Soluciones IBM® Client Security

Utilización de Client Security Software Versión 5.3 con Tivoli® Access Manager

Soluciones IBM® Client Security

Utilización de Client Security Software Versión 5.3 con Tivoli® Access Manager

Primera edición (mayo de 2004)

Antes de utilizar esta información y el producto al que da soporte, no olvide leer el Apéndice A, “Normativas de exportación de los EE.UU. para Client Security Software”, en la página 39 y el Apéndice D, “**Avisos y marcas registradas**”, en la página 47.

Este manual es la traducción del original inglés *IBM® Client Security Solutions, Using Client Security Software Version 5.3 with Tivoli® Access*.

Contenido

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

El ″Apéndice C, “**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 3.9 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/us/security/index.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 13 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 13 para obtener más información.

Información adicional

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

Capítulo 1. Introducción

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

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

IBM Embedded Security Subsystem

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

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

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

El chip IBM Security Chip incorporado

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

IBM Embedded Security Subsystem soporta:

- Operaciones PKI RSA3, como cifrado para información confidencial y firmas digitales para autenticación
- Generación de claves RSA
- Generación de números seudo-aleatorios
- Cálculo de funciones RSA en 200 milisegundos
- Memoria EEPROM para el almacenamiento de pares de claves RSA
- Todas las funciones TCPA definidas en la especificación Vs. 1.1

- Comunicación con el procesador principal a través del bus LPC (Low Pin Count)

IBM Client Security Software

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

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

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

Relación entre contraseñas y claves

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

Contraseña del administrador

La contraseña del administrador se utiliza para autenticar al administrador en IBM Embedded Security Subsystem. Esta contraseña, que debe tener una longitud de

ocho caracteres, se mantiene y autentica dentro de los límites del hardware del subsistema de seguridad incorporado. Una vez autenticado, el administrador puede realizar las acciones siguientes:

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

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

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

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

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

Claves públicas y privadas de hardware

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

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

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

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

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

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

Claves públicas y privadas del administrador

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

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

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

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

Archivador ESS

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

Claves públicas y privadas del usuario

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

Jerarquía de intercambio de claves de IBM

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

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

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

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

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

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

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

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

importante tener en cuenta que cada sistema tendrá una clave pública y privada de hardware exclusivas. La posibilidad de números aleatorios de IBM Embedded Security Subsystem garantiza que cada par de claves de hardware sea estadísticamente único.

Características PKI (Public Key Infrastructure) de CSS

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

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

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

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

Capítulo 2. 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/us/security/index.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 guía *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 Embedded 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. Pulse el botón **Política de aplicaciones**.
6. 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.

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 en el menú desplegable Acciones las acciones que desea que controle Tivoli Access Manager.
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 > Configuración > Panel de control > IBM Embedded Security Subsystem**.
2. Escriba la contraseña del administrador 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** y después pulse el botón **Política de aplicaciones**.

   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** y después pulse el botón **Política de aplicaciones**.

   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

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

Funciones del administrador

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

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

Autorización de los usuarios

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

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

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

Supresión de usuarios

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

Establecimiento de una contraseña del administrador del BIOS (ThinkCentre)

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

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

Atención:

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

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

Para establecer una contraseña del administrador del BIOS:

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

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

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

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

Establecimiento de una contraseña del supervisor (ThinkPad)

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

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

Atención:

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

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

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

Ejemplo 1

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

   Se abre el menú principal del programa Setup Utility.
3. Seleccione **Password** (Contraseña).
4. Seleccione **Supervisor Password** (Contraseña del supervisor).
5. Escriba la contraseña y pulse Intro.
6. Escriba la contraseña de nuevo y pulse Intro.

7. Pulse **Continue** (Continuar).
8. Pulse F10 para guardar y salir.

Ejemplo 2

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

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

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

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

Protección de la contraseña del administrador

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

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

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

Atención:

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

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

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

   Se abre el menú principal del programa Setup Utility.

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

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

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

Atención:

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

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

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

Limitaciones o problemas conocidos de CSS Versión 5.2

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

Limitaciones de itinerancia

Utilización de un servidor de itinerancia CSS

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

Utilización de IBM Security Password Manager en un entorno de itinerancia

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

de la red de itinerancia. Por tanto, si un usuario ya ha iniciado la sesión en un sistema, debe cerrar la sesión e iniciar la sesión de nuevo antes de que estén disponibles nuevas entradas en la red de itinerancia.

Retardo de renovación de certificado e itinerancia de Internet Explorer

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

Contraseña de Lotus Notes e itinerancia de credenciales

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

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

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

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

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

Limitaciones de las tarjetas de identificación por contacto

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

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

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

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

Soporte de tarjeta de identificación por contacto y Cisco LEAP

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

Soporte de software Ensure

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

Restauración de las claves

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

Nombres de usuario local y de dominio

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

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

Reinstalación del software de huellas dactilares Targus

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

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

Frase de paso del supervisor del BIOS

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

Utilización de Netscape 7.x

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

Utilización de un disquete para archivar

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

Limitaciones de las smart cards

Registro de smart cards

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

Autenticación de smart cards

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

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

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

Limitaciones de los usuarios limitados de Windows XP

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

Otras limitaciones

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

Utilización de Client Security Software con sistemas operativos Windows

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

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

Utilización de Client Security Software con aplicaciones de Netscape

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

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

- SHA-1
- MD5

Certificado de IBM Embedded Security Subsystem y los algoritmos de cifrado

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

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

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

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

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

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

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

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

Limitaciones de User Configuration Utility

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

Windows XP Professional

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

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

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

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

Windows XP Home

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

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

Limitaciones de Tivoli Access Manager

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

Mensajes de error

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

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

Tablas de resolución de problemas

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

Información de resolución de problemas de instalación

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

Síntoma del problema	**Posible solución**
Se muestra un mensaje de error durante la instalación del software	**Acción**
Cuando instala el software se muestra un mensaje que pregunta si desea eliminar la aplicación seleccionada y todos sus componentes.	Pulse **Aceptar** para salir de la ventana. Comience el proceso de instalación de nuevo para instalar la nueva versión de Client Security Software.
Durante la instalación se muestra un mensaje indicando que debe actualizar o eliminar el programa.	Efectúe una de las acciones siguientes: • Si está instalada una versión anterior a Client Security Software 5.0, seleccione **Eliminar** y borre la información del subsistema de seguridad mediante el programa IBM BIOS Setup Utility. • En caso contrario, seleccione **Actualizar** y continúe con la instalación.
El acceso de instalación se ha denegado debido a una contraseña de administrador desconocida	**Acción**
Al instalar el software en un cliente de IBM con IBM Embedded Security Subsystem habilitado, la contraseña del administrador para IBM Embedded Security Subsystem es desconocida.	Borre la información del subsistema de seguridad para continuar con la instalación.

Información de resolución de problemas de Administrator Utility

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

Síntoma del problema	**Posible solución**
El botón Siguiente no está disponible después de entrar y confirmar la frase de paso de UVM en Administrator Utility	**Acción**
Cuando se añaden usuarios a UVM, puede que el botón **Siguiente** no esté disponible después de entrar y confirmar la frase de paso de UVM en Administrator Utility.	Pulse el elemento **Información** en la barra de tareas de Windows y continúe el procedimiento.
Se muestra un mensaje de error al cambiar la clave pública del administrador	**Acción**
Cuando borra la información de IBM Embedded Security Subsystem y después restaura el archivador de claves, puede que aparezca un mensaje de error si cambia la clave pública del administrador.	Añada los usuarios a UVM y solicite nuevos certificados, si procede.
Se muestra un mensaje de error al intentar recuperar una frase de paso de UVM	**Acción**

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

Información de resolución de problemas de User Configuration Utility

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

Síntoma del problema	Posible solución
Los usuarios limitados no pueden realizar ciertas funciones de User Configuration Utility en Windows XP Professional	**Acción**

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

Información de resolución de problemas específicos de ThinkPad

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

Síntoma del problema	Posible solución
Se muestra un mensaje de error al intentar efectuar una función del administrador de Client Security	**Acción**
Aparece un mensaje de error después de intentar efectuar una función del administrador de Client Security.	La contraseña del supervisor del ThinkPad debe estar inhabilitada para efectuar ciertas funciones del administrador de Client Security. Para inhabilitar la contraseña del supervisor, complete el procedimiento siguiente: 1. Pulse F1 para acceder a IBM BIOS Setup Utility. 2. Entre la contraseña actual del supervisor. 3. Entre una contraseña del supervisor en blanco y confirme una contraseña en blanco. 4. Pulse Intro. 5. Pulse F10 para guardar y salir.
Un sensor de huellas dactilares preparado para UVM diferente no funciona correctamente	**Acción**

Síntoma del problema	Posible solución
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.
Client Security no funciona correctamente para un usuario inscrito en UVM	**Acción**
Es posible que el usuario cliente inscrito en UVM haya cambiado su nombre de usuario de Windows. Si ocurre eso, se perderá toda la funcionalidad de Client Security.	Vuelva a inscribir el nombre de usuario nuevo en UVM y solicite todas las credenciales nuevas.
Nota: en Windows XP, los usuarios inscritos en UVM cuyo nombre de usuario de Windows se haya cambiado previamente, no serán reconocidos por UVM. Esta limitación se produce incluso si el nombre de usuario de Windows se cambió antes de instalar Client Security Software.	
Problemas al leer correo electrónico cifrado utilizando Outlook Express	**Acción**
El correo electrónico cifrado no puede descifrarse debido a las diferencias en los niveles de cifrado de los navegadores Web utilizados por el remitente y el destinatario.	Compruebe lo siguiente: 1. El nivel de cifrado para el navegador Web que utiliza el remitente es compatible con el nivel de cifrado del navegador Web que utiliza el destinatario. 2. El nivel de cifrado para el navegador Web es compatible con el nivel de cifrado proporcionado por el firmware de Client Security Software.
Problemas al utilizar un certificado desde una dirección que tiene asociados varios certificados	**Acción**

Síntoma del problema	Posible solución
Outlook Express puede listar varios certificados asociados con una sola dirección de correo electrónico y algunos de esos certificados pueden quedar invalidados. Un certificado queda invalidado si la clave privada asociada con el certificado ya no existe en IBM Embedded Security Subsystem del sistema del remitente donde se generó el certificado.	Pida al destinatario que reenvíe su certificado digital; después seleccione ese certificado en la libreta de direcciones de Outlook Express.
Mensaje de anomalía al intentar firmar digitalmente un mensaje de correo electrónico	**Acción**
Si el redactor de un mensaje de correo electrónico intenta firmarlo digitalmente cuando el redactor aún no tiene un certificado asociado con su cuenta de correo electrónico, se muestra un mensaje de error.	Utilice los valores de seguridad en Outlook Express para especificar que se asocie un certificado con la cuenta de usuario. Consulte la documentación proporcionada para Outlook Express para obtener más información.
Outlook Express (128 bits) sólo cifra mensajes de correo electrónico con el algoritmo 3DES	**Acción**
Cuando se envía correo electrónico cifrado entre clientes que utilicen Outlook Express con la versión de 128 bits de Internet Explorer 4.0 ó 5.0, sólo puede utilizarse el algoritmo 3DES.	Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con Outlook Express.
Los clientes Outlook Express devuelven mensajes de correo electrónico con un algoritmo diferente	**Acción**
Un mensaje de correo electrónico cifrado con el algoritmo RC2(40), RC2(64) o RC2(128) es enviado desde un cliente que utiliza Netscape Messenger a un cliente que utiliza Outlook Express (128 bits). Un mensaje de correo electrónico devuelto desde el cliente Outlook Express se cifra con el algoritmo RC2(40).	No se precisa ninguna acción. Una petición de cifrado RC2(40), RC2(64) o RC2(128) procedente de un cliente Netscape a un cliente Outlook Express (128 bits) siempre se devuelve al cliente Netscape con el algoritmo RC2(40). Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con su versión de Outlook Express.
Se muestra un mensaje de error al utilizar un certificado en Outlook Express después de una anomalía de una unidad de disco duro	**Acción**
Se pueden restaurar los certificados utilizando la característica de restauración de claves en Administrator Utility. Es posible que algunos certificados, como los certificados gratuitos proporcionados por VeriSign, no puedan ser restaurados después de una restauración de claves.	Después de restaurar las claves, efectúe una de las acciones siguientes: • obtenga nuevos certificados • registre la autoridad de certificados de nuevo en Outlook Express
Outlook Express no actualiza el nivel de cifrado asociado con un certificado	**Acción**

Síntoma del problema	Posible solución
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 después pulse el botón **Enviar** una vez.
Se muestra un mensaje de error al solicitar un certificado	**Acción**
Cuando utiliza Internet Explorer, es posible que reciba un mensaje de error si solicita un certificado que utiliza el CSP de IBM Embedded Security Subsystem.	Solicite el certificado digital de nuevo.

Información de resolución de problemas de Netscape

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

Síntoma del problema	Posible solución
Problemas al leer correo electrónico cifrado	**Acción**
El correo electrónico cifrado no puede descifrarse debido a las diferencias en los niveles de cifrado de los navegadores Web utilizados por el remitente y el destinatario.	Compruebe lo siguiente: 1. El nivel de cifrado para el navegador Web que utiliza el remitente es compatible con el nivel de cifrado del navegador Web que utiliza el destinatario. 2. El nivel de cifrado para el navegador Web es compatible con el nivel de cifrado proporcionado por el firmware de Client Security Software.

Síntoma del problema	Posible solución
Mensaje de anomalía al intentar firmar digitalmente un mensaje de correo electrónico	**Acción**
Si no se ha seleccionado el certificado de IBM Embedded Security Subsystem en Netscape Messenger y el redactor de un mensaje de correo electrónico intenta firmar el mensaje con el certificado, se muestra un mensaje de error.	Utilice los valores de seguridad de Netscape Messenger para seleccionar el certificado. Cuando se abra Netscape Messenger, pulse el icono de seguridad en la barra de herramientas. Se abre la ventana Información sobre seguridad. Pulse **Messenger** en el panel izquierdo y después seleccione el **Certificado del chip IBM Security Chip incorporado**. Consulte la documentación proporcionada por Netscape para obtener más información.
Se devuelve un mensaje de correo electrónico al cliente con un algoritmo diferente	**Acción**
Un mensaje de correo electrónico cifrado con el algoritmo RC2(40), RC2(64) o RC2(128) es enviado desde un cliente que utiliza Netscape Messenger a un cliente que utiliza Outlook Express (128 bits). Un mensaje de correo electrónico devuelto desde el cliente Outlook Express se cifra con el algoritmo RC2(40).	No se precisa ninguna acción. Una petición de cifrado RC2(40), RC2(64) o RC2(128) procedente de un cliente Netscape a un cliente Outlook Express (128 bits) siempre se devuelve al cliente Netscape con el algoritmo RC2(40). Consulte a Microsoft la información actual sobre los algoritmos de cifrado utilizados con su versión de Outlook Express.
No se puede utilizar un certificado digital generado por IBM Embedded Security Subsystem	**Acción**
El certificado digital generado por IBM Embedded Security Subsystem no está disponible para utilizarlo.	Compruebe que se ha escrito la frase de paso de UVM correcta cuando se abrió Netscape. Si escribe la frase de paso de UVM incorrecta, se muestra un mensaje de error indicando una anomalía de autenticación. Si pulsa **Aceptar**, se abre Netscape, pero no podrá utilizar el certificado generado por IBM Embedded Security Subsystem. Debe salir y volver a abrir Netscape y después escribir la frase de paso de UVM correcta.
Los certificados digitales nuevos del mismo remitente no se sustituyen dentro de Netscape	**Acción**
Cuando se recibe más de una vez un correo electrónico firmado digitalmente por el mismo remitente, el primer certificado digital asociado con el correo electrónico no se sobrescribe.	Si recibe varios certificados de correo electrónico, sólo un certificado es el certificado por omisión. Utilice las características de seguridad de Netscape para suprimir el primer certificado y después vuelva a abrir el segundo certificado o pida al remitente que envíe otro correo electrónico firmado.
No se puede exportar el certificado de IBM Embedded Security Subsystem	**Acción**

Síntoma del problema	Posible solución
El certificado de IBM Embedded Security Subsystem no puede exportarse en Netscape. La característica de exportación de Netscape puede utilizarse para hacer copias de seguridad de los certificados.	Vaya a Administrator Utility o User Configuration Utility para actualizar el archivador de claves. Cuando actualiza el archivador de claves, se crean copias de todos los certificados asociados con IBM Embedded Security Subsystem.
Se muestra un mensaje de error al intentar utilizar un certificado restaurado después de una anomalía de una unidad de disco duro	**Acción**
Se pueden restaurar los certificados utilizando la característica de restauración de claves en Administrator Utility. Es posible que algunos certificados, como los certificados gratuitos proporcionados por VeriSign, no puedan ser restaurados después de una restauración de claves.	Después de restaurar las claves, obtenga un certificado nuevo.
Se abre el agente de Netscape y produce un error en Netscape	**Acción**
Se abre el agente de Netscape y se cierra Netscape.	Desactive el agente de Netscape.
Netscape se retarda si intenta abrirlo	**Acción**
Si añade el módulo PKCS#11 de IBM Embedded Security Subsystem y después abre Netscape, puede producirse un pequeño retardo antes de que se abra Netscape.	No se precisa ninguna acción. Este mensaje es sólo informativo.

Información de resolución de problemas de certificados digitales

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

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

Información de resolución de problemas de Tivoli Access Manager

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

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

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

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

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

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

Apéndice B. Información sobre contraseñas y frases de paso

Este apéndice contiene información sobre contraseñas y frases de paso.

Normas para contraseñas y frases de paso

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

Normas para contraseñas del administrador

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

Las normas siguientes se aplican a la contraseña del administrador:

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

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

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

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

Normas para frases de paso de UVM

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

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

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

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

  Por ejemplo, si se establece que son ″6″ los caracteres permitidos, 1234567xxx es una contraseña no válida.
- Establecer un número mínimo de caracteres numéricos permitidos (sí, 1)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Intentos incorrectos

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

Número de intentos erróneos en sistemas TCPA y no TCPA

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

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

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

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

Restablecimiento de una frase de paso

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

Restablecimiento de una frase de paso de forma remota

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

- **Administradores**

  Un administrador remoto debe hacer lo siguiente:

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

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

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

- **Usuarios**

  El usuario debe hacer lo siguiente:

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

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

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

Restablecimiento de una frase de paso de forma manual

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

Apéndice C. 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 de 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.