Soluciones IBM® Client Security

Guía del administrador de Client Security Software Versión 5.3

Soluciones IBM® Client Security

Guía del administrador de Client Security Software Versión 5.3

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 87 y el Apéndice D, "**Avisos y marcas registradas**", en la página 95.

Este manual es la traducción del original inglés *IBM® Client Security Solutions, Client Security Software Version 5.3 Administrator's Guide*.

Contenido

Prefacio

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

Esta guía está organizada de la forma siguiente:

El ″Capítulo 1, “Introducción”″ contiene una visión general de las aplicaciones y componentes incluidos en el software, así como una descripción de las características PKI (Public Key Infrastructure).

El ″Capítulo 2, “Cifrado y descifrado de archivos y carpetas”″ contiene información sobre cómo utilizar IBM Client Security Software para proteger los archivos y carpetas confidenciales.

El ″Capítulo 3, “Itinerancia de credenciales de CSS”″ contiene información sobre cómo configurar una red de itinerancia de credenciales de CSS, registrar un cliente itinerante, autorizar e importar usuarios, sincronizar datos del usuario y restaurar una red de itinerancia.

El ″Capítulo 4, “Cómo utilizar Client Security Software”″ contiene ejemplos sobre cómo utilizar los componentes proporcionados por Client Security Software para configurar las características de seguridad que necesitan los usuarios clientes de IBM.

El ″Capítulo 5, “Autorización de los usuarios”″ contiene información sobre la autenticación de usuarios cliente, incluido cómo autorizar y eliminar usuarios en User Verification Manager (UVM).

El ″Capítulo 6, “Después de haber autorizado a los usuarios con UVM”″ contiene instrucciones informativas sobre cómo configurar la protección de UVM para el inicio de sesión del sistema operativo, cómo utilizar la protección de UVM para Lotus Notes y cómo utilizar Client Security Software con aplicaciones de Netscape.

El ″Capítulo 7, “Trabajo con la política de UVM”″ contiene instrucciones sobre cómo editar una política local de UVM, utilizar la política de UVM para un cliente remoto y cambiar la contraseña para un archivo de políticas de UVM.

El ″Capítulo 8, “Otras funciones para el administrador de seguridad”″ contiene instrucciones sobre cómo utilizar Administrator Utility para cambiar la ubicación del archivador de claves, restaurar las claves desde el archivador, recuperar una frase de paso de UVM y habilitar o inhabilitar el chip IBM Security Chip incorporado.

El ″Capítulo 9, “Instrucciones para el usuario cliente”″ contiene instrucciones sobre las diferentes tareas que efectúa el usuario cliente con Client Security Software. Este capítulo incluye instrucciones sobre cómo utilizar la protección de inicio de sesión de UVM, el correo electrónico seguro y User Configuration Utility.

El ″Capítulo 10, “Resolución de problemas”″ contiene información útil para superar limitaciones y problemas conocidos que podría experimentar mientras sigue las instrucciones proporcionadas en esta guía.

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

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

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

El ″Apéndice D, “**Avisos y marcas registradas**”″ contiene avisos legales e información de marcas registradas.

A quién va dirigida esta guía

Esta guía va dirigida a los administradores de seguridad que vayan a:

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

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

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

Utilización de esta guía

Utilice esta guía para configurar la autenticación de usuarios y la política de seguridad de UVM para los clientes de IBM. Esta guía acompaña a los manuales *Guía de instalación de Client Security Software*, *Utilización de Client Security con Tivoli Access Manager* y *Guía del usuario de Client Security*. Esta guía y la demás documentación de Client Security puede bajarse del sitio Web de IBM en http://www.pc.ibm.com/us/security/secdownload.html.

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

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

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

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

Referencias a la *Guía del usuario de Client Security*

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

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

Información adicional

Puede obtener información adicional y actualizaciones de productos de seguridad, cuando estén disponibles, desde el sitio Web de IBM en http://www.pc.ibm.com/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. Cifrado y descifrado de archivos y carpetas

La tecnología de cifrado permite a los usuarios proteger los datos confidenciales contenidos en sus sistemas. Mediante el cifrado de un archivo se garantiza que nadie pueda acceder a la información del archivo cifrado sin cumplir previamente los requisitos de seguridad especificados. El cifrado de archivos también puede proteger los datos confidenciales de los archivos enviados a través de Internet o de una red.

IBM Client Security Software permite a los usuarios cifrar y descifrar archivos y carpetas confidenciales de las formas siguientes:

- **Cifrado de archivos individuales con el ″botón derecho″ mediante la aplicación Client Security Software.**

  Esta característica forma parte de la versión base bajada de IBM Client Security Software.
- **Cifrado transparente de archivos y carpetas, sobre la marcha, mediante el programa de utilidad Cifrado de archivos y carpetas de IBM.**

  Nota: es necesario bajar el programa de utilidad Cifrado de archivos y carpetas (FFE) de IBM para habilitar esta característica. Debe instalarse Client Security Software *antes* de instalar el programa de utilidad Cifrado de archivos y carpetas de IBM.

Cifrado con el botón derecho

La función básica de cifrado con el botón derecho de Client Security Software permite a los usuarios proteger los archivos confidenciales utilizando el botón derecho del ratón. No es necesario bajar ningún software adicional para utilizar esta función. Los archivos cifrados con esta función tendrán las características siguientes:

- Deberá descifrar manualmente el archivo cifrado cada vez que desee utilizarlo y, cuando termine, volver a cifrarlo manualmente para protegerlo de nuevo. Es necesario invocar la política de UVM cada vez que se descifra o cifra el archivo. Estos requisitos proporcionan un control manual robusto de las operaciones de cifrado y descifrado de los archivos seleccionados, pero esta protección tan rigurosa no es muy adecuada para usuarios que no desean proporcionar una contraseña, una huella dactilar o una Smart Card cada vez que utilizan un archivo cifrado.
- Los archivos se pueden enviar cifrados a una ubicación remota; sin embargo, sólo pueden descifrarse en el sistema que se ha utilizado para cifrarlos puesto que las claves utilizadas para cifrar los archivos son exclusivas del subsistema IBM Embedded Security Subsystem de dicho sistema.

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

Cifrado transparente sobre la marcha (cifrado FFE)

La característica de cifrado transparente sobre la marcha de Client Security Software se habilita bajando el programa de utilidad Cifrado de archivos y carpetas (FFE) de IBM, que está disponible en el sitio Web de IBM Client Security. FFE proporciona una forma de cifrado más adecuada y transparente que la característica básica de cifrado con el ″botón derecho″ de CSS. El cifrado de archivos y carpetas mediante FFE también puede invocarse mediante el botón derecho del ratón. Los archivos y carpetas cifrados mediante FFE tendrán las características siguientes:

- Sólo es necesario invocar la política de UVM durante el arranque. Esto proporciona una forma más adecuada de cifrado y descifrado de los archivos seleccionados porque *no* tiene que proporcionar una contraseña, una huella dactilar o una Smart Card cada vez que desea utilizar un archivo cifrado.
- Cuando una aplicación abre un archivo que está cifrado mediante el programa de utilidad Cifrado de archivos y carpetas, el archivo se descifra automáticamente. Cuando se guarda un archivo que ha sido cifrado mediante el programa de utilidad Cifrado de archivos y carpetas, el archivo se cifra automáticamente.
- Los archivos cifrados con el programa de utilidad Cifrado de archivos y carpetas (FFE) se pueden enviar a una ubicación remota; sin embargo, se enviarán descifrados.

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

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

Cualquier operación de Windows que acceda a un archivo en una carpeta protegida obtendrá acceso a los datos en formato descifrado. Esta característica hace que el cifrado sea más cómodo porque no es necesario descifrar un archivo cada vez que se utiliza o volver a cifrarlo cada vez que el programa termina con el archivo.

Estado del cifrado de las carpetas mediante FFE

El programa de utilidad Cifrado de archivos y carpetas permite a los usuarios proteger los archivos y carpetas confidenciales utilizando el botón derecho del ratón. La forma en la que el software protege un archivo y una carpeta difiere en función del modo en el que el archivo o carpeta se cifre inicialmente.

Una carpeta puede estar en uno de los estados siguientes:

- **Una carpeta desprotegida**

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

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

- **Protegida por el usuario actual**

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

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

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

- **Un padre de una carpeta protegida**

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

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

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

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

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

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

Consejos sobre el programa de utilidad Cifrado de archivos y carpetas

La información siguiente podría ser útil a la hora de efectuar ciertas operaciones del programa de utilidad FFE.

Protección en otras letras de unidad

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

Supresión de archivos y carpetas protegidos

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

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

Antes de actualizar desde la versión 2.0 o anterior del programa de utilidad FFE de IBM, baje y utilice la Herramienta de reparación de listas de control de accesos (ACL) del sitio Web de IBM Security. Este programa de utilidad de reparación debe utilizarse *antes* de desinstalar cualquier versión de FFE anterior a la 2.0. En caso contrario, el proceso de desinstalación podría fallar y dejar a los archivos afectados inaccesibles.

Antes de desinstalar el programa de utilidad IBM FFE

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

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

El programa de utilidad IBM FFE tiene las limitaciones siguientes:

Limitaciones al mover archivos y carpetas protegidos

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

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

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

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

Limitaciones al ejecutar aplicaciones

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

Limitaciones en la longitud de los nombres de vía de acceso

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

reorganice la estructura de la carpeta para reducir los niveles de profundidad o acorte los nombres de alguna carpeta o archivo.

Problemas al proteger una carpeta

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

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

Capítulo 3. Itinerancia de credenciales de CSS

La característica de itinerancia de credenciales de IBM Client Security Software permite utilizar las credenciales de usuario de UVM en sistemas habilitados para TCPA dentro de una red. Esta red, denominada red de itinerancia, mejora la flexibilidad de los usuarios y aumenta la disponibilidad de aplicaciones al permitirles trabajar fácilmente desde cualquier sistema de la red.

Requisitos de la red de itinerancia de credenciales de CSS

Una red de itinerancia de credenciales de CSS está formada por los componentes necesarios siguientes:

- Servidor de itinerancia
- Clientes itinerantes
- Una unidad de red correlacionada y compartida para almacenar los archivadores de usuarios de UVM

Nota: el servidor de itinerancia y los clientes itinerantes autorizados son simplemente sistemas habilitados para TCPA con contraseñas de administrador establecidas que tienen instalado IBM Client Security Software 5.1 o superior.

Definición del servidor de itinerancia

Para configurar una red de itinerancia de credenciales de CSS debe designar un sistema TCPA como *servidor* de itinerancia (llamado sistema A). Los otros sistemas, una vez registrados por el servidor de itinerancia, son *clientes* registrados de CSS autorizados. (El primer cliente registrado se denomina sistema B).

No hay que destacar nada especial acerca del sistema que designe como servidor de itinerancia. Puede utilizar cualquier sistema que forme parte de la red de itinerancia. El servidor de itinerancia es simplemente el sistema designado para establecer los sistemas en que "confía" la red de itinerancia. Después de que un sistema se registra con el servidor de itinerancia, todos los sistemas de la red confían en él.

Para configurar una red de itinerancia son necesarios dos pasos:

1. Configurar el sistema A (servidor) estableciendo las claves, el archivador y los usuarios itinerantes.
2. Registrar el sistema B y todos los demás sistemas como clientes itinerantes en la red de itinerancia de credenciales de CSS.

El servidor de itinerancia define la red de itinerancia de credenciales de CSS e inicia el proceso de registro de los clientes itinerantes, aunque el punto central de una red de itinerancia de credenciales de CSS es la unidad de red correlacionada en la que se almacenan los archivadores de usuarios. Este archivador es el lugar donde se almacenan todas las actualizaciones de las credenciales de usuario. El archivador *no* deberá estar situado en el servidor de itinerancia ni en ninguno de los clientes itinerantes. Después de inicializar los clientes de CSS, el servidor de itinerancia actúa como cualquier otro cliente registrado de CSS.

Configuración del servidor de itinerancia

Para configurar un servidor de itinerancia, complete el procedimiento siguiente:

1. En el sistema designado, inicie la Consola del administrador y pulse **Configurar itinerancia de credenciales**. O bien, si el sistema ya está configurado para itinerancia, seleccione **Volver a configurar este sistema como un servidor de itinerancia de CSS**, pulse **Siguiente** y, a continuación, pulse **Aceptar**.
2. Cree la carpeta `c:\roaming` en el sistema designado como servidor de itinerancia.
3. Inicie la Consola del administrador y pulse **Configurar itinerancia de credenciales**.
4. Seleccione **Configurar este sistema como un servidor de itinerancia de CSS** y pulse **Siguiente**.
5. Pulse **Configurar**.
6. Seleccione **Crear claves del archivador nuevas** y escriba la nueva carpeta de claves en el campo Carpeta de las claves del archivador, donde la carpeta de las claves del archivados se almacena en la carpeta `c:\roaming`.
7. Elija utilizar un par de claves existente o crear un nuevo par de claves y, a continuación, pulse **Siguiente**.
8. Entre la carpeta del archivador y pulse **Siguiente**.

   Nota: la carpeta del archivador y la carpeta de claves deben poder accederse desde otros sistemas que estén registrados para itinerancia (clientes itinerantes). El directorio `c:\roaming` debe ser una unidad de red correlacionada.

   Si el archivador tiene actualmente archivos, la página siguiente del asistente preguntará qué debe hacer con los archivos.
9. Pulse **Finalizar**.

Registro de clientes en el servidor de itinerancia

Para registrar un cliente itinerante en el servidor de itinerancia, complete el procedimiento siguiente:

1. Inmediatamente después de completar la configuración del servidor de itinerancia, aparece la pantalla Configuración de la red de itinerancia de credenciales. Seleccione **Habilitar registro de clientes** y pulse **Siguiente**.
2. Entre el nombre del usuario del sistema B con derechos de administrador que completará el registro de clientes.
3. Entre y confirme la contraseña de 8 caracteres que va a utilizar dicho usuario. No confunda este proceso con el de autorizar a un usuario para utilizar UVM, que se realiza más tarde.
4. Si desea registrar el cliente mediante User Configuration Utility, necesita crear un archivo de configuración del administrador para dicho usuario. Este proceso genera un archivo que es exclusivo para este usuario. Almacene este archivo en una ubicación a la que pueda acceder el usuario y el sistema B.

   Nota: no es necesario generar este archivo cuando se registra un cliente mediante Administrator Utility.
5. Entre la contraseña del administrador del sistema B y pulse **Siguiente**.
6. Si ha creado un archivo de configuración del administrador, guarde el archivo en una ubicación a la que pueda acceder el usuario y el sistema B.

Después de completar los procedimientos anteriores, el servidor de itinerancia estará configurado. Debe completarse el registro en cada cliente itinerante antes de que la red de itinerancia esté preparada para su utilización.

Finalización del proceso de registro de clientes itinerantes

Después de que la lista de sistemas fiables se ha registrado en el servidor de itinerancia, debe completar uno de los procedimientos siguientes en los sistemas cliente. El servidor de itinerancia debe estar en ejecución y conectado al archivador para que pueda completarse el proceso de registro de los clientes itinerantes.

Registro de un cliente itinerante mediante Administrator Utility

Para registrar un cliente itinerante mediante Administrator Utility, complete el procedimiento siguiente:

1. Pulse **Configuración de claves**.
2. Pulse **No** si se le pregunta si desea restaurar las claves desde el archivador.
3. Seleccione Registrar este sistema con un servidor de itinerancia de CSS y pulse **Siguiente**.
4. Entre la ubicación del archivador creado por el sistema A, escriba la contraseña de registro del sistema designada para este usuario en el sistema A y pulse **Siguiente**.

   Completar el registro lleva aproximadamente un minuto.

Registro de un cliente itinerante mediante User Configuration Utility

Para registrar un cliente itinerante mediante User Configuration Utility, complete el procedimiento siguiente:

1. En la pestaña Configuración del usuario, pulse **Registrarse con un servidor de itinerancia de CSS**.
2. Seleccione el archivo de configuración del administrador generado en el sistema A, escriba la contraseña de registro del sistema designada para este usuario en el sistema A y pulse **Siguiente**.
3. Entre la ubicación del archivador creado por el sistema A y pulse **Siguiente**.

   Completar el registro lleva aproximadamente un minuto.

Registro de un cliente itinerante mediante despliegue masivo (de forma silenciosa)

Para registrar un cliente itinerante mediante despliegue masivo, complete el procedimiento siguiente:

1. Cree el archivo `csec.ini`. Consulte la *Guía de instalación de Client Security Software* para obtener detalles sobre cómo crear un archivo .ini de CSS.
2. En la sección `csssetup` del archivo, añada `"enableroaming=1"`. Esto indica que el sistema deberá registrarse como cliente itinerante.
3. En la misma sección, añada la entrada `"username=OPTION"`. Hay tres opciones posibles para este valor:
   - **Opción 1: la serie `"[promptcurrent]"` - incluidos los corchetes.** Esta designación debería utilizarse si se ha generado en el servidor de itinerancia un archivo .dat para el usuario que tiene iniciada la sesión actualmente y el usuario actual conoce la contraseña de registro del sistema. Esta opción hace

que aparezca una ventana emergente para solicitar al usuario que entre la contraseña de registro del sistema (sysregpwd) antes del despliegue.

- **Opción 2: la serie "[current]" - incluidos los corchetes.** Esta designación debería utilizarse si se ha generado en el servidor un archivo .dat para el usuario que tiene iniciada la sesión actualmente. La sysregpwd se gestiona del modo que se describe en el paso siguiente.
- **Opción 3: un nombre de usuario real como "juan".** Si se utiliza ese nombre de usuario específico, el servidor de itinerancia debe haber generado previamente "juan.dat". La sysregpwd para este caso también se gestiona como se describe en el paso siguiente.

4. Si se utiliza la opción dos o tres anterior, deberá suministrarse otra entrada "sysregpwd=SYSREGPW". Esta es la contraseña de ocho dígitos de registro del sistema asociada con el usuario actual (si se implementa la opción dos) o del usuario designado (si se implementa la opción tres).
5. Para completar el registro del cliente, conecte el sistema al archivador configurado por el servidor de itinerancia. Este archivador se designa en el archivo csec.ini. La carpeta de claves establecida en el servidor de itinerancia de credenciales de CSS también se designa en el archivo csec.ini.
6. Cifre el archivo csec.ini mediante la Consola del administrador.

Ejemplos del archivo csec.ini

Los ejemplos siguientes muestran un archivo csec.ini y cómo cambia en función de la opción de itinerancia de credenciales que se seleccione. Estas opciones son las siguientes:

- **Sin valores de itinerancia.** Este archivo base no tiene habilitada la itinerancia de credenciales.
- **Opción de itinerancia 1.** Este archivo tiene habilitada la itinerancia con la opción 1 para el registro de clientes. El usuario actual debe presentar la contraseña de registro del sistema antes del despliegue.
- **Opción de itinerancia 2.** Este archivo tiene habilitada la itinerancia con la opción 2 para el registro de clientes. El usuario actual debe presentar el ID de usuario y la contraseña de registro del sistema designados en el archivo .ini.
- **Opción de itinerancia 3.** Este archivo tiene habilitada la itinerancia con la opción 3 para el registro de clientes. El usuario está designado en el archivo .ini. La contraseña de registro del sistema del usuario designado debe presentarse en el archivo .ini.

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

[CSSSetup]	**Opción 1** [CSSSetup]	**Opción 2** [CSSSetup]	Opción 3 [CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\nombre sistema\jgk, lugar en el que el sistema almacenó el par de claves en el servidor de itinerancia	kpl=c:\\nombre sistema\jgk, lugar en el que el sistema almacenó el par de claves en el servidor de itinerancia	kpl=c:\\nombre sistema\jgk, lugar en el que el sistema almacenó el par de claves en el servidor de itinerancia

kal=c:\jgk\archive pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\nombre sistema\archive, lugar en el que el sistema almacenó el archivador en el servidor de itinerancia pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\nombre sistema\archive, lugar en el que el sistema almacenó el archivador en el servidor de itinerancia pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\nombre sistema\archive, lugar en el que el sistema almacenó el archivador en el servidor de itinerancia pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0
clean=0	**enableroaming=1** **username=** **[promptcurrent]** clean=0	**enableroaming=1** **username=** **[current]** **sysregpwd=12345678** clean=0	**enableroaming=1** **username=** **juan** **sysregpwd=12345678** clean=0
[UVMEnrollment] enrollall=0 enrollusers=1 user1=juan user1uvmpw= q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays= 184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=juan user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=juan user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=juan user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184
[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0

Gestión de una red de itinerancia

El administrador de una red de itinerancia debe autorizar a los usuarios y gestionar el acceso de usuarios y clientes a la red. Esto puede incluir el importar un perfil de usuario, sincronizar los datos de usuario o añadir y eliminar usuarios y clientes, tareas rápidas y sencillas de realizar en una red de itinerancia de CSS. También podría implicar el restaurar la red de itinerancia, cambiar el par de claves del administrador o cambiar la ubicación del archivador.

Autorización de los usuarios

Después de completar los procedimientos anteriores, la red de itinerancia de credenciales de CSS queda configurada y los clientes itinerantes están registrados para itinerancia. Ahora se puede autorizar a los usuarios mediante Administrator Utility.

Sincronización de los datos de usuario

Los datos de cada usuario se almacenan en la ubicación del archivador. También se almacena una copia de los datos localmente en cada sistema que se haya utilizado de forma itinerante. Cuando se efectúan cambios, tales como obtener un certificado o cambiar una frase de paso, se actualizan los datos locales. Si el sistema está conectado al archivador, también se actualizan los datos del usuario. Cuando el usuario inicia una sesión en otro sistema, las actualizaciones se bajan automáticamente a ese sistema, siempre que también esté conectado al archivador.

Sin embargo, la conexión con el archivador no está siempre garantizada, por lo que a veces los datos de un usuario pueden ser diferentes entre los sistemas y el archivador. Si se cambian los datos de un usuario en un sistema que no esté conectado al archivador, los cambios no se reflejarán en el archivador y, en consecuencia, tampoco en otros sistemas. Una vez conectado el sistema al archivador, los cambios se actualizan en el archivador y después se resuelven todas las incoherencias en los datos de los otros sistemas conectados. No obstante, si se efectúan cambios en otro sistema que esté conectado al archivador antes de que el primer sistema que tenía cambios se conecte al archivador, se producirán incoherencias no corregibles en los datos. Los datos del archivador contienen cambios que no están presentes en el primer sistema, mientras que el sistema contiene cambios que no están en el archivador. Si ocurre esto, se notifica al usuario la existencia de dos configuraciones diferentes y se le solicita que elija la configuración que desee conservar, la local o la del archivador. Los cambios de configuración no elegidos, se perderán. Por tanto, es importante asegurarse de que cualquier cambio efectuado en la configuración de un usuario se actualiza en el archivador antes de hacer cambios en cualquier otro sistema.

Recuperación de una frase de paso perdida en un entorno de itinerancia

Cuando se pierde u olvida una frase de paso, el administrador puede restablecer la frase de paso del usuario en el servidor de itinerancia o en cualquier cliente registrado. Este cambio se actualizará en todos los sistemas de la red *excepto* en los sistemas que tengan habilitada la protección de inicio de sesión de UVM seguro en los que se haya importado el usuario. En estos casos, la actualización de la frase de paso *no* se reflejará en el sistema. Para poder tener acceso al sistema, el usuario necesitará un archivo de sobrescritura de contraseña y tendrá que completar el proceso de sobrescritura de contraseña.

Importación de un perfil de usuario

Se puede importar un perfil de usuario en un sistema nuevo de la red de itinerancia mediante Administrator Utility, User Configuration Utility o UVM GINA. Si desea importar un usuario que no tiene cuenta de usuario en el nuevo sistema, debe crear una cuenta de usuario de Windows mediante el Panel de control de Windows.

Nota: para importar un usuario en una red de itinerancia, el usuario debe autorizarse en otro sistema de la red de itinerancia.

Importación de un perfil de usuario mediante User Configuration Utility

Para importar un perfil de usuario en un sistema nuevo de la red de itinerancia mediante User Configuration Utility, inicie la sesión en el sistema con el usuario que desea importar y pulse **Inicio > Programas > Access IBM > IBM Client**

Security Software > Modificar los valores de seguridad y, a continuación, pulse **Importar configuración existente desde archivador** en la pestaña Configuración del usuario.

Importación de un perfil de usuario mediante Administrator Utility

Para importar un perfil de usuario en un sistema nuevo de la red de itinerancia mediante Administrator Utility, seleccione el usuario y después pulse **Autorizar**. Pulse **Sí** cuando se le pregunte si desea importar el usuario desde el archivador.

Importación de un perfil de usuario mediante UVM GINA

Se puede importar un perfil de usuario en un sistema nuevo de la red de itinerancia mediante UVM GINA. Este proceso comienza en la pantalla de inicio de sesión de UVM. Si un usuario no está aún autorizado para utilizar UVM en un sistema específico de la red, aparece un cuadro de mensaje preguntando si se desea importar el usuario desde el archivador.

Notas:

1. Si desea importar un usuario que no tiene cuenta de usuario en el nuevo sistema, debe crear una cuenta de usuario de Windows mediante el Panel de control de Windows antes de continuar.
2. Para acceder al archivador en el servidor de itinerancia, el directorio debe ser una unidad de red correlacionada.

Para importar un perfil de usuario en un sistema nuevo de la red de itinerancia mediante UVM en un sistema que ejecuta Windows 2000, complete el procedimiento siguiente:

1. Al iniciar la sesión, entre el nombre de usuario y la frase de paso de UVM del usuario que desea importar. Se muestra un mensaje que pregunta si desea importar el perfil de usuario desde el archivador.
2. Pulse **Sí** en el indicador para importar el usuario y pulse **Aceptar**.
3. Si la ubicación del archivador está en una unidad de red, pulse **Sí** en la solicitud que indica que se debe proporcionar un recurso compartido de red.
4. Entre la contraseña de Windows en la pantalla de inicio de sesión estándar de Windows. Aparece la solicitud de la vía de acceso del archivador.
5. Entre la vía de acceso de red del archivador.
6. Entre el nombre de usuario y contraseña para la vía de acceso de red.
7. Pulse **Aceptar**. Si la operación se completa correctamente, aparece un mensaje indicando que el perfil se ha importado satisfactoriamente.

Para importar un perfil de usuario en un sistema nuevo de la red de itinerancia mediante UVM en un sistema que ejecuta Windows XP, complete el procedimiento siguiente:

1. Al iniciar la sesión, entre el nombre de usuario y la frase de paso de UVM del usuario que desea importar. Se muestra un mensaje que pregunta si desea importar el perfil de usuario desde el archivador.
2. Pulse **Sí** en el indicador para importar el usuario y pulse **Aceptar**.
3. Si la ubicación del archivador está en una unidad de red, pulse **Sí** en la solicitud que indica que se debe proporcionar un recurso compartido de red.
4. En el indicador estándar de correlaciones de unidades de red de Windows, entre la vía de acceso de red del archivador.
5. Pulse **Finalizar**.

6. Entre el nombre de usuario y contraseña para la vía de acceso de red y pulse **Aceptar**. Si la operación se completa correctamente, aparece un mensaje indicando que el perfil se ha importado satisfactoriamente.

Nota: para importar un usuario en una red de itinerancia, el usuario debe autorizarse en otro sistema de la red de itinerancia.

Después de importar el perfil de usuario, la autenticación con UVM se basa en la política de seguridad del sistema. Los requisitos de seguridad para ese sistema deben haberse definido correctamente antes de que el usuario pueda iniciar una sesión.

Eliminación y reincorporación de usuarios en una red de itinerancia

Para eliminar un usuario de una red de itinerancia, el administrador de la red debe completar el procedimiento siguiente de la Consola del administrador:

1. Inicie el programa de utilidad Consola del administrador y entre la contraseña del administrador.
2. Pulse **Configurar itinerancia de credenciales**.
3. Seleccione **Eliminar usuarios de UVM y de la red de itinerancia de credenciales** y pulse **Siguiente**. Repita el número de veces que sea necesario.
4. Seleccione el usuario que desea eliminar y pulse **Eliminar**.

   Nota: una vez eliminado el usuario de la red, todas las credenciales pertenecientes al usuario se pierden para siempre.

No se puede autorizar a los usuarios eliminados para que utilicen UVM y la red de itinerancia hasta que el administrador de la red los reincorpore.

Para reincorporar un usuario en la red de itinerancia, el administrador de la red debe completar el procedimiento siguiente de la Consola del administrador:

1. Inicie el programa de utilidad Consola del administrador y entre la contraseña del administrador.
2. Pulse **Configurar itinerancia de credenciales**.
3. Seleccione **Reincorporar los usuarios eliminados** y pulse **Siguiente**.
4. Seleccione el usuario que desea reincorporar y pulse **Reincorporar**. Repita el número de veces que sea necesario.

   Una vez reincorporado el usuario, puede volver a ser autorizado para utilizar UVM. El reincorporar un usuario no le autoriza automáticamente a utilizar UVM.

Eliminación y reincorporación de clientes registrados en una red de itinerancia

Para eliminar un cliente registrado de una red de itinerancia, el administrador de la red debe completar el procedimiento siguiente de la Consola del administrador:

1. Inicie el programa de utilidad Consola del administrador y entre la contraseña del administrador.
2. Pulse **Configurar itinerancia de credenciales**.
3. Seleccione **Eliminar clientes registrados de la red de itinerancia de credenciales** y pulse **Siguiente**.

4. Seleccione el sistema que desea eliminar y pulse **Eliminar**. Repita el número de veces que sea necesario.

   Nota: una vez eliminado el cliente de la red, todas las credenciales basadas en la máquina pertenecientes al sistema se pierden para siempre.

Los clientes eliminados no pueden registrarse con el servidor de itinerancia de red hasta que no sean reincorporados por el administrador de la red.

Para reincorporar un cliente registrado en la red de itinerancia, el administrador de la red debe completar el procedimiento siguiente de la Consola del administrador:

1. Inicie el programa de utilidad Consola del administrador y entre la contraseña del administrador.
2. Pulse **Configurar itinerancia de credenciales**.
3. Seleccione **Reincorporar los clientes eliminados** y pulse **Siguiente**.
4. Seleccione el cliente que desea reincorporar y pulse **Reincorporar**. Repita el número de veces que sea necesario.

   Una vez reincorporado el cliente, puede registrarse con el servidor de itinerancia. El reincorporar un cliente no implica que se registre de nuevo automáticamente.

Nota: todos los usuarios cuyas credenciales estaban presentes en el sistema en el momento en que se eliminó el cliente, tendrán que importarlas de nuevo.

Restricción de acceso a clientes registrados en una red de itinerancia

En algunas ocasiones, puede que el administrador de la red desee permitir que algunos usuarios accedan a un cliente registrado concreto y restringir el acceso a otros usuarios.

Para gestionar los derechos de acceso del usuario, el administrador de la red debe completar el procedimiento siguiente de la Consola del administrador:

1. Inicie el programa de utilidad Consola del administrador y entre la contraseña del administrador.
2. Pulse **Configurar itinerancia de credenciales**.
3. Seleccione **Gestionar el acceso de usuario para los clientes registrados** y pulse **Siguiente**.
4. Seleccione el cliente registrado que desea gestionar en el recuadro **Seleccionar un sistema en la red de itinerancia de CSS**. Los usuarios que tienen acceso y los que no lo tienen se listan en los dos recuadros de lista.
5. Efectúe una de las acciones siguientes:
   - Para restringir el acceso a un usuario, seleccione el usuario en la lista **Usuarios con acceso** y pulse **Restringir**. Repita el número de veces que sea necesario.
   - Para otorgar acceso a un usuario restringido, seleccione el usuario en la lista **Usuarios sin acceso** y pulse **Permitir**. Repita el número de veces que sea necesario.

Las funciones de gestión de acceso de la red de itinerancia necesitan que se cree una nueva carpeta en el archivador. La nueva carpeta, llamada Protected, debe ser de escritura para el administrador de la red y de sólo lectura para el resto de

usuarios. Si los usuarios tuvieran acceso de escritura sobre esta carpeta, podrían reincorporarse ellos mismos manualmente o a sus sistemas.

Restauración de una red de itinerancia

En caso de una anomalía de software o hardware, podría necesitarse restaurar la red de itinerancia. Si el servidor de itinerancia ha sufrido daños o si los datos utilizados por CSS se han dañado en un cliente registrado, puede restaurar los datos mediante Administrator Utility del mismo modo que en un entorno que no tenga itinerancia. Si se produce un error o se borra la información de IBM Embedded Security Subsystem de un cliente registrado, el cliente debe volver a registrarse con el servidor de itinerancia. No se precisa ninguna otra acción.

Cambio del par de claves del administrador

No es recomendable cambiar el par de claves del administrador en una red de itinerancia.

Para cambiar el par de claves del administrador en una red de itinerancia, deben completarse los pasos siguientes para que el cambio se refleje en todos los sistemas de la red.

1. En el servidor de itinerancia, cambie el par de claves del administrador mediante Administrator Utility.
2. Vuelva a registrar todos los clientes en la red.
3. Siempre que se le pregunte, diga que desea conservar los archivos existentes.

Cambio de la carpeta del archivador

El cambio de la carpeta del archivador en un entorno de itinerancia es ligeramente distinto al de un entorno que no tenga itinerancia ya que todos los sistemas de la red acceden a la misma ubicación del archivador.

Para cambiar la carpeta del archivador en una red de itinerancia, complete el procedimiento siguiente:

1. Copie los archivos desde la carpeta del archivador anterior a la nueva utilizando el procedimiento siguiente:
   a. Inicie Administrator Utility y entre la contraseña del administrador.
   b. Pulse **Configuración de claves**.
   c. Seleccione Cambiar la ubicación del archivador y pulse **Siguiente**.
   d. Entre la nueva carpeta del archivador y pulse **Siguiente**.
   e. Pulse **Sí** cuando se le solicite copiar todos los archivos de la carpeta anterior en la nueva.
2. Actualice todos los demás sistemas de la red para que utilicen la nueva carpeta del archivador, mediante el procedimiento siguiente:
   a. Inicie Administrator Utility y entre la contraseña del administrador.
   b. Pulse **Configuración de claves**.
   c. Seleccione Cambiar la ubicación del archivador y pulse **Siguiente**.
   d. Entre la nueva carpeta del archivador y pulse **Siguiente**.
   e. Pulse **No** cuando se le solicite copiar todos los archivos de la carpeta anterior en la nueva.

Cifrado de archivos y carpetas (FFE)

La funcionalidad de Cifrado de archivos y carpetas no se ve afectada por un entorno de itinerancia. No obstante, las carpetas protegidas se gestionan por separado en cada sistema. De este modo, si un usuario A protege una carpeta en un sistema A, una carpeta con el mismo nombre en un sistema B, si la hubiese, no se protege a menos que el usuario la proteja activamente en el sistema B.

IBM Password Manager

Todas las contraseñas protegidas mediante IBM Password Manager están disponibles en todos los sistemas de la red de itinerancia.

Términos y definiciones de itinerancia

Los términos siguientes son útiles para comprender los conceptos y procedimientos relacionados con configurar una red de itinerancia:

Registro de clientes itinerantes
El proceso de registrar un sistema con el servidor de itinerancia.

Clientes itinerantes
Todos los sistemas TCPA en los que se confía en la red de itinerancia.

Servidor de itinerancia
El sistema TCPA utilizado para iniciar la red de itinerancia.

Contraseña de registro del cliente itinerante
La contraseña utilizada para registrar el sistema con el servidor de itinerancia.

Capítulo 4. Cómo utilizar Client Security Software

Los administradores pueden utilizar varios componentes proporcionados por Client Security Software para configurar las características de seguridad que requieren los usuarios clientes de IBM. Utilice los ejemplos siguientes como apoyo para planificar la política y configuración de Client Security. Por ejemplo, los usuarios de Windows 2000 y Windows XP pueden establecer la protección de UVM para el inicio de sesión del sistema que prohíbe a los usuarios no autorizados el inicio de sesión en el cliente de IBM.

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

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

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

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

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

      Nota: si establece las huellas dactilares como un requisito de autenticación que forma parte de la política de UVM para un cliente, cada usuario deberá registrar sus huellas dactilares.
4. Edite y guarde una política local de UVM en cada cliente que requiere autenticación para lo siguiente:
   - Iniciar una sesión en Windows

- Obtener un certificado digital
- Utilizar una firma digital para Outlook Express

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

Los usuarios cliente pueden efectuar ahora las tareas siguientes:

- Utilizar la protección de UVM para bloquear y desbloquear Windows.
- Solicitar un certificado digital y seleccionar Embedded Security Subsystem como el suministrador de servicio criptográfico asociado al certificado.
- Utilizar el certificado digital para cifrar mensajes de correo electrónico creados con Outlook Express.

Ejemplo 2 - Dos clientes de IBM con Windows 2000 que utilizan Lotus Notes

En este ejemplo, los dos clientes de IBM (cliente 1 y 2) tienen los dos instalado Windows 2000 y Lotus Notes. Dos usuarios requieren establecer la autenticación con UVM en el cliente 1; un usuario requiere establecer la autenticación con UVM en el cliente 2; ambos clientes requieren protección de inicio de sesión de UVM para el inicio de sesión de Windows. El administrador decide editar la política de UVM en el cliente 1 copiarla al cliente 2.

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

1. Instale el software en el cliente 1 y el 2. Dado que se utilizará la misma política de UVM, deberá utilizar la misma clave pública del administrador cuando instale el software en los dos clientes, el 1 y el 2. Lea el manual *Guía de instalación de Client Security Software* para obtener detalles sobre la instalación del software.
2. Configure la autenticación de usuarios con UVM para cada cliente. A continuación, efectúe lo siguiente:
   a. Autorice a los usuarios para UVM asignándolos una frase de paso de UVM. Dado que el cliente 1 tiene dos usuarios, debe repetir el proceso para autorizar usuarios para UVM hasta que hayan autorizado los dos usuarios.
   b. Configure la protección de inicio de sesión de UVM para el inicio de sesión de Windows en cada cliente.
3. Habilite el soporte de Lotus Notes de protección de UVM en ambos clientes.
4. Edite y guarde una política de UVM en el cliente 1 y, a continuación, cópiela en el cliente 2. La política de UVM requerirá la autenticación del usuario para borrar el protector de pantalla e iniciar la sesión de Lotus Notes y en Windows. Para obtener más detalles, consulte “Edición y utilización de la política de UVM” en la página 46.
5. Reinicie cada cliente con objeto de habilitar la protección de inicio de sesión de UVM para el inicio de sesión de Windows.
6. Informe a los usuarios cliente de las frases de paso de UVM y de la política que se ha establecido para cada cliente.

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

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

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

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

1. Instale el componente Client Security en el servidor Tivoli Access Manager. Para obtener detalles, consulte el manual *Utilización de Client Security con Tivoli Access Manager*.
2. Instale Client Security Software en todos los clientes. Dado que se utilizará una política de UVM, deberá utilizar la misma clave pública del administrador cuando instale el software en todos los clientes. Lea el manual *Guía de instalación de Client Security Software* para obtener detalles sobre la instalación del software.
3. Instale en cada cliente los sensores de huellas dactilares preparados para UVM y los productos de software asociados. Para obtener información sobre los productos preparados para UVM disponibles, vaya a la página http://www.pc.ibm.com/us/security/index.html en la World Wide Web.
4. Configure la autenticación de usuarios con UVM en cada cliente. Consulte “Eliminación de usuarios” en la página 33 para obtener detalles. A continuación, efectúe lo siguiente:
   a. Autorice a los usuarios para UVM asignándolos una frase de paso de UVM.
   b. Configure la protección de inicio de sesión de UVM para el inicio de sesión de Windows en cada cliente.
   c. Registre las huellas dactilares para cada usuario cliente. Si es necesaria la autenticación en clientes de IBM, todos los usuarios de ese cliente deberán registrar sus huellas dactilares.
5. Configure la información de configuración de Tivoli Access Manager en cada cliente. Para obtener detalles, consulte el manual *Utilización de Client Security con Tivoli Access Manager*.
6. Edite y guarde una política de UVM en uno de los clientes y a continuación cópiela en los otros clientes. Establezca la política de UVM de modo que Tivoli Access Manager pueda controlar los objetos de autenticación siguientes:
   - Iniciar una sesión en Windows
   - Obtener un certificado digital
   - Utilizar una firma digital para Outlook Express

Para obtener más detalles, consulte “Edición y utilización de la política de UVM” en la página 46.

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

Capítulo 5. Autorización de los usuarios

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

Autenticación de usuarios cliente

La autenticación de los usuarios finales en el nivel del cliente es una cuestión importante de la seguridad del sistema. Client Security Software proporciona la interfaz necesaria para gestionar la política de seguridad de un cliente de IBM. Esta interfaz forma parte del software de autenticación, User Verification Manager (UVM), que es el componente principal de Client Security Software.

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

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

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

Elementos de autenticación

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

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

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

Antes de autorizar usuarios

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

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.

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

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

Notas:

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

Autorización de los usuarios

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

Para autorizar usuarios con UVM, complete el procedimiento siguiente:

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

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

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

   Nota: los nombres de usuario de la lista se definen en las cuentas de usuario creadas en Windows.
4. Pulse **Autorizar**.

Se muestra la pantalla Configuración de autenticación del usuario.

5. Entre y confirme una frase de paso inicial de User Verification Manager para el usuario recién autorizado y después pulse **Siguiente**.

   Si la frase de paso no cumple los requisitos de la política de seguridad, se muestra una pantalla indicando que la frase de paso entrada no es válida. Si ocurre esto, pulse **Aceptar** y después pulse **Ver requisitos de la frase de paso** para ver los parámetros que debe cumplir una frase de paso válida.

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

6. Pulse **Aceptar** para continuar.

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

   - **Hacer que el usuario almacene la contraseña de Windows más tarde utilizando User Configuration Utility.** Para hacer que el usuario almacene su contraseña de Windows más tarde utilizando User Configuration Utility, seleccione el botón de selección adecuado y después pulse **Siguiente**.
   - **Almacenar ahora la contraseña actual de Windows del usuario.** Para almacenar ahora la contraseña actual de Windows del usuario, entre y confirme la contraseña del usuario en los campos proporcionados y después pulse **Siguiente**.

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

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

7. Pulse **Finalizar**.

Eliminación de usuarios

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

Para desautorizar usuarios con UVM, complete el procedimiento siguiente:

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

   Se muestra el mensaje Entre la contraseña del administrador.

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

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

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

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

5. Pulse **Sí** para continuar.

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

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

Creación de usuarios nuevos

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

Para crear usuarios nuevos, utilice el procedimiento siguiente:

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

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

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

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

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

Capítulo 6. Después de haber autorizado a los usuarios con UVM

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

- **Configuración de la protección de inicio de sesión de UVM para Windows.** Consulte "Consideraciones al configurar la protección de inicio de sesión de UVM" para obtener más información.
- **Archivo de claves de cifrado de usuarios.** Consulte "Cambio de la ubicación del archivador de claves" en la página 50 para obtener más información.
- **Configuración del protector de pantalla de Client Security.** Consulte el Capítulo 9, "Instrucciones para el usuario cliente", en la página 59 para obtener más información.
- **Registro de las huellas dactilares de los usuarios con UVM.** Consulte "Registro de las huellas dactilares de los usuarios con UVM" en la página 37 para obtener más información.

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

Protección de inicio de sesión de UVM para Windows

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

Consideraciones al configurar la protección de inicio de sesión de UVM

Lea la información siguiente antes de establecer y utilizar la protección de UVM para el inicio de sesión de Windows:

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

  Además, si no se ha registrado la contraseña de Windows (o se ha registrado de forma incorrecta) con UVM, el usuario deberá proporcionar la contraseña de Windows correcta para iniciar la sesión.
- No borre la información del chip IBM Security Chip incorporado mientras esté habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema. Para obtener más información, consulte "Funciones del administrador" en el Capítulo 10, "Resolución de problemas", en la página 65.
- Si quita la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM** en Administrator Utility, el sistema vuelve al proceso de inicio de sesión de Windows sin utilizar la protección de inicio de sesión de UVM.
- Si sustituye el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM y habilita la función LEAP de Cisco, debe reinstalar Cisco Aironet Client Utility (ACU).

Configuración de la protección de inicio de sesión de UVM

Para configurar la protección de inicio de sesión de UVM para Windows, complete el procedimiento siguiente:

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

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

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

Cuando se reinicia el sistema, se le solicitará que inicie la sesión del sistema. Para obtener más información sobre la protección de UVM, consulte "Protección de inicio de sesión de UVM para Windows" en la página 35.

Recuperación de frases de paso de UVM

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

Para iniciar el procedimiento de recuperación de una frase de paso de UVM, complete el procedimiento siguiente:

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

   Se abrirá la ventana principal de Administrator Utility.
2. Seleccione un usuario en el área Usuarios de Windows autorizados para usar UVM.
3. Pulse **Cambiar frase de paso**.

   Se abrirá la pantalla Cambiar frase de paso.
4. Escriba la vía de acceso y el nombre de directorio del archivador de claves o pulse **Examinar** para localizar el directorio.
5. Escriba la vía de acceso y el nombre de archivo de la clave privada del administrador en el campo Archivo de claves privadas del archivador o pulse **Examinar** para localizar el archivo.
6. Pulse **Aceptar**.

   Si se ha dividido la clave privada del administrador en varios archivos, se mostrará un mensaje que le solicitará que escriba la ubicación y el nombre de cada archivo. Pulse **Leer siguiente** después de escribir todos los nombres de archivo en el campo Archivo de claves.
7. Escriba la nueva frase de paso de UVM para el usuario en el campo Frase de paso de UVM y confírmela en al campo Confirmar frase de paso de UVM. Pulse **Ver requisitos de la frase de paso** para ver una lista de normas impuestas por la política de seguridad de UVM.
8. Seleccione y establezca las normas de caducidad de la frase de paso disponibles en el área de Caducidad de la frase de paso.

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

Registro de las huellas dactilares de los usuarios con UVM

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

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

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

   Se muestra la ventana Modificar la configuración de usuarios de Client Security- Editar los atributos del usuario de UVM.
3. Seleccione el recuadro de selección **Registrar huellas dactilares y/o smart card** y después pulse **Siguiente**.

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

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

Utilización de la protección de inicio de sesión de UVM para Lotus Notes

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

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

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

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

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

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

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.

3. Pulse el recuadro de selección **Habilitar soporte de Lotus Notes**.

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

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

   Se muestra la pantalla Clave privada del administrador necesaria.
10. Especifique la ubicación de la clave privada; para ello escriba el nombre de la vía de acceso en el campo que se proporciona o pulse **Examinar** y seleccione la carpeta adecuada.
11. Pulse **Aceptar**.

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

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

Utilización de la protección de UVM dentro de Lotus Notes

Antes de poder utilizar la protección de UVM para Lotus Notes, debe seguir los pasos en "Configuración de la protección de UVM dentro de Lotus Notes".

Configuración de la protección de UVM dentro de Lotus Notes

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

1. Inicie una sesión de Lotus Notes.

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

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

Restablecimiento de la contraseña de Lotus Notes

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

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

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

   Se mostrará la ventana Seguridad del usuario.
4. Pulse **Establecer contraseña**.

   Se mostrará la ventana IBM User Verification Manager.
5. Pulse el botón de selección **Crear su propia contraseña**.

6. Entre y verifique la nueva contraseña de Lotus Notes en los campos disponibles y después pulse **Aceptar**.

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

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

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

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

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

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

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

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

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

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

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

1. Salga de Lotus Notes.
2. Inhabilite la protección de UVM para el ID de usuario actual. Consulte “Inhabilitación de la protección de inicio de sesión de UVM para un ID de usuario de Lotus Notes” para obtener detalles.
3. Entre en Lotus Notes y cambie el ID de usuario. Consulte la documentación de Lotus Notes para obtener información sobre el cambio de ID de usuario.
4. Para configurar la protección de UVM para el ID de usuario al que ha cambiado, entre en la herramienta Configuración de Lotus Notes (proporcionada por Client Security Software) y configure la protección de UVM. Consulte “Utilización de la protección de UVM dentro de Lotus Notes” en la página 38.

Utilización del módulo PKCS#11 del chip IBM Security Chip incorporado

Las instrucciones proporcionadas en este apartado son específicas para el uso de Client Security Software en lo que se refiere generalmente a la obtención y utilización de certificados digitales con aplicaciones que soporten PKCS#11, como las aplicaciones de Netscape o RSA SecurID Software Token .

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

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

Instalación del módulo PKCS#11 del chip IBM Security Chip incorporado

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

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

1. Abra Netscape y después pulse **Archivo > Abrir página**.
2. Localice el archivo de instalación `ibmpkcsinstallt.html` o `ibmpkcsinstalls.html`.

   Si aceptó el directorio por omisión cuando instaló el software, el archivo se encuentra en C:\Archivos de programa\IBM\Security.
3. Abra el archivo de instalación `ibmpkcsinstallt.html` o `ibmpkcsinstalls.html` en Netscape.

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

   Se abre la ventana de frase de paso de UVM.
5. Escriba la frase de paso de UVM y pulse **Aceptar**.

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

Selección de IBM Embedded Security Subsystem para generar un certificado digital

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

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

Actualización del archivador de claves

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

Utilización del certificado digital del módulo PKCS#11

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

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

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

Capítulo 7. Trabajo con la política de UVM

Nota: antes de intentar editar la política de UVM para el cliente local, asegúrese de que se hayan establecido las claves. De lo contrario, se mostrará un mensaje de error cuando el editor de política intente abrir el archivo de políticas locales.

Después de haber autorizado a los usuarios para utilizar UVM, debe editar y guardar una política de seguridad para cada cliente de IBM. La política de seguridad proporcionada por Client Security Software se llama política de UVM, que combina los valores proporcionados en "Autorización de los usuarios" con los requisitos de autenticación de clientes. Un archivo de políticas de UVM se puede copiar en los clientes de una red.

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

- Todos los usuarios deben escribir una frase de paso de UVM y utilizar una autenticación de tarjeta de identificación por contacto para iniciar la sesión en Windows.

  Nota: no es necesario editar una política de UVM para utilizar la autenticación de proximidad.
- Todos los usuarios deben escribir una frase de paso de UVM cada vez que se obtiene un certificado digital.

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

La política de UVM establece los requisitos de objetos de autenticación para el cliente de IBM, no para el usuario individual. Por lo tanto, si establece que la política de UVM requiera la autenticación de huellas dactilares para un objeto (como el inicio de sesión de Windows), cada usuario que se autorice para utilizar UVM debe registrar una huella dactilar para utilizar ese objeto. Para obtener detalles, consulte "Eliminación de usuarios" en la página 33.

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

Edición de una política de UVM

Cuando se edita la política de UVM sólo se utiliza en el cliente para el que se ha editado. Si ha instalado Client Security en su ubicación por omisión, el archivo de política de UVM está almacenado como \Archivos de programa\IBM\Security\UVM_Policy\globalpolicy.gvm. Utilice el editor de

política de UVM para editar y guardar archivos de políticas de UVM. Se proporciona en Administrator Utility la interfaz del editor de política de UVM.

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

Cuando establece que la política de UVM requiera huellas dactilares como objetos de autenticación (como el inicio de sesión de Windows), cada usuario de UVM autorizado debe tener registradas sus huellas dactilares para utilizar ese objeto.

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

Selección de objetos

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

Los objetos de política de UVM válidos incluyen los siguientes:

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

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

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

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

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

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

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

Password Manager
Este objeto controla los requisitos de autenticación necesarios cuando se

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

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

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

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

Elementos de autenticación

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

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

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

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

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

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

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

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

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

Utilización del editor de política de UVM

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

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

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

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

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

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

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

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

Edición y utilización de la política de UVM

Para utilizar la política de UVM en varios clientes de IBM, edite y guarde la política de UVM 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.

Capítulo 8. Otras funciones para el administrador de seguridad

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

Para abrir Administrator Utility, complete el procedimiento siguiente:

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

   Dado que el acceso a Administrator Utility está protegido por la contraseña del administrador, se mostrará un mensaje que le solicitará que escriba la contraseña del administrador. Esta contraseña debe tener exactamente una longitud de ocho caracteres.
2. Escriba la contraseña del administrador y después pulse **Aceptar**.

Utilización de Administrator Console

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

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

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

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

- **Ubicación de la clave pública del archivador.** Este campo permite al administrador localizar la clave pública del administrador.
- **Ubicación de la clave privada del archivador.** Este campo permite al administrador localizar la clave privada del administrador.

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

Cambio de la ubicación del archivador de claves

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

Nota: el usuario cliente también puede cambiar la ubicación del archivador de claves mediante User Configuration Utility. Para obtener más información, consulte el Capítulo 9, "Instrucciones para el usuario cliente", en la página 59.

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

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

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

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

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

Cambio del par de claves del archivador

Cuando guarda las claves del administrador en la ubicación del archivador, las claves copiadas se denomina par de claves del archivador. Estas claves se suelen almacenar en un disquete o en un directorio de la red.

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

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

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

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

   Aparece la pantalla Modificar configuración de claves - Clave pública.
3. En el área Claves nuevas del archivador, escriba el nombre de archivo de la clave pública nueva del archivador en el campo Clave pública del archivador. También puede pulsar **Examinar** para buscar el archivo nuevo o pulsar **Crear** para generar una clave pública nueva del archivador.

   Nota: asegúrese de crear la clave pública nueva en una ubicación distinta a la que contiene los archivos de claves del archivador antiguos.
4. En el área Claves nuevas del archivador, escriba el nombre de archivo de la clave privada nueva del archivador en el campo Clave privada del archivador. También puede pulsar **Examinar** para buscar el archivo nuevo o pulsar **Crear** para generar un par de claves nuevo del archivador.

   Nota: asegúrese de crear el par de claves nuevo en una ubicación distinta a la que contiene los archivos de claves del archivador antiguos.
5. En el área Claves antiguas del archivador, escriba el nombre de archivo de la clave pública antigua del archivador en el campo Clave pública del archivador o pulse **Examinar** para buscar el archivo.
6. En el área Claves antiguas del archivador, escriba el nombre de archivo de la clave privada antigua del archivador en el campo Clave privada del archivador o pulse **Examinar** para buscar el archivo.
7. En el área Ubicación del archivador, escriba la vía de acceso donde está almacenado el archivador de claves o pulse **Examinar** para seleccionar la vía de acceso.
8. Pulse **Siguiente**.

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

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

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

Restauración de las claves desde el archivador

Necesitará restablecer las claves si cambia la placa del sistema o si un error en una unidad de disco duro pone en peligro la integridad de las claves de usuario. Cuando restaura claves, se copian los últimos archivos de claves de usuario del archivador de claves y se almacenan en el IBM Embedded Security Subsystem. La restauración de las claves escribirá encima de cualquier clave que esté almacenada actualmente en el chip de seguridad.

Si sustituye la placa del sistema original por otra nueva que contiene IBM Embedded Security Subsystem y aún son válidas las claves de cifrado en la unidad de disco duro, puede restaurar las claves de cifrado que se han asociado previamente al sistema "volviendo a cifrarlas" con IBM Embedded Security Subsystem en la placa del sistema nueva. Puede realizar una restauración de claves *después* de habilitar el chip nuevo y establecer una contraseña del administrador.

Para obtener detalles sobre cómo habilitar el nuevo subsistema de seguridad y establecer una contraseña del administrador, consulte el apartado "Habilitación de IBM Embedded Security Subsystem y establecimiento de la contraseña del administrador" en la página 56.

Nota: se habilita automáticamente el inicio de sesión de UVM después de una restauración de claves. Por consiguiente, si era necesaria la autenticación de huellas dactilares para el inicio de sesión de UVM en el sistema que se está restaurando, *deberá* instalar el software de huellas dactilares *antes* de rearrancar después de la restauración para evitar que se bloquee el sistema.

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

Requisitos para la restauración de claves

Las operaciones de restauración de claves sólo pueden realizarse satisfactoriamente si se cumplen las siguientes condiciones:

- El nombre del sistema restaurado debe coincidir con el nombre del sistema original.
- El sistema restaurado debe tener acceso al par de claves del administrador de CSS y a la ubicación del archivador del sistema original.
- El sistema restaurado debe tener un IBM Security Subsystem limpio y habilitado. Utilice el BIOS para habilitar y borrar el chip.
- El sistema restaurado debe tener el mismo nivel de IBM Security Subsystem que el sistema original (a saber, TCPA o no TCPA).

Escenarios de restauración

Son posibles los tres escenarios de restauración de IBM Client Security siguientes:

- **Sustitución de la placa del sistema.** Si es necesario sustituir la placa del sistema original o si hay que trasladar el disco duro a un nuevo sistema, es necesario restablecer IBM Security Subsystem con las claves para que coincidan con el sistema original a partir del archivador de claves.
- **Sustitución de todo el sistema.** Si el sistema original se pierde o es robado, es necesario restablecer tanto IBM Security Subsystem como IBM Client Security Software a partir de la información almacenada en la ubicación del archivador.
- **Sustitución de la unidad de disco duro.** Si se produce un error en la unidad de disco duro del sistema original y se instala una unidad de disco duro nueva en el sistema original, es necesario restablece IBM Client Security Software a partir de la ubicación del archivador.

Sustitución de la placa del sistema

Para sustituir la placa del sistema de un sistema en el que está habilitado BM Embedded Security Subsystem, complete el procedimiento siguiente:

1. Pulse el icono **IBM Client Security Subsystem** en el Panel de control de Windows.
2. Entre y confirme la contraseña del administrador; después pulse **Aceptar**.
3. Entre la ubicación del archivador y la ubicación de la clave del administrador del sistema original en los campos correspondientes; después pulse **Aceptar**.
4. Pulse **Aceptar**.
5. Pulse **Salir** para cerrar Administrator Utility.

   El sistema estará ahora totalmente restaurado. Rearranque el sistema antes de continuar.

Sustitución de todo el sistema

Después de instalar IBM Client Security Software en un sistema nuevo, se ejecuta automáticamente CSS Setup Wizard cuando se reinicia el sistema. Para iniciar una sustitución de todo el sistema y restablecer la información almacenada en la ubicación del archivador, complete el procedimiento siguiente:

1. Pulse **Siguiente** en la página inicial de CSS Setup Wizard.
2. Entre y confirme la contraseña del administrador para el nuevo sistema y pulse **Siguiente**.
3. Seleccione el botón de selección **Utilizar una clave de seguridad existente** y entre la ubicación de las claves pública y privada del administrador archivadas del sistema original en los campos correspondientes.
4. En el área Información de seguridad de copia de seguridad, entre una ubicación temporal del archivador.

   Notas:

   a. Suprima esta ubicación más adelante después de restaurar totalmente el sistema a partir del archivador del sistema original.

   b. El resto de la información se sobrescribe durante la restauración del archivador del sistema original; por lo tanto, utilice los valores por omisión.
5. Pulse **Siguiente**.
6. Pulse **Siguiente** en la página Proteger las aplicaciones con IBM Client Security.
7. Pulse **Siguiente** en la página Autorizar a los usuarios.
8. Pulse **Siguiente** en la página Seleccionar el nivel de seguridad del sistema.
9. Pulse **Finalizar** en la página Revise los valores de seguridad.
10. Pulse **Aceptar**.
11. Siga con el procedimiento del apartado “Sustitución de la unidad de disco duro”.

Sustitución de la unidad de disco duro

Para restaurar IBM Client Security Software a partir de la ubicación del archivador después de la sustitución de la unidad de disco duro, complete el procedimiento siguiente:

1. Pulse el icono **IBM Client Security Subsystem** en el Panel de control de Windows.
2. Entre la contraseña del administrador que se ha establecido en CSS Security Wizard y pulse **Aceptar**.
3. Pulse **Configuración de claves**.
4. Seleccione el botón de selección **Restaurar las claves de IBM Security Subsystem desde el archivador** y pulse **Siguiente**.

5. Entre la ubicación del archivador y las ubicaciones de la clave del administrador del sistema original en los campos correspondientes y pulse **Siguiente**.
6. Pulse **Aceptar**.
7. Pulse **Finalizar** para volver a la página principal de configuración.
8. Pulse **Salir** para cerrar Administrator Utility.

   El sistema estará ahora totalmente restaurado. Rearranque el sistema antes de continuar.

Restablecimiento del contador de errores de autenticación

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

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

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

   Se mostrará un mensaje que notifica que la operación se ha completado satisfactoriamente.
4. Pulse **Aceptar**.

Cambio de la información de configuración de Tivoli Access Manager

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

Configuración de la información de configuración de Tivoli Access Manager en un cliente

Después de instalar Tivoli Access Manager en el cliente local, puede configurar la información de configuración de Access Manager mediante Administrator Utility. Para definir la información de configuración de Tivoli Access Manager en el cliente de IBM, Client Security Software utiliza un archivo de configuración. Este archivo de configuración se utiliza para enlazar Tivoli Access Manager con los objetos que la política de UVM cede para ser controlados por él.

Para configurar la información de configuración de Tivoli Access Manager en un cliente, complete el procedimiento siguiente de Administrator Utility:

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

   Se mostrará la pantalla Configuración de aplicaciones y políticas de UVM.
2. Seleccione el recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**.
3. Pulse el botón **Política de aplicaciones**. Se mostrará la pantalla Modificar la configuración de políticas de Client Security.
4. En el área Información de configuración de Tivoli Access Manager, seleccione la vía de acceso completa del archivo de configuración `TAMCSS.conf`. Por ejemplo, `C:\TAMCSS\TAMCSS.conf`. Para que esté disponible esta área, Tivoli Access

Manager debe estar instalado en el cliente. También puede pulsar **Examinar** para buscar el archivo de configuración.

5. Pulse el botón **Editar política** y entre la contraseña del administrador.
6. Seleccione en el menú desplegable Acciones las acciones que desea que controle Tivoli Access Manager.
7. Seleccione el recuadro de selección **Access Manager controla el objeto seleccionado** para que aparezca una marca en el recuadro.
8. Pulse el botón **Aplicar**. Los cambios entrarán en vigor la próxima vez que se renueve la antememoria. Si desea que los cambios entren en vigor inmediatamente, pulse el botón **Renovar antememoria local** en la pantalla Modificar la configuración de políticas de Client Security.

Renovación de la antememoria local

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

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

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

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

Cambio de la contraseña del administrador

Debe establecer una contraseña del administrador para habilitar IBM Embedded Security Subsystem en un cliente. Después de establecer una contraseña del administrador, el acceso a Administrator Utility está protegido por esta contraseña. Para mejorar la seguridad, debería cambiar periódicamente la contraseña del administrador. Las contraseñas que permanecen si cambiar durante un largo período de tiempo pueden ser más vulnerables a ataques externos. Proteja la contraseña del administrador para impedir que los usuarios no autorizados cambien valores en Administrator Utility. Para obtener información sobre las normas para la contraseña del administrador, consulte el Apéndice B, “Información sobre contraseñas y frases de paso”, en la página 89.

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

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

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

   Se muestra la pantalla Cambiar contraseña del chip IBM Security Chip.
3. En el campo Contraseña nueva, escriba la contraseña nueva.

4. En el campo Confirmación, escriba de nuevo la contraseña.
5. Pulse **Aceptar**.

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

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

Consulta de información sobre Client Security Software

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

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

Inhabilitación de IBM Embedded Security Subsystem

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

Importante: no borre la información de IBM Embedded Security Subsystem mientras esté habilitada la protección de UVM. Si lo hace, quedará bloqueado su acceso al sistema. Para borrar la protección de UVM, abra Administrator Utility y quite la selección del recuadro de selección **Sustituir el inicio de sesión estándar de Windows con el inicio de sesión seguro de UVM**. Debe reiniciar el sistema para que se inhabilite la protección de UVM para el inicio de sesión del sistema.

Para inhabilitar Embedded Security Subsystem, complete el procedimiento siguiente de Administrator Utility:

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

Para utilizar IBM Embedded Security Subsystem y sus claves de cifrado después de que se inhabilita el subsistema, deber volver a habilitar el subsistema de seguridad.

Habilitación de IBM Embedded Security Subsystem y establecimiento de la contraseña del administrador

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

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

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

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

   Se mostrará un mensaje que le solicita que habilite IBM Embedded Security Subsystem para el cliente de IBM.
2. Pulse **Sí**.

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

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

Habilitación del soporte de Entrust

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

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

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

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

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

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

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

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

Capítulo 9. Instrucciones para el usuario cliente

Este apartado proporciona información para ayudar a un usuario cliente a efectuar las tareas siguientes:

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

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

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

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

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

Desbloqueo del cliente

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

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

   Se abre la ventana de frase de paso de UVM.

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

Notas:

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

User Configuration Utility

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

Características de User Configuration Utility

User Configuration Utility permite al usuario cliente hacer lo siguiente:

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

Limitaciones de User Configuration Utility en Windows XP

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

Windows XP Professional

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

- Client Security Software está instalado en una partición que posteriormente se ha convertido a formato NTFS

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

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

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

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

Windows XP Home

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

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

Utilización de User Configuration Utility

Para utilizar User Configuration Utility, complete el procedimiento siguiente:

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

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

Utilización de correo electrónico y navegación en la Web seguros

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

Un certificado digital (también denominado ID digital o certificado de seguridad) es una credencial electrónica emitida y firmada digitalmente por una autoridad de certificados. Cuando se emite un certificado digital para un usuario, la autoridad

de certificados está validando la identidad del usuario como propietario del certificado. Una autoridad de certificados es un proveedor fiable de certificados digitales y puede ser otra empresa emisora, como VeriSign; la autoridad de certificados también puede configurarse como un servidor dentro de su empresa. El certificado digital contiene su identidad, como su nombre y dirección de correo electrónico, las fechas de caducidad del certificado, una copia de su clave pública y la identidad de la autoridad de certificados y su firma digital.

Utilización de Client Security Software con aplicaciones de Microsoft

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

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

Obtención de un certificado digital para aplicaciones de Microsoft

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

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

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

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

Transferencia de certificados desde el CSP de Microsoft

El Asistente de transferencia de certificados de IBM CSS permite transferir los certificados que se han creado con el CSP de Microsoft por omisión al IBM Embedded Security Subsystem CSP. Transferir los certificados aumenta enormemente la protección ofrecida a las claves privadas asociadas con los certificados porque éstos se almacenarán de forma segura mediante IBM Embedded Security Subsystem, en lugar de mediante un software vulnerable.

Existen dos tipos de certificados de seguridad que pueden transferirse:

- **Certificados de usuario:** el propósito de un certificado de usuario es autorizar a un usuario determinado. Es habitual obtener un certificado de usuario de una

autoridad de certificados (CA), como cssdesk. Una autoridad de certificados es una entidad fiable que almacena, emite y publica certificados. Puede necesitar un certificado de usuario para firmar el correo electrónico, cifrarlo o para iniciar la sesión en un servidor específico.

- **Certificados de máquina:** el propósito de un certificado de máquina es identificar de forma exclusiva un sistema específico. Cuando se utiliza un certificado de máquina, la autenticación se basa en el sistema utilizado y no en la persona que lo está utilizando.

La aplicación Asistente de transferencia de certificados de CSS sólo transfiere los certificados Microsoft que estén marcados como exportables y está limitada a certificados cuyo tamaño de clave no supere los 1024 bits.

Si un usuario necesita transferir un certificado de máquina y no dispone de derechos de administrador en el sistema, un administrador puede enviar un archivo de configuración del administrador que permite al usuario transferir un certificado sin tener que proporcionar la contraseña del administrador. Utilice el programa de utilidad Consola del administrador, situado en la carpeta `c:\\archivos de programa\ibm\security`, para crear un archivo de configuración del administrador.

Para utilizar el Asistente de transferencia de certificados de CSS, complete el procedimiento siguiente:

1. Pulse **Inicio > Access IBM > IBM Client Security Software > Asistente de transferencia de certificados de CSS**.

   Aparece la pantalla de bienvenida del Asistente de transferencia de certificados de IBM CSS.
2. Pulse **Siguiente** para comenzar.
3. Seleccione los tipos de certificado que desea transferir y pulse **Siguiente**. El Asistente de transferencia de certificados de CSS sólo puede transferir certificados del almacén de certificados Microsoft que estén marcados como exportables.
4. Seleccione los certificados que desea transferir pulsando en el nombre del certificado en el área Emitido para de la interfaz y pulse **Siguiente**. Un mensaje indica que el certificado se ha transferido con éxito.

   Nota: para transferir un certificado de máquina se necesita la contraseña del administrador o un archivo de configuración del administrador.
5. Pulse **Aceptar** para volver al Asistente de transferencia de certificados de CSS.

Después de transferirse, los certificados se asocian con el IBM Embedded Security Subsystem CSP y las claves privadas están protegidas por IBM Embedded Security Subsystem. Cualquier operación que utilice estas claves privadas, como la creación de firmas digitales o el descifrado de correo electrónico, se efectuará dentro del entorno protegido de IBM Embedded Security Subsystem.

Actualización del archivador de claves para aplicaciones de Microsoft

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

Utilización del certificado digital para aplicaciones de Microsoft

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

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

Configuración de las preferencias de sonido de UVM

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

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

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

Capítulo 10. 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.