Soluciones IBM Client Security

Utilización de Client Security Software Versión 5.1 con Tivoli Access Manager

Soluciones IBM Client Security

Utilización de Client Security Software Versión 5.1 con Tivoli Access Manager

Primera edición (abril de 2003)

Esta publicación es la traducción del original inglés *Using Client Security Software Version 5.1 with Tivoli Access Manager*.

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 33 y el Apéndice D, “**Avisos y marcas registradas**”, en la página 39.

Contenido

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

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

Capítulo 2. Instalación del componente Client Security en un servidor Tivoli Access Manager 5
Requisitos previos 5
Cómo bajar e instalar el componente Client Security 5
Adición de componentes Client Security en el servidor Tivoli Access Manager 6
Establecimiento de una conexión segura entre el cliente de IBM y el servidor Tivoli Access Manager 7

Capítulo 3. Configuración de los clientes de IBM 9
Requisitos previos 9
Definición de la información de configuración de Tivoli Access Manager 9
Establecimiento y utilización de la característica de antememoria local 10
Habilitación de Tivoli Access Manager para controlar los objetos del cliente de IBM 10
Edición de una política local de UVM 11
Edición y utilización de la política de UVM para clientes remotos 12

Capítulo 4. Resolución de problemas 13
Funciones del administrador 13
Establecimiento de una contraseña del administrador (ThinkCentre) 13
Establecimiento de una contraseña del supervisor (ThinkPad) 14
Protección de la contraseña de hardware 15
Borrado de la información del chip IBM Security Chip incorporado (ThinkCentre) 15
Borrado de la información del chip IBM Security Chip incorporado (ThinkPad) 15
Administrator Utility 16
Supresión de usuarios 16
Acceso denegado a objetos seleccionados con el control de Tivoli Access Manager 16
Limitaciones conocidas 17
Utilización de Client Security Software con sistemas operativos Windows 17
Utilización de Client Security Software con aplicaciones de Netscape 17
El certificado del chip IBM Security Chip incorporado y los algoritmos de cifrado 17
Utilización de la protección de UVM para un ID de usuario de Lotus Notes 18
Limitaciones de User Configuration Utility 18
Mensajes de error 19
Tablas de resolución de problemas 19
Información de resolución de problemas de instalación 19
Información de resolución de problemas de Administrator Utility 20
Información de resolución de problemas de User Configuration Utility 22
Información de resolución de problemas específicos de ThinkPad 22

Información de resolución de problemas de Microsoft. 23
Información de resolución de problemas de Netscape 26
Información de resolución de problemas de certificados digitales 28
Información de resolución de problemas de Tivoli Access Manager. 29
Información de resolución de problemas de Lotus Notes 29
Información de resolución de problemas de cifrado 30
Información de resolución de problemas de dispositivos preparados para UVM 31

Apéndice A. Normativas de exportación de los EE.UU. para Client Security Software 33

Apéndice B. Normas para contraseñas y frases de paso 35
Normas para contraseñas de hardware 35
Normas para frases de paso de UVM 35

Apéndice C. Normas para la utilización de la protección de UVM para el inicio de sesión del sistema 37

Apéndice D. Avisos y marcas registradas 39
Avisos 39
Marcas registradas 40

Prefacio

Esta guía contiene información útil sobre la configuración de Client Security Software para utilizarlo con IBM Tivoli Access Manager.

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, Instalación del componente Client Security en un servidor Tivoli Access Manager″ contiene los requisitos previos e instrucciones para instalar el soporte de Client Security en el servidor Tivoli Access Manager.

El ″Capítulo 3, Configuración de los clientes de IBM″ contiene información sobre los requisitos previos e instrucciones para configurar los clientes de IBM para que utilicen los servicios de autenticación proporcionados por Tivoli Access Manager.

El ″Capítulo 4, “Resolución de problemas”″ contiene información útil para resolver problemas que podría experimentar mientras sigue las instrucciones proporcionadas en esta guía.

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

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

El ″Apéndice C, “**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 corporativos que van a utilizar Tivoli Access Manager versión 3.8 y versión 3.9 para gestionar los objetos de autenticación configurados mediante la política de seguridad de User Verification Manager (UVM) en un cliente de IBM.

Los administradores deben conocer los conceptos y procedimientos siguientes:

- Instalación y gestión de SecureWay Directory LDAP (Lightweight Directory Access Protocol)
- Procedimientos de instalación y configuración de Tivoli Access Manager Runtime Environment
- Gestión del espacio de objetos de Tivoli Access Manager

Utilización de esta guía

Utilice esta guía para configurar el soporte de Client Security para utilizarlo con Tivoli Access Manager. Esta guía acompaña a los manuales *Guía de instalación de Client Security Software*, *Guía del administrador de Client Security Software* y *Guía del usuario de Client Security Software*.

Esta guía y la demás documentación de Client Security puede bajarse desde el sitio Web de IBM en http://www.pc.ibm.com/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*. Después de haber configurado y puesto en marcha el servidor Tivoli Access Manager y de haber instalado Runtime Environment en el cliente, utilice las instrucciones de la *Guía de instalación de Client Security Software* para instalar Client Security Software en los clientes de IBM. Consulte el Capítulo 3, “Configuración de los clientes de IBM”, en la página 9 para obtener más información.

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

En este documento se hacen referencias a la *Guía del administrador de Client Security Software*. La *Guía del administrador de Client Security Software* contiene información sobre cómo configurar la autenticación de usuarios y la política de UVM para el cliente de IBM. Después de haber instalado Client Security Software, utilice la *Guía del administrador de Client Security Software* para configurar la autenticación de usuarios y la política de seguridad. Consulte el Capítulo 3, “Configuración de los clientes de IBM”, en la página 9 para obtener más información.

Información adicional

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

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. Instalación del componente Client Security en un servidor Tivoli Access Manager

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

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

Antes de poder utilizar Client Security con Tivoli Access Manager, debe estar instalado el componente Client Security de Tivoli Access Manager. Este componente puede bajarse del sitio Web de IBM en http://www.pc.ibm.com/ww/security/secdownload.html.

Requisitos previos

Antes de poder establecer una conexión entre el cliente de IBM y el servidor Tivoli Access Manager, deben estar instalados los componentes siguientes en el cliente de IBM:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

Para obtener información detallada sobre la instalación y utilización de Tivoli Access Manager, consulte la documentación proporcionada en el sitio Web http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Cómo bajar e instalar el componente Client Security

El componente Client Security está disponible para bajarlo gratuitamente del sitio Web de IBM.

Para bajar e instalar el componente Client Security en el servidor Tivoli Access Manager y el cliente de IBM, complete el procedimiento siguiente:

1. Utilizando la información del sitio Web, compruebe si su máquina tiene instalado el chip IBM Security Chip incorporado; para ello busque su número de modelo en la tabla de requisitos del sistema; después pulse **Continue** (Continuar).
2. Seleccione el botón de selección que se corresponda con su tipo de máquina y pulse **Continue** (Continuar).
3. Cree un ID de usuario, regístrese con IBM rellenando el formulario en línea y revise el Acuerdo de licencia; después pulse **Accept Licence** (Acepto la licencia).

   Se le redirigirá automáticamente a la página para bajarse Client Security.
4. Siga los pasos de esta página para instalar todos los controladores de dispositivo necesarios, los archivos readme, el software, los documentos de referencia y los programas de utilidad adicionales.

5. Instale Client Security Software completando el procedimiento siguiente:
   a. En el escritorio de Windows, pulse **Inicio > Ejecutar**.
   b. En el campo Ejecutar, escriba `d:\directorio\csec50.exe`, donde d:\directorio\ es la letra de la unidad y el directorio donde se encuentra el archivo.
   c. Pulse **Aceptar**.

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

      El asistente extraerá los archivos e instalará el software. Cuando se haya completado la instalación, se le dará la opción de reiniciar el sistema en ese momento o hacerlo más tarde.
   e. Seleccione el botón de selección adecuado y pulse **Aceptar**.
6. Cuando se reinicie el sistema, en el escritorio de Windows, pulse **Inicio > Ejecutar**.
7. En el campo Ejecutar, escriba `d:\directorio\TAMCSS.exe` , donde d:\directorio\ es la letra de la unidad y el directorio donde se encuentra el archivo, o pulse **Examinar** para localizar el archivo.
8. Pulse **Aceptar**.
9. Especifique una carpeta de destino y pulse **Unzip** (Descomprimir).

   El asistente extraerá los archivos en la carpeta especificada. Un mensaje indica si los archivos se han descomprimido satisfactoriamente.
10. Pulse **Aceptar**.

Adición de componentes Client Security en el servidor Tivoli Access Manager

El programa de utilidad pdadmin es una herramienta de línea de mandatos que el administrador puede utilizar para efectuar la mayoría de las tareas de administración de Tivoli Access Manager. La ejecución de varios mandatos permite al administrador utilizar un archivo que contenga varios mandatos de pdadmin para efectuar una tarea completa o una serie de tareas. La comunicación entre el programa de utilidad y Management Server (pdmgrd) está protegida sobre SSL. El programa de utilidad pdadmin se instala como parte del paquete Tivoli Access Manager Runtime Environment.

El programa de utilidad pdadmin acepta un argumento de nombre de archivo que identifique la ubicación de tal archivo, por ejemplo:

```
MSDOS>pdadmin [-a <usuario-admin >][-p <contraseña >]<nombrevía-archivo >
```

El mandato siguiente es un ejemplo de cómo crear el espacio de objetos IBM Solutions, las acciones de Client Security y las entradas ACL individuales en el servidor Tivoli Access Manager:

```
MSDOS>pdadmin -a director_seg -p contraseña C:\TAM_Add_ClientSecurity.txt
```

Consulte la *Tivoli Access Manager Base Administrator Guide* para obtener más información sobre el programa de utilidad pdadmin y su sintaxis de mandatos.

Establecimiento de una conexión segura entre el cliente de IBM y el servidor Tivoli Access Manager

El cliente de IBM debe establecer su propia identidad autenticada dentro del dominio seguro de Tivoli Access Manager para solicitar decisiones de autorización del Servicio de autorización de Tivoli Access Manager.

Se debe crear una identidad exclusiva para la aplicación en el dominio seguro de Tivoli Access Manager. Para que la identidad autenticada efectúe las comprobaciones de autenticación, la aplicación debe ser miembro del grupo remote-acl-users. Cuando la aplicación desee contactar uno de los servicios del dominio seguro, primero debe iniciar una sesión en éste.

El programa de utilidad svrsslcfg permite a las aplicaciones IBM Client Security comunicarse con Tivoli Access Manager Management Server y Authorization Server.

El programa de utilidad svrsslcfg efectúa las tareas siguientes:

- Crea una identidad de usuario para la aplicación. Por ejemplo, UsuarioDemo/NOMBRESISTPPAL
- Crea un archivo de claves de SSL para ese usuario. Por ejemplo, UsuarioDemo.kdb y UsuarioDemo.sth
- Añade el usuario al grupo remote-acl-users

Se necesitan los parámetros siguientes:

- **-f archivo_cfg**: vía de acceso y nombre del archivo de configuración, utilice TAMCSS.conf
- **-d dir_bdc**: el directorio que contiene los archivos de la base de datos del conjunto de claves para el servidor.
- **-n nombre_servidor**: el nombre de usuario de Windows/UVM real del usuario que va a ser el cliente de IBM.
- **-P contraseña_admin**: la contraseña del administrador de Tivoli Access Manager.
- **-s tipo_servidor**: debe especificarse como ″remote″.
- **-S contraseña_servidor**: la contraseña para el usuario recién creado. Este parámetro es necesario.
- **-r núm_puerto**: establece el número de puerto de escucha para el cliente de IBM. Este es el parámetro especificado en la variable de puerto del servidor SSL para Tivoli Access Manager Management Server de Tivoli Access Manager Runtime.
- **-e duración_contraseña**: establece el período de caducidad de la contraseña en número de días.

Para establecer una conexión segura entre el cliente de IBM y el servidor Tivoli Access Manager, complete el procedimiento siguiente:

1. Cree un directorio y mueva el archivo TAMCSS.conf al directorio nuevo.

   Por ejemplo, `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Ejecute svrsslcfg para crear el usuario.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <nombre_servidor> - s remote -S <contraseña_servidor> -P <contraseña_admin> -e 365 -r 199

Nota: sustituya <nombre_servidor> por el nombre de usuario de UVM y el nombre de sistema principal del que será el cliente de IBM. Por ejemplo: –n UsuarioDemo/MiNombreSistPpal. El nombre de sistema principal del cliente de IBM puede averiguarse escribiendo “hostname” en el indicador de MSDOS. El programa de utilidad svrsslcfg creará una entrada válida en el servidor Tivoli Access Manager y proporcionará un archivo de claves SSL exclusivo para la comunicación cifrada.

3. Ejecute svrsslcfg para añadir la ubicación de ivacld al archivo TAMCSS.conf.

   Por omisión, Tivoli Access Manager Authorization Server escucha en el puerto 7136. Esto puede verificarse mirando el parámetro tcp_req_port en la sección ivacld del archivo ivacld.conf en el servidor Tivoli Access Manager. Es importante que obtenga el nombre de sistema principal correcto de ivacld. Utilice el mandato pdadmin server list para obtener esta información. Los servidores se denominan: <nombre_servidor>-<nombre_sistppal>. A continuación hay un ejemplo de ejecución de pdadmin server list:

```
MSDOS> pdadmin server list ivacld-MiSistPpal.ibm.com
```

Después se utiliza el mandato siguiente para añadir una entrada de duplicación para el servidor ivacld mostrado abajo. Se asume que ivacld escucha en el puerto por omisión 7136.

```
svrsslcfg -add_replica  -f <vía acceso archivo config.> -h
<nombre_sistppal> MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h
MiSistPppal.ibm.com
```

Capítulo 3. Configuración de los clientes de IBM

Antes de poder utilizar Tivoli Access Manager para controlar los objetos de autenticación para los clientes de IBM, debe configurar cada cliente mediante Administrator Utility, un componente que se proporciona con Client Security Software. Esta sección contiene los requisitos previos y las instrucciones para configurar los clientes de IBM.

Requisitos previos

Asegúrese de que se instala el software siguiente en el cliente de IBM en el orden siguiente:

1. **Sistema operativo Microsoft Windows soportado.** Puede utilizar Tivoli Access Manager para controlar los requisitos de autenticación para los clientes de IBM que tengan Windows XP, Windows 2000 o Windows NT Workstation 4.0.
2. **Client Security Software versión 3.0 o posterior.** Después de instalar el software y habilitar el chip IBM Security Chip incorporado, puede utilizar Client Security Administrator Utility para configurar la autenticación de usuarios y editar la política de seguridad de UVM. Para obtener instrucciones completas sobre la instalación y utilización de Client Security Software, consulte la *Guía de instalación de Client Security Software* y la *Guía del administrador de Client Security Software*.

Definición de la información de configuración de Tivoli Access Manager

Después de haber instalado Tivoli Access Manager en el cliente local, puede definir la información de configuración de Access Manager mediante Administrator Utility, un componente de software que se proporciona con Client Security Software. La información de configuración de Access Manager consta de los valores siguientes:

- Selección de la vía de acceso completa al archivo de configuración
- Selección del intervalo de renovación de la antememoria local

Para definir la información de configuración de Tivoli Access Manager en el cliente de IBM, complete el procedimiento siguiente:

1. Pulse **Inicio > Configuración > Panel de control > IBM Client Security Subsystem**.
2. Escriba la contraseña del administrador y pulse **Aceptar**.

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

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
4. Pulse el recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**.
5. En el área Información de configuración de Tivoli Access Manager, seleccione la vía de acceso completa al archivo de configuración TAMCSS.conf. Por ejemplo, `C:\TAMCSS\TAMCSS.conf`

   Tivoli Access Manager debe estar instalado en el cliente para que esta área esté disponible.
6. Pulse el botón **Política de aplicaciones**.

7. Pulse el botón **Editar política**.

   Se muestra la pantalla Entre la contraseña del administrador.
8. Escriba la contraseña del administrador en el campo proporcionado y pulse **Aceptar**.

   Se muestra la pantalla Política de IBM UVM.
9. Seleccione las acciones que desea que controle Tivoli Access Manager en el menú desplegable Acciones.
10. Seleccione el recuadro de selección Access Manager controla el objeto seleccionado para que aparezca una marca de selección en él.
11. Pulse el botón **Aplicar**.

    Estos cambios tendrán lugar en la próxima renovación de la antememoria. Si desea que los cambios tengan lugar inmediatamente, pulse el botón **Renovar antememoria local**.

Establecimiento y utilización de la característica de antememoria local

Después de seleccionar el archivo de configuración de Tivoli Access Manager, puede establecerse el intervalo de 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 planificar una renovación automática de la antememoria local en incrementos de meses (0-12) o días (0-30).

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

1. Pulse **Inicio > Programas > Programas de utilidad de Client Security Software > Administrator Utility**.
2. Escriba la contraseña de hardware y pulse **Aceptar**.

   Se abre la ventana Administrator Utility. Para obtener información completa sobre la utilización de Administrator Utility, consulte la *Guía del administrador de Client Security Software*.
3. En Administrator Utility, pulse el botón **Configurar soporte de aplicaciones y políticas**.

   Se mostrará la pantalla Modificar la configuración de políticas de Client Security.
4. Efectúe una de las acciones siguientes:
   - Para renovar la antememoria local ahora, pulse **Renovar antememoria local**.
   - Para establecer la cadencia de renovación automática, escriba el número de meses (0-12) y días (0-30) en los campos proporcionados y pulse **Renovar antememoria local**. Se renovará la antememoria local y se actualizará la fecha de caducidad del archivo para indicar la fecha en la que se efectuará la próxima renovación automática.

Habilitación de Tivoli Access Manager para controlar los objetos del cliente de IBM

La política de UVM se controla mediante un archivo de políticas globales. El archivo de políticas globales, llamado archivo de políticas de UVM, contiene requisitos de autenticación para acciones que se efectúan en el sistema cliente de IBM, como iniciar una sesión en el sistema, quitar el protector de pantalla o firmar los mensajes de correo electrónico.

Antes de poder habilitar Tivoli Access Manager para controlar los objetos de autenticación para un cliente de IBM, utilice el editor de política de UVM para editar el archivo de políticas de UVM. El editor de política de UVM forma parte de Administrator Utility.

Importante: si se habilita Tivoli Access Manager para que controle un 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.

Edición de una política local de UVM

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

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. Sólo los usuarios que se hayan añadido a UVM pueden utilizar el editor de política de UVM.

Nota: si establece que la política de UVM necesite huellas dactilares para una objeto 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.

Para iniciar 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 Modificar la configuración de políticas de Client Security.
2. Pulse el botón **Editar política**.

   Se muestra la pantalla Entre la contraseña del administrador.
3. Escriba la contraseña del administrador en el campo proporcionado y pulse **Aceptar**.

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

   Entre los ejemplos de acciones válidas 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.
5. Para cada objeto que seleccione, tiene que seleccionar **Tivoli Access Manager controla el objeto seleccionado** para habilitar Tivoli Access Manager para ese objeto.

   Importante: si se habilita Tivoli Access Manager para que controle un objeto, se da el control del objeto al espacio de objetos de Tivoli Access Manager. Si posteriormente desea volver a establecer el control local sobre ese objeto, deberá reinstalar Client Security Software.

   Nota: mientras edita la política de UVM, puede ver información sobre el resumen de políticas pulsando **Resumen de políticas**.
6. Pulse **Aplicar** para guardar los cambios.

7. Pulse **Aceptar** para 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 4. 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.

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).

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)

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.

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

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: 59P7651

(1P) P/N: 59P7651