se mostrará un mensaje que le solicitará que escriba la contraseña del chip de seguridad.
5. Escriba una nueva contraseña para el chip de seguridad en el campo Contraseña nueva y, a continuación, escríbala de nuevo en el campo Confirmación.
6. Pulse **Aceptar**.

Habilitación del soporte de Entrust

El chip IBM Security Chip incorporado funciona con Client Security Software para ampliar las características de seguridad de Entrust. Si se habilita el soporte de Entrust en sistemas con Client Security Software se transfieren las funciones de seguridad del software de Entrust al chip IBM Security Chip.

Client Security Software encontrará automáticamente el archivo entrust.ini para habilitar el soporte de Entrust; no obstante, si el archivo entrust.ini no se encuentra en la vía de acceso habitual, se abrirá un diálogo para que el usuario pueda buscar el archivo entrust.ini. Después de que el usuario localice y seleccione el archivo, Client Security puede habilitar el soporte de Entrust. Después de pulsar el recuadro de selección **Habilitar soporte de Entrust**, es necesario rearrancar el sistema para que Entrust haga uso del chip IBM Security Chip incorporado.

Para habilitar el soporte de Entrust, complete el procedimiento siguiente:

1. En el escritorio de Windows del cliente de IBM, pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.

   Se abrirá la ventana principal de Administrator Utility.
2. Pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
3. Seleccione el recuadro de selección **Habilitar soporte de Entrust**.
4. Pulse **Aplicar**.

   Se mostrará la pantalla Soporte de Entrust de IBM Client Security con un mensaje que indica que está habilitado el soporte de Entrust.

Nota: debe reiniciar el sistema para que los cambios tengan efecto.

Capítulo 8. Instrucciones para el usuario cliente

Esta sección proporciona información para ayudar a un usuario cliente a efectuar las tareas siguientes:

- Utilizar la protección de UVM para el inicio de sesión del sistema
- Configurar el protector de pantalla de Client Security
- Utilizar User Configuration Utility
- Utilizar correo electrónico y navegación en la Web seguros
- Configurar las preferencias de sonido de UVM

Utilización de la protección de UVM para el inicio de sesión del sistema

Esta sección contiene información sobre la utilización de la protección de inicio de sesión de UVM para el inicio de sesión del sistema. Antes de poder utilizar la protección de UVM, debe estar habilitada para el sistema.

La protección de UVM permite controlar el acceso al sistema operativo mediante una interfaz de inicio de sesión. La protección de inicio de sesión de UVM sustituye a la aplicación de inicio de sesión de Windows, de modo que cuando un usuario desbloquea el sistema, se abre la ventana de inicio de sesión de UVM en lugar de la ventana de inicio de sesión de Windows. Después de habilitar la protección de UVM para el sistema, se abrirá la interfaz de inicio de sesión de UVM cuando se inicie el sistema.

Cuando el sistema esté en ejecución, puede acceder a la interfaz de inicio de sesión de UVM pulsando **Control + Alt + Supr** para concluir o bloquear el sistema, o abrir el Administrador de tareas o cerrar la sesión del usuario actual.

Desbloqueo del cliente

Para desbloquear un cliente Windows que utilice la protección de UVM, complete el procedimiento siguiente:

1. Pulse **Control + Alt + Supr** para acceder a la interfaz de inicio de sesión de UVM.
2. Escriba el nombre de usuario y el dominio en el que va a iniciar la sesión y después pulse **Desbloquear**.

   Se abre la ventana de frase de paso de UVM.

   Nota: aunque UVM reconoce varios dominios, su contraseña de usuario debe ser la misma para todos ellos.
3. Escriba la frase de paso de UVM y pulse **Aceptar** para acceder al sistema operativo.

Notas:

1. Si la frase de paso de UVM no se corresponde con el nombre de usuario y el dominio entrados, se abre de nuevo la ventana de inicio de sesión de UVM.
2. Dependiendo de los requisitos de autenticación de política de UVM para el cliente, también pueden ser necesarios procesos de autenticación adicionales.

© Copyright IBM Corp. 2002

El protector de pantalla de Client Security

El protector de pantalla de Client Security consiste en una serie de imágenes en movimiento que se muestran después de que el sistema esté desocupado durante un período de tiempo especificado. La configuración del protector de pantalla de Client Security es una forma de controlar el acceso al sistema mediante una aplicación de protector de pantalla. Cuando el protector de pantalla de Client Security se muestre en el escritorio, debe escribir la frase de paso de UVM para acceder al escritorio del sistema.

Configuración del protector de pantalla de Client Security

Esta sección contiene información sobre la configuración del protector de pantalla de Client Security. Antes de utilizar el protector de pantalla de Client Security, debe haber registrado al menos un usuario en la política de seguridad del sistema.

Para configurar el protector de pantalla de Client Security, complete el procedimiento siguiente:

1. Pulse **Inicio > Configuración > Panel de control**.
2. Efectúe una doble pulsación en el icono **Pantalla**.
3. Pulse la pestaña **Protector de pantalla**.
4. En el menú desplegable Protector de pantalla, seleccione **Client Security**. Para cambiar la velocidad del protector de pantalla, pulse **Configuración** y seleccione la velocidad deseada.
5. Pulse **Aceptar**.

Comportamiento del protector de pantalla de Client Security

El comportamiento del protector de pantalla de Client Security varía en función de los valores de Administrator Utility de UVM y el protector de pantalla de Windows. El sistema comprueba primero los valores de Windows y después los valores de Administrator Utility de UVM. En consecuencia, el protector de pantalla sólo bloquea el sistema si se ha seleccionado el recuadro de selección **Protegido por contraseña** en la pestaña de configuración del protector de pantalla de Windows.

Si se ha seleccionado este recuadro, el sistema solicita la contraseña de Windows o la frase de paso de UVM, en función de si se ha seleccionado el recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM** en Administrator Utility. Si se ha seleccionado, el sistema solicita la frase de paso de UVM. Si no se ha solicitado, el sistema solicita la contraseña de Windows.

Además, se han podido establecer otros requisitos de autenticación en la política de seguridad del sistema; por lo tanto, es posible que se efectúen más procesos de autenticación. Por ejemplo, es posible que tenga que explorar sus huellas dactilares para desbloquear el sistema.

Nota: si inhabilita el chip IBM Security Chip incorporado o elimina todos los usuarios de la política de seguridad, dejará de estar disponible el protector de pantalla de Client Security.

User Configuration Utility

User Configuration Utility permite al usuario cliente efectuar varias tareas de mantenimiento de seguridad que no precisan el acceso del administrador.

Características de User Configuration Utility

User Configuration Utility permite al usuario cliente hacer lo siguiente:

- **Actualizar contraseñas y archivador.** Esta pestaña permite realizar las funciones siguientes:
  - **Cambiar la frase de paso de UVM.** Para mejorar la seguridad, puede cambiar periódicamente la frase de paso de UVM.
  - **Actualizar la contraseña de Windows.** Cuando cambie la contraseña de Windows para un usuario cliente autorizado para UVM con el programa Administrador de usuarios de Windows, también debe cambiar la contraseña utilizando IBM Client Security Software User Configuration Utility. Si un administrador utiliza Administrator Utility para cambiar la contraseña de inicio de sesión de un usuario, se suprimirán todas las claves de cifrado de usuario creadas para ese usuario y los certificados digitales quedarán invalidados.
  - **Restablecer la contraseña de Lotus Notes.** Para mejorar la seguridad, los usuarios de Lotus Notes pueden cambiar su contraseña de Lotus Notes.
  - **Actualizar el archivador de claves.** Si crea certificados digitales y desea hacer copias de la clave privada almacenada en el chip IBM Security Chip incorporado o si desea mover el archivador de claves a otra ubicación, puede actualizar el archivador de claves.
- **Configurar las preferencias de sonido de UVM.** User Configuration Utility permite seleccionar un archivo de sonido para que se ejecute cuando la autenticación tiene éxito o cuando da error.
- **Configuración del usuario.** Esta pestaña permite realizar las funciones siguientes:
-
  - **Restablecer usuario.** Esta función permite restablecer la configuración de seguridad. Cuando restablece su configuración de seguridad, se borran todas las claves, certificados, huellas dactilares, etc. anteriores.
  - **Restaurar la configuración de seguridad del usuario desde el archivador.** Esta función permite restaurar los valores desde el archivador. Resulta útil se se han dañado los archivos o si desea volver a una configuración anterior.
  - **Registrarse con un servidor de itinerancia de CSS.** Esta función le permite registrar este sistema con un servidor de itinerancia de CSS. Una vez registrado el sistema, podrá importar su configuración actual en este sistema.

Limitaciones de User Configuration Utility en Windows XP

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

Utilización de User Configuration Utility

Para utilizar User Configuration Utility, complete el procedimiento siguiente:

1. Pulse **Inicio > Programas > Access IBM > IBM Client Security Software > Modificar los valores de seguridad**.

   Se muestra la pantalla principal de IBM Client Security Software User Configuration Utility.
2. Escriba la frase de paso de UVM del usuario cliente que precise cambiar la frase de paso de UVM o la contraseña de Windows y pulse **Aceptar**.
3. Seleccione una de las pestañas siguientes:
   - **Actualizar contraseñas y archivador.** Esta pestaña permite cambiar la frase de paso de UVM, actualizar la contraseña de Windows en UVM, restablecer la contraseña de Lotus Notes en UVM y actualizar el archivador de cifrado.
   - **Configurar sonidos de UVM** Esta pestaña permite seleccionar un archivo de sonido para que se ejecute cuando la autenticación tiene éxito o cuando da error.
   - **Configuración del usuario.** Esta pestaña permite que un usuario restaure su configuración de usuario desde un archivador o que restablezca su configuración de seguridad.
4. Pulse **Aceptar** para salir.

Utilización de correo electrónico y navegación en la Web seguros

Si envía transacciones no seguras por Internet, corre el peligro de que sean interceptadas y leídas. Puede prohibir el acceso no autorizado a sus transacciones de Internet mediante la obtención de un certificado digital y su utilización para firmar digitalmente y cifrar sus mensajes de correo electrónico o para proteger su navegador Web.

Un certificado digital (también denominado ID digital o certificado de seguridad) es una credencial electrónica emitida y firmada digitalmente por una autoridad de certificados. Cuando se emite un certificado digital para un usuario, la autoridad de certificados está validando la identidad del usuario como propietario del certificado. Una autoridad de certificados es un proveedor fiable de certificados digitales y puede ser otra empresa emisora, como VeriSign; la autoridad de certificados también puede configurarse como un servidor dentro de su empresa. El certificado digital contiene su identidad, como su nombre y dirección de correo electrónico, las

fechas de caducidad del certificado, una copia de su clave pública y la identidad de la autoridad de certificados y su firma digital.

Utilización de Client Security Software con aplicaciones de Microsoft

Las instrucciones proporcionadas en esta sección son específicas para el uso de Client Security Software en lo que se refiere generalmente a la obtención y utilización de certificados digitales con aplicaciones que soporten Microsoft CryptoAPI, como Outlook Express.

Para obtener detalles sobre cómo crear los valores de seguridad y utilizar aplicaciones de correo electrónico, como Outlook Express y Outlook, consulte la documentación proporcionada con esas aplicaciones.

Nota: para utilizar navegadores de 128 bits con Client Security Software, el chip IBM Security Chip incorporado debe soportar el cifrado de 256 bits. El nivel de cifrado proporcionado por Client Security Software se encuentra en Administrator Utility.

Obtención de un certificado digital para aplicaciones de Microsoft

Cuando utilice una autoridad de certificados para crear un certificado digital que se va a utilizar con aplicaciones de Microsoft, se le solicitará que elija un proveedor de servicios criptográficos (CSP) para el certificado.

Para utilizar las posibilidades criptográficas del chip IBM Security Chip incorporado para las aplicaciones de Microsoft, asegúrese de seleccionar **IBM embedded Security Subsystem CSP** como el proveedor de servicios criptográficos cuando obtenga el certificado digital. Esto asegura que la clave privada del certificado digital se almacena en el chip IBM Security Chip.

Además, si está disponible, seleccione un cifrado fuerte (o alto) para mayor seguridad. Ya que el chip IBM Security Chip incorporado puede ofrecer un cifrado de hasta 1024 bits de la clave privada del certificado digital, seleccione esta opción si está disponible dentro de la interfaz de la autoridad de certificados; también se hace referencia al cifrado de 1024 bits como cifrado fuerte.

Después de seleccionar **IBM embedded Security Subsystem CSP** como el CSP, es posible que tenga que escribir la frase de paso de UVM, explorar sus huellas dactilares o hacer ambas cosas para cumplir los requisitos de autenticación para obtener un certificado digital. Los requisitos de autenticación están definidos en la política de UVM para el sistema.

Transferencia de certificados desde el CSP de Microsoft

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.

Para ejecutar la Herramienta de transferencia de certificados, complete el procedimiento siguiente:

1. Ejecute el programa `xfercert.exe` desde el directorio raíz del software de seguridad (generalmente C:\Archivos de programa\IBM\Security). El diálogo principal muestra los certificados asociados con el CSP de software de Microsoft por omisión.

   Nota: sólo se mostrarán en la lista los certificados cuyas claves privadas se marcaron como *exportables* cuando se crearon.
2. Seleccione los certificados que desea transferir al IBM embedded Security Subsystem CSP.
3. Pulse el botón **Transferir certificados**.

Los certificados están asociados ahora con el IBM embedded Security Subsystem CSP y las claves privadas están protegidas por el chip IBM Security Chip incorporado. Cualquier operación que utilice estas claves privadas, como la creación de firmas digitales o el descifrado de correo electrónico, se efectuará dentro del entorno protegido del chip.

Actualización del archivador de claves para aplicaciones de Microsoft

Después de crear un certificado digital, efectúe una copia de seguridad del certificado mediante la actualización del archivador de claves. Puede actualizar el archivador de claves utilizando Administrator Utility.

Utilización del certificado digital para aplicaciones de Microsoft

Utilice los valores de seguridad de las aplicaciones de Microsoft para ver y utilizar certificados digitales. Consulte la documentación proporcionada por Microsoft para obtener más información.

Después de crear el certificado digital y utilizarlo para firmar un mensaje de correo electrónico, UVM le solicitará los requisitos de autenticación la primera vez que firme digitalmente un mensaje de correo electrónico. Es posible que tenga que escribir la frase de paso de UVM, explorar sus huellas dactilares o hacer ambas cosas para cumplir los requisitos para utilizar el certificado digital. Los requisitos de autenticación están definidos en la política de UVM para el sistema.

Configuración de las preferencias de sonido de UVM

User Configuration Utility permite configurar las preferencias de sonido utilizando la interfaz proporcionada. Para cambiar las preferencias de sonido por omisión, complete el procedimiento siguiente:

1. Pulse **Inicio** > **Programas** > **Access IBM** > **IBM Client Security Software** > **Modificar los valores de seguridad**.

   Se muestra la pantalla de IBM Client Security Software User Configuration Utility.
2. Seleccione la pestaña **Configurar sonidos de UVM**.
3. En el área Sonidos de autenticación de UVM, en el campo Autenticación con éxito, escriba la vía de acceso al archivo de sonido que le gustaría asociar a una autenticación con éxito o pulse **Examinar** para seleccionar el archivo.
4. En el área Sonidos de autenticación de UVM, en el campo Autenticación con error, escriba la vía de acceso al archivo de sonido que le gustaría asociar a una autenticación con error o pulse **Examinar** para seleccionar el archivo.
5. Pulse **Aceptar** para completar el proceso.

Capítulo 9. 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. Normas para la utilización de la protección de UVM para el inicio de sesión del sistema

La protección de UVM asegura que sólo aquellos usuarios que se hayan añadido a UVM para un cliente de IBM específico pueden acceder al sistema operativo. El sistema operativo Windows incluye aplicaciones que proporcionan protección de inicio de sesión. Aunque la protección de UVM está diseñada para trabajar en paralelo con esas aplicaciones de inicio de sesión de Windows, la protección de UVM es diferente según el sistema operativo.

La interfaz de inicio de sesión de UVM sustituye al inicio de sesión del sistema operativo, de modo que la ventana de inicio de sesión de UVM se abre cada vez que un usuario intenta iniciar una sesión en el sistema.

Lea los consejos siguientes antes de establecer y utilizar la protección de UVM para el inicio del sesión del sistema:

- No borre la información del chip IBM Security Chip incorporado mientras esté 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.
- Si quita la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM** en Administrator Utility, el sistema vuelve al proceso de inicio de sesión de Windows sin la protección de inicio de sesión de UVM.
- Tiene la opción de especificar el número máximo de intentos permitido para escribir la contraseña correcta para la aplicación de inicio de sesión de Windows. Esta opción *no* se aplica a la protección de inicio de sesión de UVM. No hay un límite que pueda establecerse para el número de intentos permitido para escribir la frase de paso de UVM.

© Copyright IBM Corp. 2002

Apéndice D. 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: 59P7648

(1P) P/N: 59P7648