SecureEntry

Seguridad para plataformas corporativas

Antes de empezar

Antes de instalar SecureEntry, debería vd. leer detalladamente este manual de referencia, para asegurarse de que comprende la filosofía del producto, así como de que dispone del software y hardware apropiado y prerrequisito para el mismo. Observe que SecureEntry es un programa sumamente complejo, y que por su naturaleza es muy importante que vd. tenga una idea clara de lo que está haciendo en cada momento.

Además de este manual, sírvase leer el documento *README.DOC* que encontrará en el primer disquete de instalación. En el encontrará descritos los cambios de última hora.

Derechos de copia

Qué es SecureEntry

SecureEntry es un producto de software que complementa a cualquier estación de trabajo OS/2, tanto monopuesto como conectada en entorno de red, añadiendo un extenso número de funciones en las áreas de seguridad y personalización.

Con SecureEntry vd. podrá definir los usuarios y grupos de usuarios a los que les está permitida la utilización de la máquina, y a la vez configurar su entorno de trabajo de tal modo que, una vez identificados, se prepare dicho entorno para la sesión. El entorno de trabajo de un usuario está compuesto por características de personalización, así como por restricciones a ciertas partes del sistema a las que le debe ser denegado el acceso.

El efecto neto de lo que se acaba de comentar es que SecureEntry convierte así la estación de trabajo monousuario en otra de tipo compartido y de uso serializado. Desde el punto de vista del usuario final, pocas cosas cambian, excepto el hecho de que se ve obligado a identificarse antes de iniciar la sesión de trabajo. Es

en este punto en el que SecureEntry activará los *perfiles de seguridad y personalización* específicos del usuario.

SecureEntry ha sido diseñado de tal modo que se puedan añadir tipos nuevos de perfiles de seguridad, de un modo sencillo, con objeto de incorporar características de seguridad y personalización a componentes software/hardware específicos del cliente. A modo de ejemplo, vd. puede definir un componente que conste del archivo Lotus Notes de identificación, para que SecureEntry se encargue de que cada usuario conectado disponga del suyo propio siempre.

SecureEntry provee de los siguientes componentes de seguridad base :

Restricciones del escritorio : Permite definir restricciones sobre las propiedades (estilos) de los objetos existentes en el escritorio OS/2. Por ejemplo, se pueden definir ciertos objetos como invisibles, o no copiables para usuarios o grupos determinados.

Definición de escritorios personalizados : Permite definir carpetas personales, así como el contenido de las mismas, a añadir a los objetos existentes en el escritorio, De tal modo que dichas carpetas 'viajen' con el usuario cuando cambia de estación de trabajo. Este componente permite además definir para qué carpetas debe SecureEntry guardar las posiciones de los objetos definidos como parte del entorno de usuario (carpetas con memoria).

Definición de características del launchpad : Permite definir un barra de herramientas específico y personalizado para usuarios o grupos (launchpad OS/2).

Restricciones de la lista de tareas : El propósito de este componente es personalizar y restringir la lista de tareas, tanto en aspectos estéticos como pueda ser el color de fondo, así como las operaciones que se pueden realizar desde la misma, y los programas que deben o no aparecer en esta.

Restricciones de las ventanas : Este componente sirve para fijar ventanas de aplicación en un lugar dado de la pantalla y/o restringir las opciones de los menús asociados a las mismas. Así por ejemplo, se puede forzar que las ventanas de las sesiones de emulación salgan siempre maximizadas y no se pueda cambiar el font vía barra de menús.

Características del SES : Con este componente se personalizan los aspectos relacionados con el control de sesión para un usuario o grupo. Se pueden seleccionar bitmaps de bloqueo, el comportamiento del sistema a la hora de pulsar Ctrl-Alt-Supr,...

Restricciones de la disquetera : Permite establecer el tipo de acceso a la disquetera permitido a un usuario o grupo de usuarios, desde no acceso hasta acceso de lectura/escritura. Opcionalmente se puede configurar de tal modo que el contenido de los disquetes sea encriptado dinámicamente.

Restricciones del treelock : Este componente trabaja a nivel de gestor de sistema de archivos, y permite al administrador definir que partes de los sistemas de archivos montados en la máquina serán visibles y accesibles por los distintos usuarios o grupos, así como los derechos de acceso asociados (lectura, escritura, ejecución,...), con una granularidad que puede llegar a ser a nivel de proceso. Por ejemplo, se puede llegar a definir que un usuario determinado tan solo pueda escribir archivos en un directorio determinado cuando trabaje con un procesador de textos específico. Este componente se conoce con el nombre de 'treelock'.

Definición de combinaciones de acceso rápido : Este componente permite definir combinaciones de teclado/ratón para abrir los objetos deseados del escritorio cuando sean detectadas.

Definición de objetos con activadores : Usando este componente, vd. puede definir programas activadores a ejecutar cuando el/los objetos deseados sean abiertos. El componente incluye además un programa activador ejemplo, que valida claves de acceso de uso único para, por ejemplo, forzar la introducción de la misma antes de permitir el acceso a los programas o carpetas deseados.

Definición de WarpCenters : Con este componente vd. puede definir, en entornos warp 4 (Merlin) el warpcenter que utilizarán sus usuarios y grupos de usuarios.

Definición de Aplicaciones Públicas : Con este componente vd. puede definir, en entornos del LAN Server, las aplicaciones públicas que utilizarán sus usuarios y grupos de usuarios.

El componente de Procesos Auditables : Este componente permite medir la utilización de CPU por parte de distintos procesos y en base a un usuario.

Además de los componentes mencionados, SecureEntry no estaría completo si no proporcionase además una serie de funciones y herramientas que permiten acabar de asegurar la máquina, desde el momento de arranque hasta el de apagado. Éstas son :

Proceso de arranque protegido : Sustituye el proceso estándar del archivo *STARTUP.CMD* por otro propio de SecureEntry (*EDYSTART.CMD*), de tal modo que no pueda ser interrumpido durante su ejecución. Esta función incorpora además un programa de monitorización para que el usuario pueda seguir el proceso de arranque por medio de mensajes y una barra de progreso.

Programa de control de sesión : Se trata del 'corazón' de SecureEntry, y está siempre activo, llevando el control de los estados de la máquina, y interactuando con el usuario para que éste se identifique cuando sea necesario. Es el responsable de llevar a cabo la autenticación, bloqueo, conclusión, etc...

Subsistema de administración : Permite definir tanto los componentes como los usuarios y grupos presentes en la instalación, de un modo totalmente independiente del tipo de configuración seleccionado, con una vista única y consistente de la base de datos de componentes y usuarios. SecureEntry proporciona herramientas de administración a todos los niveles :

Gráfico

Batch

Por línea de comandos

Por interfície de aplicación (REXX o compilada).

Chequeo de la integridad de archivos : Que vd. puede utilizar para garantizar la integridad de los archivos críticos del sistema a intervalos predefinidos.

Otras herramientas : Como por ejemplo las utilidades de máquina virtual DOS, o el finalizador de aplicaciones selectivo, pueden ser utilizadas para facilitar la integración final de la solución con su software de producción.

Interfícies de programación : SecureEntry proporciona una serie de interfícies de programación y exits ('ganchos') de usuario para añadir procesos específicos de cada instalación.

Combinando todo esto con el amplio espectro de entornos soportados, así como el nivel de personalización alcanzable por medio de SecureEntry, se llega a comprender el nuevo sentido que SecureEntry puede dar al concepto de seguridad aplicado a las estaciones de trabajo en entornos OS/2.

SecureEntry es un paquete de software complejo por naturaleza, y por ello debería vd. leer completa y detalladamente este manual antes de utilizarlo.

IMPORTANTE : Mantenimiento, código beta y empaquetado

Mantenimiento

SecureEntry 3.0 no se desarrolla siguiendo el esquema de versionado de otros productos. Su naturaleza modular nos permite seguir un ciclo de desarrollo mucho más flexible, y a la vez orientado al cliente :

No se proporcionan nuevas versiones del producto con grandes saltos incrementales de funcionalidad. En su lugar, se distribuyen a intervalos regulares nuevos empaquetamientos del producto que pueden usarse como base para nuevas instalaciones, o bien para actualizar instalaciones ya existentes del mismo. Estos empaquetamientos incluyen :

Soluciones a los problemas reportados por los clientes

Nuevas funciones

Para los primeros, nos permitimos sugerir la política de aplicar mantenimiento solamente en aquellos casos en los que los incidentes reportados provoquen problemas en la instalación específica. Estos incidentes están documentados en el archivo *README.DOC* que acompaña a cada empaquetamiento.

En el caso de las nuevas funciones, es importante tener en cuenta que éstas son incorporadas durante un tiempo en estado 'beta' a los diferentes paquetes, y que durante este periodo, dichas funciones pueden presentar problemas de funcionamiento. Cuando se considera que una nueva función está lo suficientemente probada, deja de estar en estado 'beta', a completamente soportada en entornos de producción, y se documenta apropiadamente este cambio en el archivo *README.DOC*.

Por último, debemos mencionar que solamente se aceptarán peticiones de mantenimiento para problemas reportados en máquinas de producción que no estén utilizando funciones en beta. Del mismo modo, solamente está permitido el uso de aquellas funciones existentes en el producto en el momento del contrato, excepto si existiese un contrato de mantenimiento evolutivo en vigor, en cuyo caso las nuevas funciones añadidas a posteriori también estarán soportadas.

Empaquetado : Copias de evaluación y de producción

SecureEntry se distribuye con dos tipos de empaquetado diferentes :

Una *copia de evaluación* es 100% funcional, e incorpora absolutamente todo el código del producto, pero solamente es válida durante un periodo prefijado de, normalmente, 180 días a partir de la fecha del empaquetado. Una vez este periodo haya expirado, el producto pedirá, cada vez con mayor insistencia, que se desinstale o contrate formalmente. **NO ESTÁ PERMITIDO UTILIZAR COPIAS DE EVALUACIÓN EN ENTORNOS DE PRODUCCIÓN REALES**

Una *copia de producción* no expira, y se suministra solamente bajo contrato.

Vd. puede aplicar mantenimiento sobre una copia de evaluación con otra de producción sin necesidad de desinstalar el producto. La actualización hará que la instalación sea considerada de producción en adelante. Del mismo modo, se puede utilizar una copia de evaluación para actualizar una instalación con copia de producción quedando la instalación como de producción.

El tipo de copia suministrado puede verificarse examinando el archivo *SENTRY.SIG* que se encuentra en todos los disquetes de instalación del producto, o en el directorio de instalación del mismo, directorio *INSTALL*

Código UCM

Observe que la política de distribución del código de UCM para administración centralizada de usuarios SecureEntry es diferente :

No existe versión de evaluación del código UCM bajo entornos MVS/ESA. Si vd. desea evaluar la funcionalidad que UCM ofrece, sírvase instalar para evaluación la solución en entorno OS/2. Dicho código se provee integrado con la copia base de SecureEntry/2.

El código UCM para entornos OS/2 se suministra integrado en las copias de SecureEntry/2. Independientemente de que la copia SecureEntry/2 sea de evaluación o de producción, el código UCM suministrado siempre es en régimen de evaluación, y expira a los 180 días de la fecha de generación de dicha copia. Si una vez instalado y evaluado vd. decide contratar la solución UCM, deberá desproteger el código UCM con objeto de evitar que expire, tal y como se detalla en la sección correspondiente de la guía de administración UCM.

Prerrequisitos hardware

Es preciso lo siguiente para ejecutar satisfactoriamente SecureEntry 3.0 :

1. Una máquina con 12 MB de memoria (mínimo), y procesador 486 o superior.
2. Espacio libre en disco de aproximadamente 11.5 Mb. (2 Mb adicionales requeridos por el tutorial, si vd. planea instalarlo)
3. Tarjeta de conexión a red de área local para instalaciones tipo LAN.

Observe que si está vd. utilizando el soporte de WorkSpace On-Demand, también puede usar máquinas cliente de tipo 'Network Station' con arquitectura Intel(c), como por ejemplo las Network Station IBM de la serie 2800, que han sido probadas satisfactoriamente como clientes de IPL Remoto de servidores WorkSpace On-Demand habilitados con SecureEntry/2.

Prerrequisitos software

El software descrito a continuación debe estar instalado en la(s) máquina(s) en las que se pretenda ejecutar SecureEntry 3.0 :

1. OS/2 WARP con Fixpack 17 o superior, o OS/2 WARP 4 (Merlin). La resolución de pantalla mínima soportada para las funciones de administración de SecureEntry es de 800 x 600 puntos.
2. OS/2 SES (Servicios de seguridad para WARP3). Este software es necesario siempre que vd. no instale el emulador SES suministrado con SecureEntry.
3. IBM LAN Server/Requester 4.0 Para instalaciones tipo Lan Server. El controlador de dominio deberá usarse para la función de servidor de SecureEntry.
4. WorkSpace On-Demand, solamente si vd. desea usar el soporte SecureEntry para WorkSpace On-Demand. Para WorkSpace On-Demand 1.0, el nivel mínimo necesario para el sistema OS/2 Warp 4 a ejecutar por los clientes WorkSpace On-Demand es el FixPak 8. Para WorkSpace On-Demand 2.0, no se necesita ningún FixPak adicional para el sistema OS/2 Warp 4 que ejecutan los clientes WorkSpace On-Demand, aunque se recomienda el nivel de FixPack 9 en cualquier caso pues corrige errores detectados de sobreutilización de los recursos del sistema.
5. Si va usted a usar el Componente de Procesos Auditables, se le recomienda enérgicamente tener instalado el Fixpak 40 para Warp 3.0, o el Fixpak 10 para Warp 4.0.

6. Si está vd. instalando UCM, también necesitará :
    1. DDCS/2 single user en las estaciones de administración UCM
    2. El siguiente software instalado en su ordenador central :
        1. MVS/ESA
        2. DB2
        3. RACF V1.9.2 o posterior (si utiliza validación RACF).

Si vd. tiene de otra versión de SecureEntry instalada.

Si vd. dispone de SecureEntry 2.0 o 1.0 ya instalados:

Deberá previamente desinstalar la versión obsoleta antes de proseguir. Utilice la herramienta de desinstalación correspondiente a la versión de que disponga. En cualquier caso, los perfiles de escritorio que ya tuviese definidos son 100% compatibles con SecureEntry 3.0, así como los launchpads. SecureEntry 3.0 es capaz de migrar estos a la nueva base de datos, utilizando el programa de migración *MIGRADB.CMD* una vez en el servidor y cuando ya esté instalado SecureEntry 3.0. Observe que esta utilidad espera que la variable de entorno *SGM_LS* (obsoleta en SecureEntry 3.0) esté aún definida, con lo que probablemente deberá vd. tomar nota de su valor antes de desinstalar la versión antigua de SecureEntry. En caso de que vd. no disponga de utilidad de desinstalación para su versión de SecureEntry, puede usar *UNINSTAL.CMD* de SecureEntry 3.0. la herramienta dará varios mensajes de error, pero dejará la máquina en un estado lo suficientemente correcto como para que, después de un rearranque, SecureEntry 3.0 puede instalarse encima.

Si vd. está instalando sobre una versión 'alfa' de SecureEntry 3.0 (empaquetamientos 35..72):

Haga lo siguiente :

1. Guarde, si desea conservarla, la base de datos de perfiles de seguridad y usuarios. Esta se encuentra en el archivo *SGMSHELL\NOUSER\EDYREGDB.VLB*. En este caso, y para mantener la compatibilidad a nivel de cifrado de la misma, recuerde entrar como nombre de institución la cadena de carácteres *SER* cuando reinstale SecureEntry.
2. Guarde los archivos *SGMSHELL\DLL\EDYCUST.DLL* y *SGMSHELL\EXEC\EDYCUST.CMD*, en caso de que existieran (vd. estaba utilizando exits de usuario), y desee mantener su función una vez actualizado el software.
3. Guarde el archivo *SGMSHELL\DLL\EDYFILT.DLL*, en caso de que existiera (vd. estaba utilizando un filtro de nombres), y desee mantener su función una vez actualizado el software.
4. Guarde también el archivo *EDYSTART.CMD*, localizado en el directorio raíz del disco de arranque, como mínimo como referencia de qué procesos se están arrancando durante la puesta en marcha de la máquina.
5. Si vd. dispone de perfiles de seguridad asignados a nivel máquina, los encontrará en el directorio *SGMSHELL\NOUSER*. En este caso, y suponiendo que desee mantenerlos con la nueva actualización, cópielos en el último disquete de instalación de SecureEntry 3.0, dentro del directorio NOUSER, que probablemente deberá crear. De este modo, cuando instale la nueva versión de SecureEntry, estos perfiles se copiarán en su lugar original.

6. Ejecute el comando *UNINSTAL.CMD* que encontrará en el primer disquete de instalación de SecureEntry 3.0. Probablemente este comando dé algunos mensajes de error. ignórelos. Una vez terminado y cuando haya rearrancado la máquina, la versión alfa de SecureEntry estará desinstalada, por lo menos lo suficientemente bien como para reinstalar encima la nueva versión.
7. Ahora proceda a instalar SecureEntry, tal como se explica en el capítulo siguiente.
8. Una vez instalado, y antes de rearrancar, restaure los archivos previamente guardados :

   Vuelva a poner el código de exits de usuario (EDYCUST.*) donde corresponda. Recuerde migrar el código REXX previamente (EDYCUST.CMD) siguiendo el esqueleto que se suministra en el directorio *SGMSHELL\API\SOURCES\EDYCUST*.

   Reemplace el archivo *EDYSTART.CMD* por el previamente guardado, no sin antes verificar manualmente que el contenido sea el correcto.

   Ponga en su lugar la DLL de filtro de nombres (*EDYFILT.DLL*).

   Vuelva a copiar su base de datos de componentes y/o usuarios, si fuese necesario (archivo *EDYREGDB.VLB*) en el directorio *SGMSHELL\NOUSER*. Recuerde que este archivo se mantiene con atributos de sólo lectura, por lo que será necesario ejecutar *ATTRIB -R EDYREGDB.VLB* antes de borrar el antiguo.

Si vd. dispone de una versión beta o GA de SecureEntry 3.0 instalada :

Siga el procedimiento de actualización de software descrito en Proceso de actualización SecureEntry 3.0.

Si vd. tiene otra versión de UCM instalada

Si vd. dispone de UCM 3.0 ya instalado, y desea migrar a la versión V4R0, entonces debe seguir los pasos que se detallan a continuación:

1. Siga el procedimiento de actualización tal como se especifica en la guía de administración UCM para poner a nivel el software de host.
2. Siga el procedimiento de actualización de la estación administradora de UCM, tal como se indica en Configuración de la estación administradora de UCM.
3. Vd. puede saltarse lo que sigue si no tiene intención de activar la nueva función de actualización en línea de oficinas, ya que a continuación se describe como migrar y activar dicha función.

   Vd. deberá, inicialmente y como prerrequisito, migrar el código de las máquinas de todas sus oficinas a nivel de empaquetado 191 o superior. Puede hacer esto siguiendo el proceso de actualización de SecureEntry, tal como se indica en Proceso de actualización SecureEntry 3.0. Observe que este procedimiento de actualización no instala el parámetro de política para refresco dinámico en la línea de carga del *EDYSRV*, que se halla en el archivo *EDYSTART.CMD* de las máquinas servidoras. Si desea que este parámetro se añada automáticamente, puede escribir una serie de líneas REXX que realicen el cambio, y registrar el archivo REXX resultante como una salida de usuario para actualización (*POSTSERV.CMD*), tal como se explica en Personalización de la instalación. Los valores posibles para este parámetro (política de refresco) se explican en EDYSRV y EDYFREE.

   Durante el periodo en el que se esté activando el procedimiento de refresco dinámico de oficinas, vd. puede utilizar ambos métodos de refresco para actualizar las definiciones (grupos y recursos)

en sus servidores : Proceso batch (*EDYUCDIS.EXE*, *UCMP01*, ...) y proceso en línea (*EDYSRV.EXE* cargado con parámetro de política de refresco dinámico).

A pesar de que ambos métodos pueden coexistir una temporada, tenga en cuenta que las tablas de cambios en el host no deberían ser borradas durante este periodo, de tal modo que la información necesaria sea encontrada por ambos procesos. Para garantizar esto, haga lo siguiente :

Cuando ejecute los procesos batch *UCMP01* y *UCMP02* para obtener la información de cambios de sus oficinas, deberá usar el parámetro *Force Delete* con valor *'N'*.

No cambie el valor umbral de número de oficinas. Este parámetro de la nueva función de refresco dinámico, y al que se accede desde la herramienta de administración de usuarios y grupos en la estación administradora de UCM, debe mantenerse con valor *'0000'*. De este modo, los procesos de actualización dinámica de oficinas no borrarán las tablas de cambios.

Una vez haya vd. activado el parámetro de refresco dinámico en la línea de carga del proceso *EDYSRV.EXE* en todas sus oficinas, y no prevea utilizar más los procesos batch de refresco de oficinas, puede entonces modificar el valor umbral de número de oficinas, y actualizarlo con el número de oficinas con UCM instalado de que disponga en su organización.

Instalación de SecureEntry

El proceso de instalación de SecureEntry se compone de dos subprocesos diferentes :

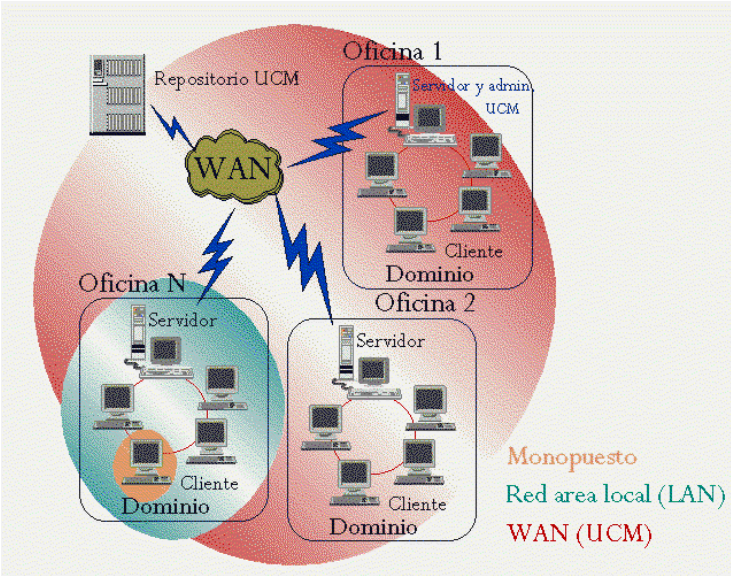
En primer lugar, la fase de definición, que es siempre interactiva, le permite definir los parámetros y características específicas de su instalación. Este proceso termina generando un archivo de respuestas para la siguiente fase y, opcionalmente, invocando a la segunda fase con los valores seleccionados. Este proceso se llama invocando al ejecutable *INSTALL.EXE*.

A continuación, la fase de instalación física comienza. Es en este punto en el que se transfieren al sistema los archivos necesarios, y se configura el entorno según las características especificadas, de tal modo que una vez rearrancada la máquina, se complete la instalación de SecureEntry 3.0. Esta parte de la instalación puede ejecutarse en modo interactivo o batch, invocando al ejecutable *INSTALB.EXE*

Tipos de instalación

Uno de los puntos fuertes de SecureEntry es su flexibilidad. Es decir, la capacidad de este software para ejecutarse en distintos entornos, y de adaptarse para encajar en proyectos con requisitos de seguridad muy variados, manteniendo una apariencia y consistencia, tanto de uso como de administración, que hace que con muy pocas salvedades, estas diferencias queden escondidas tanto para el administrador como para el usuario final.

La siguiente figura muestra de forma gráfica las diferentes opciones de instalación:



A continuación se describen con detalle la topología y posibilidades de cada uno de los entornos mostrados:

- Entornos monoestación
- Entornos IBM Lan server
- Entornos de red. Otras redes
- Otros entornos (control centralizado)

Entornos monoestación

Es éste el tipo de configuración más sencillo, diseñado para máquinas que no están conectadas a una red de área local. En este entorno, todas las funciones de administración y de usuario se ejecutan en la misma estación de trabajo. Ésta dispone de su propia base de datos de usuarios, grupos y perfiles de seguridad, de tal modo que es autosuficiente para decidir qué reglas de seguridad y características de personalización aplicar en cada momento, según el identificador del usuario que se halle conectado. Éste tipo de configuración es especialmente apropiado para usuarios particulares y trabajadores con máquinas portátiles compartidas, siendo también especialmente útil como introducción a las posibilidades del producto en ámbitos de demostración y formación.

Entornos IBM Lan server

Trabajando en máquinas conectadas en red, y cuando IBM Lan Server esté instalado, se puede configurar SecureEntry como una 'mochila' a éste último, que le complementa añadiendo potentes funciones de personalización y seguridad, así como atributos extendidos a los usuarios y grupos ya definidos. Esto se consigue gracias a la sincronización entre las conexiones SecureEntry y UPM, de tal modo que, transparentemente, SecureEntry utilizará las funciones de validación y autenticación de éste último, que a su vez delega en Lan Server, para conectarse y obtener la información necesaria sobre el usuario conectado.

En cuanto a la administración, SecureEntry provee igualmente con funciones transparentes de sincronización, de tal modo que, utilizando las aplicaciones y procesos de administración del producto se está, efectivamente, administrando el conjunto Lan Server + SecureEntry con una vista única.

una vez instalado SecureEntry con éste tipo de configuración, todos los grupos y usuarios Lan Server serán considerados automáticamente grupos y usuarios SecureEntry, con la posibilidad adicional de poderles ser asociados uno o varios perfiles de seguridad y/o personalización propios de SecureEntry.

Es importante notar que, en éste tipo de entorno, se crea efectivamente un grupo de estaciones de trabajo, que comparten la base de datos de perfiles de seguridad, de tal modo que cualquier usuario dado de alta podrá conectarse en cualquier máquina del dominio, y SecureEntry le aplicará los derechos y características asignadas. Es por éste motivo que una de las máquinas debe ser configurada como servidora de perfiles de seguridad. Es en ésta máquina, que coincide con el controlador de dominio Lan Server, donde residirá dicha base de datos.

Desde el punto de vista del administrador, este entorno no es muy diferente del anterior (monoestación), siendo las principales diferencias :

La herramienta gráfica de administración SecureEntry permite también configurar características propias de Lan Server, cómo recursos compartidos, usuarios asignados a más de un grupo, recursos compartidos en tiempo de conexión, etc...

La herramienta SecureEntry de administración batch acepta una serie de palabras clave nuevas (no disponibles en monoestación) para definir características Lan Server.

Los nombres de los grupos de usuarios a los que se desee poder asignar componentes deben comenzar por las letras 'SG', para identificar, de un modo unívoco, que perfiles de seguridad aplicar, dado que un usuario Lan Server puede pertenecer a más de un grupo.

Dado que el subsistema de definición de usuarios y grupos del que depende SecureEntry en éste entorno es Lan Server, también sus reglas específicas deberán ser respetadas (sintaxis de nombres, jerarquías, y rango de valores admisibles).

Puesto que los diferentes perfiles de seguridad podrán ser activados en cualquier máquina del dominio, todas deberán disponer de los objetos/recursos definidos en ellos. Por ejemplo, si se configura una barra de herramientas con un objeto dado, este objeto habrá que crearlo en todas las máquinas. Se pueden obtener buenos resultados clonando los discos duros de las máquinas clientes a partir de uno 'maestro'.

Como último comentario, SecureEntry permite configurar un controlador de dominio secundario de salvaguarda, de tal modo que tome el relevo si el principal presenta algún problema. Esto está descrito en Preparación de un controlador de dominio secundario (backup) para instalaciones Lan Server de forma detallada.

Entornos de red. Otras redes

Si vd. dispone de una red que no sea Lan Server, y teniendo como único prerrequisito el que disponga de soporte para directorios compartidos, puede entonces configurar SecureEntry para que todas las máquinas compartan las definiciones de usuarios y perfiles de seguridad centralizadamente, de modo que se utilice el subsistema de red solamente como medio de transporte, y dejando el resto de funciones de control y seguridad a SecureEntry. Evidentemente, en este tipo de entornos, SecureEntry no será capaz de administrar los recursos propios de su software de red.

En realidad, éste tipo de configuración es similar a un entorno monoestación, pero ofrece funcionalidades propias del entorno Lan Server, en el sentido de que cualquier usuario definido podrá identificarse y trabajar en cualquier máquina de la red.

Vd. solamente tendrá que preocuparse al instalar, de definir un directorio compartido donde SecureEntry pondrá su base de datos. Del mismo modo, deberá añadir la carga del soporte de red vía *CONFIG.SYS* o *EDYSTART.CMD* en todas las máquinas, de modo que dicho directorio compartido esté accesible una vez estos archivos hayan sido procesados.

Si vd. desea integrar todavía más su red con SecureEntry, queda la posibilidad de escribir un *LMP* (Procedimiento de conexión) e incorporarlo a la cadena conexión para que SecureEntry valide al usuario identificado en el diálogo de conexión frente a su software de red, tal y como se detalla más adelante.

Otros entornos (control centralizado)

Por encima de cualquiera de los entornos ya descritos, vd. puede montar el software adicional *UCM* (control centralizado de usuarios), que funcionando de modo cooperativo con su sistema central, le puede proporcionar:

> Validación de usuario/password a RACF, con sincronización de passwords en la red, utilizando un link APPC. Opcionalmente se puede utilizar también el emulador de RACF que UCM provee.
>
> Administración de perfiles, usuarios y grupos centralizada en una base de datos DB2/MVS, con refresco dinámico de la base de datos (en tiempo de conexión).

Usando estas dos funciones adicionales, vd. puede conseguir extender el concepto de red local SecureEntry al de red corporativa, donde cualquier usuario sea capaz de identificarse en cualquier máquina de su corporación, con sus reglas de seguridad y personalización específicas.

UCM debe contratarse por separado. No obstante, el software de lan del mismo se distribuye como parte del paquete SecureEntry estándar.

Proceso de definición

Antes de iniciar la instalación de SecureEntry, verifique que dispone del software y hardware necesarios. Del mismo modo, y si vd. está instalando *UCM*, proceda primero a instalar el mismo, tal como se especifica en la guía de administración de UCM.

Como paso previo a la instalación debe vd. hacer lo siguiente :

1. Anote y después borre los objetos que pudiese haber en la carpeta de arranque del OS/2. Estos objetos/programas, los podrá vd. arrancar, una vez instalado SecureEntry, desde el archivo *EDYSTART.CMD*, o desde una exit de usuario (*EDYCUST.CMD*), o bien incorporándolos a la lista de objetos de la carpeta SecureEntry *EdyStart*, que sustituye a esta función del OS/2.
2. Si vd. está instalando en un entorno IBM Lan Server, asegúrese de haberse conectado como administrador del sistema antes de instalar SecureEntry en la máquina servidora de perfiles de seguridad. Esto es necesario para que el proceso de instalación pueda crear la base de datos y el alias necesario para la compartición de la misma.
3. Igualmente, en el caso de instalaciones Lan Server, asegúrese de que no tenga definidos a priori grupos de usuarios cuyo identificador empiece por los carácteres 'SG', pues serían confundidos y tratados como grupos de seguridad SecureEntry.
4. Si vd. está instalando SecureEntry en un servidor de WorkSpace On-Demand, y tiene previsto habilitar las estaciones cliente del mismo para que utilicen SecureEntry, entonces tenga en cuenta que :

El servidor de WSOD (WorkSpace On-Demand) debe estar correctamente instalado antes de iniciar el proceso de instalación SecureEntry.

Vd. deberá instalar con el emulador SecureEntry de servicios de SES (deberá dejar desmarcada la casilla : *Usar los servicios SES de OS/2:*).

Vd. deberá instalar SecureEntry en un directorio llamado *SGMSHELL* dentro de la vía de acceso *IBMLAN\RPL\BBxx.yy*. Esta será la vía de instalación propuesta por la herramienta de instalación cuando se detecte WorkSpace On-Demand.

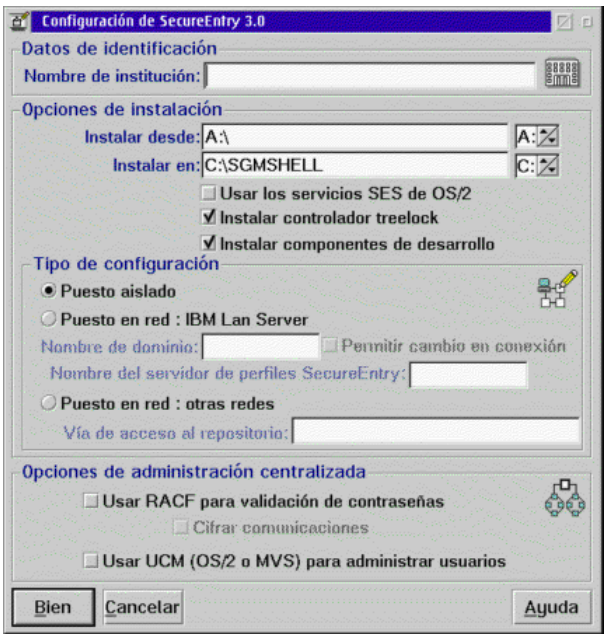
Posteriormente, y una vez completado el proceso de instalación, deberá vd. leer El soporte para WorkSpace On-Demand, y proceder a habilitar las diferentes estaciones clientes de WSOD.

Entonces, tecleando :

```
INSTALL [archivo_de_respuestas ]
```

desde el primer disquete de instalación de SecureEntry, arrancará el proceso de instalación. Este comienza por el subproceso de definición, en el que vd. deberá entrar datos referentes a la configuración deseada. Una vez entrados, el proceso generará un archivo de respuestas, que puede ser utilizado para instalar otras máquinas sin tener que volver a especificar dichos datos. Por defecto, este archivo de respuestas se denomina *SENTRY.CNF* y se crea en la misma vía de acceso donde resida el módulo *INSTALL.EXE*. Cuando el subproceso termina, encadena opcionalmente con la siguiente fase de la instalación (instalación física).

El diálogo de configuración tiene el siguiente aspecto :



Los campos a rellenar son :

Nombre de institución: Entre aquí el nombre de su institución. Este nombre se utilizará para generar una llave maestra privada con la que será cifrada su base de datos de usuarios y perfiles de seguridad.

Es imprescindible que este campo tome algún valor, y a la vez, que sea el mismo para todas las máquinas de un mismo dominio (en entornos de red), o grupo de trabajo.

Instalar desde: Esta es la vía de acceso a los archivos de instalación SecureEntry, para el proceso de instalación física.

Instalar en: Vía de acceso al disco y directorio donde se desea instalar SecureEntry. Observe que si el programa detecta la presencia de WorkSpace On-Demand, entonces le propondrá la vía de instalación *IBMLAN\RPL\BBxx.yy\SGMSHELL*, requerida para poder posteriormente habilitar los clientes WSOD para el uso de SecureEntry.

Usar los servicios SES de OS/2: Desmarque este botón para que SecureEntry se instale sin utilizar los servicios de seguridad de OS/2, y en su lugar utilice un emulador propio de los mismos. Esto es especialmente útil para versiones OS/2 donde estos servicios no estén disponibles (i.e, SMP), o cuando se desee ahorrar algo de memoria y disco. SES es un paquete aparte en OS/2 WARP 3.0, ya integrado en OS/2 WARP 4.0. En este último caso debe instalarse con el procedimiento de configuración selectiva de OS/2. Si vd. decide no utilizar los servicios de SES, la única diferencia funcional será el proceso de la exit de superusuario, como se explicará más adelante, que suele ser una función muy específica y apenas utilizada. El emulador SES es también un requisito para instalar en modo de coexistencia con otras aplicaciones que usan SES, o entornos WorkSpace On-Demand.

Instalar controlador treelock: Mantenga marcado este botón solamente si sus máquinas disponen de una versión del sistema operativo con soporte para funciones de monitorización de acceso a archivos (OS/2 WARP 3.0 no SMP con FP17 o superior, u OS/2 WARP 4.0 a cualquier nivel). En caso contrario, o si no planea configurar restricciones de acceso a nivel de sistema de archivos, desmárquelo.

Instalar componentes de desarrollo: Desmarque este botón en entornos de producción en los que no desee desarrollar software con los interfícies proporcionados por SecureEntry, como un medio de ahorrar algo de espacio en disco.

Puesto aislado: Esta opción selecciona la configuración en entorno monopuesto.

Puesto en red : IBM LAN server: Utilice esta opción para configurar máquinas SecureEntry en entorno Lan Server. En este caso, deberá entrar también :

> *Nombre dominio:* Entre aquí el identificador de su dominio Lan Server.
>
> *Permitir cambio en conexión:* Utilice esta opción para permitir la selección de otros dominios donde esté instalado SecureEntry desde el diálogo de conexión.
>
> *Nombre del servidor de perfiles:* Entre aquí el identificador del controlador de dominio Lan Server. Es en esta máquina donde se instalará la base de datos de perfiles de seguridad SecureEntry.

Puesto en red. *Otras redes:* Con esta opción se especifica el entorno de otras redes. Necesitará vd. proporcionar :

> *Vía de acceso al repositorio:* Entre aquí la vía de acceso remota al directorio compartido donde SecureEntry debe colocar su base de datos de usuarios y perfiles de seguridad. Esta vía debe ser la misma para todas las máquinas participantes del entorno.

Usar RACF para validación de contraseñas: Si vd. ha contratado UCM, entonces puede marcar este botón para especificar que las contraseñas de sus usuarios sean validadas contra RACF en tiempo de conexión. Si mantiene desmarcado el botón, pero instala UCM, la validación de usuarios y contraseñas se efectuará contra el emulador RACF provisto por UCM. RACF solamente está disponible para entornos UCM sobre MVS.

Alternativamente, vd. puede utilizar, como validador principal de contraseñas, la herramienta de productividad *NSC/2* En este caso no es necesario UCM, y deberá instalar dicho soporte posteriormente, tal y como se indica en el capítulo relacionado con el LMP asociado a NSC/2.

Cifrar comunicaciones: Utilizando RACF, vd. tiene la opción adicional de hacer uso de la facilidad SecureEntry de cifrado para usuarios y passwords durante la conexión. Selecciónela marcando este botón. Recuerde que vd. no necesitará esta funcionalidad si su red APPC ya es suficientemente segura, o está utilizando encripción de comunicaciones a un nivel más bajo.

Cuando se utiliza el emulador de RACF para autenticar usuarios, esta facilidad estará siempre activa.

Usar UCM en MVS para administración centralizada: Cuando haya contratado UCM, puede utilizar esta opción para indicar que las máquinas deben ser instaladas con el software de administración centralizada activo, de tal modo que la información de usuarios, grupos y recursos sea actualizada en la red dinámicamente desde el host cuando sea necesario. En este caso, y si desea asociar además un identificador nemotécnico a cada oficina, probablemente estará interesado en preparar la variable de entorno UCM **SGM_UCM_THIS_BRANCH** vía un archivo **CONFIG.ADD** de instalación personalizada, tal como se explica en Personalización de la instalación.

Una vez haya entrado los datos requeridos y generado el archivo de respuestas, el programa le preguntará si desea encadenar éste proceso con el de la instalación física, en cuyo caso deberá especificar vd. además, si está instalando una máquina cliente o el servidor de perfiles (instalaciones de red). En cualquier caso, con el archivo de respuestas, vd. podrá instalar las otras máquinas de su(s) oficina(s) sin necesidad de volver a suministrar los datos de configuración, invocando directamente el comando de llamada del proceso de instalación física.

Personalización de la instalación

Es probable que vd. desee distribuir ciertos componentes de seguridad predefinidos durante la instalación de SecureEntry, o ciertos archivos personalizados. En este punto se explica como conseguirlo.

Para distribuir archivos, vd. puede copiar en el primer o último de los disquetes de instalación dichos archivos, dentro del directorio en el que deberán residir, a partir del directorio base de instalación *SecureEntry*. Así por ejemplo, para instalar con un perfil de barra de herramientas (launchpad) por defecto, deberá vd. copiar el perfil deseado (*EDYPAD.INI*) en el directorio *NOUSER* del primer o último disquete, creando dicho directorio si fuese necesario.

Para distribuir otros archivos, cuando no deban residir en el árbol de directorios *SecureEntry*, cópielos según el siguiente convenio :

Directorio **BOOT** Si vd. desea que estos archivos sean copiados sobre la partición de arranque del sistema operativo.

Directorio **x$** Para que los archivos incluidos sean copiados sobre la partición *'x'*.

Adicionalmente, si vd. desea dar valor a alguna variable de entorno a través de la instalación, puede crear un archivo *CONFIG.ADD* en el directorio raíz del primer disquete de instalación, con los mandatos necesarios. Como ejemplo :

```
Ejemplo de CONFIG.ADD
---------------------

SET SGM_ALLOW_CAD=TRUE
SET SGM_PM_WAIT_B4_KILL=0
```

```
SET SGM_UCM_THIS_BRANCH=Oficina  22, C/Mayor. 456
```

Para tareas más complejas, existe la posibilidad de que vd. escriba su propio código REXX, y este sea llamado al finalizar el proceso de instalación o actualización. El nombre del archivo debe ser :

POSTINST.CMD Para especificar postproceso en instalaciones nuevas.

POSTSERV.CMD Para especificar postproceso en actualización.

Cree estos archivos en el primer o último de los disquetes de instalación, dentro del directorio raíz. Estos procedimientos serán llamados vía su copia en el path de instalación SecureEntry, directorio *INSTALL*.

Proceso de instalación física

INSTALB.EXE Es el programa encargado de llevar a cabo el proceso de instalación física de *SecureEntry*, que efectúa la copia de los archivos , y los cambios de configuración necesarios según las opciones seleccionadas durante el proceso de definición de la instalación. Para invocarlo, la sintaxis de llamada es :

```
INSTALB [SERVICE] [OVERFROM:ViaOrigen] [OVERTO:ViaDestino]
        [archivo_de_respuestas] [SERVER] [BATCH]
```

Use el parámetro *SERVER* para instalar la máquina servidora SecureEntry (en entornos de red).

Use el parámetro *BATCH* para llevar a cabo instalaciones desatendidas, sin interacción con el usuario.

Utilice el parámetro *SERVICE*, junto con *OVERFROM:* y *OVERTO:* para llamar al proceso de actualización (aunque resulta más sencillo invocar directamente a *SERVICE.CMD*, tal como se explica más adelante).

Observe que normalmente no resulta necesario invocar este programa manualmente, ya que tanto el proceso de definición (*INSTALL.EXE*), como el proceso de actualización (*SERVICE.CMD*) ya se encargan de llamarlo cuando se precisa.

Una vez este proceso finaliza, solicita que se rearranque la máquina. En cualquier caso puede ser necesaria una rápida verificación del mismo. Especialmente en entornos de red, habría que asegurarse de que el procedimiento de autoarranque SecureEntry (*EDYSTART.CMD*) contiene las sentencias necesarias para arrancar el software de red, que en el caso Lan Server son : *'NET START REQ'* para los clientes, y *'NET START SRV'* para las máquinas servidoras de la red.

Además, y antes de rearrancar, si vd. ha configurado UCM o RACF, debería verificar que el comunications manager está correctamente configurado, y su sentencia de arranque se halla también en el archivo *EDYSTART.CMD*. Recuerde por último, en el caso de que esté instalando la estación administradora de UCM, que debe configurar dicha estación tal como se explica en Configuración de la estación administradora de UCM.

Configuración de la estación administradora de UCM

Pase a la siguiente sección si no está vd. instalando la función de administración centralizada UCM.

Para habilitar la administración centralizada de UCM sobre SecureEntry, vd. debe seguir los siguientes pasos :

1. Instalar DDCS/2.
2. Instalar LAN Server.
3. Configurar el Comunications Manager. Para más detalles, vea la *guía de administración UCM*
4. Configure DDCS/2 Para más detalles, vea la *guía de administración UCM*
5. Instale SecureEntry 3.0.
6. Conéctese con un usuario con privilegios de administrador.
7. Abra la carpeta **SecureEntry: Herramientas de Administración**.
8. Haga una nueva copia del objeto **Administración de usuarios y grupos** y renómbrela como **Administración de usuarios y grupos UCM**. Abra la libreta de propiedades de este objeto y cambie *EDYSNADM.EXE* por *UCMADM.CMD* como nombre de programa a invocar. Ponga como parámetro *EDYSNADM.EXE*.
9. Para utilizar una tabla de traducción ASCII/EBCDIC personalizada, ponga los siguientes archivos en el directorio *INSTALL* de la vía de instalación SecureEntry (o en los disquetes de instalación, si todavía no ha instalado) :

```
EDYA2E.DAT
 Este archivo contiene 256 códigos de carácter para la conversión ASCII a
EBCDIC.


EDYE2A.DAT
 Este archivo contiene 256 códigos de carácter para la conversión EBCDIC a
ASCII.
```

   Por defecto, UCM usará sus propias tablas de traducción. Lea Guía de administración UCM para instalar las tablas personalizadas de traducción en su sistema central.

10. Desde una ventana de comandos OS/2, entre los comandos necesarios para vincular la API UCM.
11. Ejecute el programa *INSTSUB.EXE*, el cual añadirá la información básica sobre los subsistemas instalados en la base de datos centralizada, usando la API UCM. Haga esto como sigue :

```
db2start
instsub
Db2stop
```

12. Desde la ventana OS/2, entre los comandos necesarios para vincular el programa EDYQRYBR.
13. Desde la ventana OS/2, entre los comandos necesarios para vincular el programa EDYRVUCM.

Consulte la guía de administración UCM para configurar el UCM en el sistema central.

Preparación de controlador de dominio secundario para Lan Server

Si su entorno de instalación es Lan Server, entonces puede vd. configurar una máquina como controladora de dominio secundaria (backup), de tal modo que, en caso de fallo del controlador de dominio principal, ésta tomará la responsabilidad de validar sus usuarios durante la conexión. Puesto que vd. usa SecureEntry, es necesario configurar esta máquina para que además, disponga del repositorio (base de datos) de perfiles de seguridad, de tal modo que ésta función pueda llevarse a cabo satisfactoriamente.

El proceso a seguir para configurar el controlador de dominio secundario es como sigue :

1. Configuración del controlador de dominio secundario. Tareas Lan Server :
    1. Cuando instale Lan Server :

        seleccione "controlador de dominio secundario" como rol del servidor.

        instale los servicios de **REPLICACIÓN** y **REPLICACIÓN DCDB**.

    2. Una vez Lan Server esté instalado :

        Defina el controlador de dominio secundario en el dominio, como cualquier otro servidor adicional.

    3. Ajuste: Varios parámetros, como por ejemplo el *intervalo de replicación*, pueden ser ajustados por medio del archivo *IBMLAN.INI* Consulte los manuales apropiados de Lan Server para obtener más información.

    4. Consejos de operación :

        Para configurar el controlador de dominio secundario como el principal, vd. podrá (cuando el controlador principal no esté activo), ejecutar las siguientes sentencias en el controlador secundario :

        ```
        NET STOP NETLOGON
        NET ACCOUNTS  /ROLE:PRIMARY
        NET START NETLOGON
        ```

        Para forzar la replicación del DCDB :

        ```
        NET STOP   DCDBREPL
        NET START  DCDBREPL
        ```

        Para resincronizar las palabras clave de ambos controladores de dominio :

        ```
        LOGON como administrador
        NET ACCOUNTS  /ROLE:STANDALONE
        NET USER nombre_máquina nuevapassword
        NET ACCOUNTS  /ROLE:BACKUP
        NET USER nombre_máquina nuevapassword
        ```

2. Configuración específica SecureEntry
    1. Cree un nuevo directorio compartido en el controlador de dominio secundario, con nombre de alias *SGMSHBAK*, ejecutando :

        ```
        NET ALIAS SGMSHBAK \\nombrebdc dirbackup /WHEN:STARTUP
        ```

        Donde *nombrebdc* es el nombre de servidor del controlador de dominio secundario.

2. Copie la base de datos de perfiles SecureEntry al controlador secundario :

   ```
   COPY  \\nombredc\SGMSHELL\EDYREGDB.VLB  \\nombrebdc\SGMSHBAK\EDYREGDB.VLB
   ```

   Donde *nombredc* es el nombre de servidor del controlador de dominio primario, y *nombrebdc* es el nombre de servidor del controlador de dominio secundario.

3. Establezca un mecanismo por el cual la copia reseñada de la base de datos de perfiles SecureEntry se haga periódicamente. Puede vd. utilizar el servicio de replicación de Lan Server para ello, tal como se detalla en la documentación del mismo.

4. Dé acceso a este directorio a todos los usuarios deseados. Por ejemplo, y para dar acceso a todos los usuarios Lan Server :

   ```
   NET ACCESS SGMSHBAK /ADD USERS:RWA
   ```

Una vez completados estos pasos, y en caso de que el controlador de dominio principal fallase, los usuarios de su dominio SecureEntry podrían conectarse igualmente, siendo validados y obteniendo sus perfiles de seguridad a través del controlador de dominio secundario.

Consideraciones de operativa

Tenga en cuenta que :

No hay necesidad de cambiar el rol del controlador de dominio secundario cuando falle el principal.

Los usuarios que se conecten y sean validados por el controlador secundario, recibirán un mensaje informándoles de tal circunstancia. Similarmente, su proceso de conexión será algo más lento de lo habitual.

Si vd. se ha conectado contra el controlador principal, y éste falla, deberá desconectarse y volverse a conectar para poder utilizar las utilidades de administración.

Si vd. usa las utilidades de administración contra el controlador de dominio secundario, los cambios no serán automáticamente sincronizados en el controlador principal. Para conseguirlo, puede vd. hacer (con el controlador de dominio principal activo) :

1. Siga el procedimiento de resincronización estándar Lan Server para actualizar las definiciones de usuarios, grupos y recursos.
2. Copie el archivo de base de datos de perfiles de seguridad de usuarios y grupos SecureEntry desde el controlador secundario al primario.

Cuando se conecte contra el controlador secundario, es posible que los mensajes de error recibidos sean menos precisos que en conexiones normales. Esto es debido a que el módulo de apoyo *EDYSRV.EXE* no está activo normalmente en los controladores secundarios. Si lo desea, podrá activarlo en éste caso, pero deberá acordarse de desactivarlo cuando pretenda rearrancar el controlador de dominio principal, ya que solamente puede haber un *EDYSRV.EXE* activo a la vez por dominio. Lea EDYSRV y EDYFREE para más detalles.

Proceso de actualización SecureEntry 3.0

Puede vd. usar los disquetes de instalación SecureEntry para actualizar el nivel de una versión anterior de SecureEntry 3.0. Haga lo siguiente :

1. Inserte el primer disquete de instalación SecureEntry

2. Teclee (suponiendo que la unidad sea *A:*) :

   `A:\SERVICE [ViaOrigen] [BATCH]`

   Use *ViaOrigen* para especificar una vía de acceso a los archivos nuevos, siempre que ésta no sea la misma donde resida *SERVICE.CMD*.

   Use el parámetro *'BATCH'* para ejecutar SERVICE.CMD en modo desatendido.

   El procedimiento de servicio arrancará y el software SecureEntry será actualizado.

Este procedimiento respetará sus definiciones de usuarios, grupos y perfiles de seguridad, así como los valores de *CONFIG.SYS* y sus módulos de ejecución personales (archivos *EDYCUST.** y *EDYFILT.DLL*). Es posible que deba vd. migrar alguno de estos archivos manualmente, así como los archivos EDYKILL.NOT o EDYLOGS.STR residentes en la VíaDeAccesoSecureEntry\NOUSER si dichos archivos son distintos a los proporcionados por defecto (que se encuentran en el directorio EXEC de instalación de SecureEntry). Consulte el archivo *README.DOC* suministrado con la nueva versión de SecureEntry para asegurarse.

ADVERTENCIA: El procedimiento de actualización sobreescribirá los archivos de desarrollo del subdirectorio *API*. Por tanto, tómese unos minutos para salvar aquellos archivos fuente que vd. hubiese modificado antes de actualizar SecureEntry.

Observe que el procedimiento de servicio no finalizará hasta que vd. rearranque la máquina, momento en el cual se copiarán los archivos nuevos que normalmente se encuentran en uso, y se refrescará la carpeta de administración SecureEntry. Es por ello que el primer arranque después de actualizar puede tardar algunos minutos más de lo habitual. Déjelo correr hasta que haya cesado la actividad de disco (no lo interrumpa).

Por último, recordar que este procedimiento requiere autoridad de administrador para ejecutarse. En entornos de distribución, donde se desee hacer de modo totalmente automático, el procedimiento funcionará independientemente del usuario conectado siempre que :

1. Sea invocado en modo batch (parámetro *'BATCH'*)
2. Sea invocado desde un proceso en contexto superusuario, (cargado vía *EDYSTART.CMD*, *CONFIG.SYS*,...). Vea Procesos y contextos de ejecución para obtener más información.

Qué hacer si la instalación falla

En cualquier caso, y si la instalación falla por algún motivo, puede ser de gran ayuda repasar el archivo *'SENTRY.LOG'*, que se encontrará en el directorio raíz de la partición de arranque (si la instalación falla en sus primeras fases), o bien en el directorio *INSTALL* dentro del directorio de instalación SecureEntry (en otro caso). Una vez determinado el momento en que la instalación falló, entonces :

Si la instalación falla durante el proceso de copia de archivos, se puede borrar el directorio SecureEntry y reintentar.

Si la instalación falla más tarde, intentará dejar el sistema en un estado estable, pero en cualquier caso, y si *CONFIG.SYS* ha sido modificado, entonces la versión original se podrá encontrar en *'x:\SGMSHELL\INSTALL'* con el nombre *'config.sen'*, por si fuera necesario recuperarlo.

Si aún así persiste el error, contacte con el servicio técnico del equipo de mantenimiento SecureEntry.

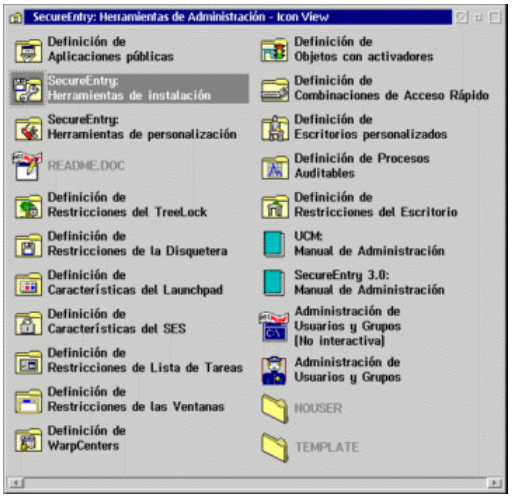
Qué hacer después de instalar

Una vez se haya completado el proceso de instalación, y rearrancado la máquina, aparecerá un diálogo de conexión. Vd. deberá conectarse :

Entornos monoestación : Conéctese usando usuario 'EDYADMIN', palabra clave 'PASSWORD', cambiando esta última (este usuario lo crea la instalación con la palabra clave expirada). Proceda a definir sus usuarios, grupos, y perfiles de seguridad.

Entornos en red Lan Server : Conéctese primero en el servidor de perfiles SecureEntry, usando un usuario administrador previamente existente, y proceda con la definición de usuarios, grupos y perfiles de seguridad.

Una vez conectado como administrador, vd. verá una nueva carpeta creada en su escritorio : Herramientas de administración SecureEntry. Contendrá :



Una carpeta con las herramientas de instalación dentro de la cual verá objetos para aplicar mantenimiento, desinstalar, los archivos de configuración, herramientas para instalar la protección de arranque, etc. En esta carpeta podrá vd. encontrar también una copia de su objeto barra de herramientas (launchpad) original.

Una carpeta con las herramientas de personalización, que básicamente contiene objetos listos para ser usados, que invocan diferentes funciones de control de sesión (i.e desconexión, bloqueo, etc).

Un icono para abrir el archivo de cambios de última hora (*README.DOC*).

Una carpeta con el banco de trabajo de cada uno de los componentes de seguridad disponibles. Dentro encontrará las herramientas necesarias para configurar un perfil de seguridad de cada tipo, así como otros objetos asociados o herramientas adicionales del componente.

Dos iconos representando los manuales de referencia en línea de SecureEntry y UCM.

Dos iconos para invocar las herramientas de administración interactiva y batch, respectivamente.

Una sombra del directorio (carpeta) *TEMPLATE*, que contiene los modelos originales para cada tipo de perfil de seguridad, así como algunos ejemplos adicionales.

Una sombra del directorio (carpeta) *NOUSER*, donde se encuentran los archivos específicos de la instalación personalizada, así como los perfiles por defecto de cada uno de los componentes de seguridad. Básicamente, cuando un componente se activa, y mientras no se conecte un usuario que tenga asignado un perfil de seguridad de su tipo, mantendrá activas las restricciones de seguridad del perfil que eventualmente pudiera haber en esta carpeta. Dentro de este directorio vd. encontrará también el objeto *EdyStart*, que actúa como una pseudo-carpeta, a la cual vd. puede añadir sombras de otros objetos a iniciar automáticamente cuando se arranque la máquina, sustituyendo efectivamente la funcionalidad OS/2 de la carpeta de inicio.

```
**********************************************
 IMPORTANTE

 Cuando vd. cambie un perfil de seguridad de la
 carpeta NOUSER, recuerde activarlo manualmente,
 con objeto de garantizar que éste se refresque.
**********************************************
```

La idea general es que vd. trabaje en la carpeta de trabajo de cada componente, creando, probando y afinando los perfiles de seguridad, hasta que esté satisfecho con los mismos. Una vez estos perfiles estén definidos, vd. podrá asignarlos a los diferentes usuarios o grupos utilizando el programa de administración interactiva, simplemente arrastrando y soltando dichos perfiles sobre el usuario/grupo deseado.

Dentro de cada carpeta de componente existen, como mínimo, los siguientes objetos :

Una sombra del modelo de perfil del componente. Arrastre desde éste objeto un perfil vacío cuando desee crear una instancia de perfil.

Un icono representando la herramienta de edición del perfil. Arrastre un perfil sobre éste icono, o haga doble-click sobre el mismo para poder ver y/o modificar su contenido.

Un icono representando la herramienta de activación del perfil. Arrastre un perfil sobre éste icono para activar las restricciones que este describa.

Antes de asignar los perfiles de seguridad, vd. tendrá que crear su estructura de usuarios y grupos, para lo que puede utilizar también el programa de administración interactiva, o bien cualquiera de las utilidades de administración batch o por línea de comandos, tal como se detalla más adelante.

Cuando un componente de seguridad no disponga de perfil de seguridad por defecto (en el directorio *NOUSER*), entonces existe un comportamiento estándar que varía según el componente. Éste es :

El componente de restricción de acceso a la disquetera, no permite el acceso a la misma. Obsérvese que SecureEntry pone, en tiempo de instalación, un perfil de seguridad con accesos plenos en el directorio *NOUSER*, de modo que vd. no observará esta regla a no ser que borre dicho perfil.

El componente de restricciones de escritorio no aplicará ninguna restricción.

El launchpad (barra de herramientas), no creará ningún objeto de tipo launchpad. Observe sin embargo, que el proceso de instalación copia su objeto launchpad original en la carpeta de *Herramientas de instalación*, de tal modo que vd. pueda fácilmente añadirlo a los objetos contenidos en la lista de objetos de autoarranque *EdyStart*, o bien utilizarlo como muestra para crear su propio perfil de personalización SecureEntry de barra de herramientas.

El componente WarpCenter creará un perfil SecureEntry con los mismos contenidos que su WarpCenter original, y lo pondrá en la carpeta NOUSER, de tal modo que después de instalar vd. verá arrancado su mismo WarpCenter.

El componente de restricción del comportamiento de ventanas, no aplicará restricción alguna.

La lista de tareas no será modificada.

Para el comportamiento de SES (control de sesión) :

1. Tiempo de bloqueo : 3 minutos, con diálogo estándar de desbloqueo y sin botones de desconexión/apagado ni control de máximo número de intentos de desbloqueo.
2. Ver diálogo de opciones al pulsar Ctrl-Alt-Del.
3. Enseñar bitmaps por defecto de bloqueo/salvapantallas.

En cuanto al treelock (restricción de archivos, tan solo se restringirá el acceso según la tabla de Restricciones implícitas.

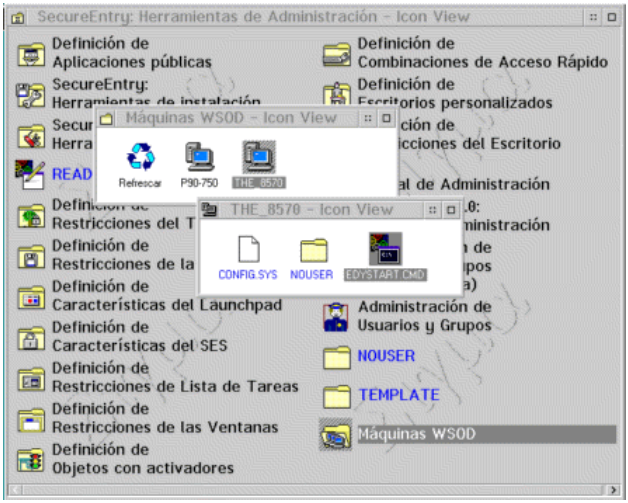
Los otros componentes no añadirán restricciones/características especiales.

Soporte para WorkSpace On-Demand

Si vd. ha instalado SecureEntry en un servidor de WorkSpace on-Demand, tal como se explicó en Proceso de definición, y desea utilizarlo desde las diferentes estaciones clientes del mismo, deberá utilizar el programa *Habilitador de WSOD* para configurar las imágenes de dichos clientes de modo que instalen efectivamente SecureEntry en tiempo de arranque remoto (RIPL). Esta utilidad se encuentra en la carpeta de *Herramientas de instalación*, dentro de la carpeta *SecureEntry:Herramientas de administración* .

Observe que todas las máquinas clientes WSOD usarán la misma copia del código SecureEntry, eliminando la necesidad de instalar el producto en cada una por separado, así como simplificando en gran medida el proceso de actualización del mismo.

En este entorno, vd. dispondrá así mismo de una carpeta de *Estaciones WSOD* , donde encontrará sombras de los objetos *NOUSER*, *CONFIG.SYS* y *EDYSTART.CMD*(en caso de que exista), para facilitar la personalización de las características del arranque de cada máquina, así como de sus restricciones de seguridad por defecto.



Observe el icono que representa al objeto *Refrescar* Este icono sirve para refrescar el contenido de la carpeta cuando se hayan habilitado estaciones cliente para SecureEntry de forma indirecta, es decir, creando nuevas configuraciones de máquina cliente a partir de un tipo de máquina previamente habilitado para SecureEntry, en lugar de utilizando el *Habilitador de WSOD*.

Una vez habilitadas las estaciones cliente que se desee, entonces para configurar un escritorio WSOD específico a un usuario, grupo o estación de trabajo bastará con definir un *perfil de aplicaciones públicas SecureEntry* utilizando el componente de Definición de Aplicaciones Públicas, con las aplicaciones deseadas para posteriormente asignarlo al usuario, grupo o a la carpeta *NOUSER* apropiada.

El habilitador de WSOD

Consejos para la administración SecureEntry-WSOD

El habilitador de WSOD

El *Habilitador de WSOD* es una aplicación que permite, de forma sencilla, habilitar/deshabilitar las estaciones clientes de un servidor WorkSpace On-Demand para que hagan uso de SecureEntry en su arranque remoto (RIPL). Para utilizar dicha aplicación deberá vd. haberse identificado como administrador del servidor de WSOD.

La primera vez que el *Habilitador de WSOD* se ejecute, éste habilitará, opcionalmente, y como paso previo requerido, el servidor para permitir su uso como servidor WSOD-SecureEntry.

Vd. podrá, a partir de entonces, configurar el servidor con cualquier combinación de estaciones cliente/tipos de máquina habilitadas/deshabilitadas para el uso de SecureEntry. El hecho de habilitar un tipo de máquina determinado no tiene otra finalidad que la de evitar la habilitación manual de las estaciones que se creen a partir de entonces a partir de dicho modelo de máquina.

Llamando interactivamente al habilitador de WSOD

El programa, cuando sea llamado sin parámetros adicionales, requerirá la intervención manual para habilitar o deshabilitar estaciones WSOD o modelos de máquina previamente creados.

Vd. puede invocar el programa tecleando :

```
SEWSODEN
```

Desde la vía de acceso SecureEntry, directorio *INSTALL*, o directamente haciendo doble-click sobre el icono que lo representa en la carpeta de *Herramientas de instalación*.

Verá entonces vd. el siguiente diálogo :

Donde la lista superior izquierda representa los tipos de máquina WSOD definidos, junto con un indicador de estado de habilitación SecureEntry, y la lista superior derecha representa las máquinas configuradas a partir del tipo de máquina seleccionado, así mismo con el indicador pertinente de estado de habilitación SecureEntry. La lista inferior contendrá el registro de actividad hasta el momento. Las acciones que puede vd. efectuar son :

Habilitar clase Con este botón puede vd. habilitar el modelo de máquina seleccionado para el uso de SecureEntry. El programa dará la opción adicional de habilitar las estaciones creadas a partir de dicho

tipo de máquina. Una vez habilitada una clase de máquina, al crear una estación de ese tipo se instanciará ésta ya habilitada para el uso de SecureEntry.

Deshabilitar clase Este botón causará que el tipo de máquina seleccionado sea deshabilitado y, opcionalmente, también las estaciones creadas a partir de dicha clase de máquina.

Habilitar estación Con este botón puede vd. habilitar para uso de SecureEntry una estación determinada (aquella que se encuentre seleccionada).

Deshabilitar estación Con este botón puede vd. deshabilitar una estación determinada, y hacer que pase así a ser una estación cliente WSOD estándar.

*Deshabilitar servidor*Cuando todas las clases de máquina y estaciones WSOD se encuentren deshabilitadas, podrá vd. utilizar este botón como último paso para deshabilitar el servidor WSOD del uso de SecureEntry. Este proceso **no** desinstala SecureEntry, si no ta sólo deshace el proceso inicial que permite que el mismo sea utilizado para compartir SecureEntry con los clientes WSOD. El habilitador WSOD terminará automáticamente cuando se ejecute esta acción satisfactoriamente.

Invocando el habilitador de WSOD en modo desatendido

Alternativamente, puede vd. ejecutar el programa en modo desatendido, siempre que lo llame con los parámetros apropiados :

```
SEWSODEN [ES | DS | EA | DA | EC:nombreclase | DC:nombreclase |
          ECW:nombreclase | DCW:nombreclase | EW:nombremáquina |
          DW:nombremáquina | EX ]
```

Donde

ES

Puede utilizarse para habilitar el servidor, siempre que sea preciso

DS

Sirve para deshabilitar el servidor. La ejecución satisfactoria de este parámetro forzará la descarga posterior del *Habilitador de WSOD*

EA

Utilice este parámetro para habilitar todas las estaciones y tipos de máquina detectados.

DA

Utilice este parámetro para deshabilitar todas las estaciones y tipos de máquina detectados.

EC

Sirve para habilitar la clase de máquina especificada.

DC

Sirve para deshabilitar la clase de máquina especificada.

ECW

Para habilitar las estaciones creadas a partir de una clase, utilice este parámetro especificando el nombre de clase de máquina deseado.

DCW

Para deshabilitar las estaciones creadas a partir de una clase, utilice este parámetro especificando el nombre de clase de máquina deseado.

EW

Este parámetro habilita la estación WSOD especificada para uso de SecureEntry.

DW

Este parámetro deshabilita la estación WSOD especificada para uso de SecureEntry.

EX

La ejecución de este parámetro fuerza la salida del programa.

Todos los parámetros son ejecutados secuencialmente. Así por ejemplo, el comando :

```
SEWSODEN  ES EC:MCAVGA ECW:MCAVGA EX
```

Quiere decir : Habilita el servidor si es necesario, y después habilita para SecureEntry la clase de máquina *MCAVGA*, para posteriormente habilitar todas las estaciones del mismo tipo, terminando el programa a continuación.

Códigos de retorno y determinación de problemas

El programa retornará 0 si no se han detectado errores. En otro caso, el código de retorno será igual al número de errores de habilitación/deshabilitación encontrados.

En caso de problemas, toda la actividad del programa queda registrada en el archivo de registro de instalación SecureEntry : *SENTRY.LOG*, que se halla en el directorio *INSTALL* dentro de la vía de acceso SecureEntry actual.

Consejos para la administración SecureEntry-WSOD

Personalización de estaciones cliente WSOD-SecureEntry

Si vd. desea habilitar sus tipos de máquina o estaciones WSOD con un conjunto de variables de entorno diferente del habitual, puede incluir la definición de dichas variables en un archivo denominado *CONFWSOD.ADD*, con el mismo formato que el descrito anteriormente para *CONFIG.ADD* en personalización de la instalación. Este archivo debe residir en el directorio *INSTALL* de su vía de acceso SecureEntry.

Adicionalmente, y para ejecutar procesos mas complejos, el *Habilitador de WSOD* llamará a los siguientes comandos REXX a modo de exits de usuario :

POSTENCL.CMD Llamado con posterioridad a la habilitación de un tipo de máquina, recibe como parámetro el nombre de la clase de máquina habilitada para uso de SecureEntry.

POSTDSCL.CMD Llamado con posterioridad a la deshabilitación de un tipo de máquina, recibe como parámetro el nombre de la clase de máquina deshabilitada para uso de SecureEntry.

POSTENWS.CMD Llamado con posterioridad a la habilitación de una estación WSOD, recibe como parámetro el nombre de la estación habilitada para uso de SecureEntry.

POSTDSWS.CMD Llamado con posterioridad a la deshabilitación de una estación WSOD, recibe como parámetro el nombre de la estación deshabilitada para uso de SecureEntry.

Estos archivos deben residir también en el directorio *INSTALL* de su vía de acceso SecureEntry.

Si vd. desea añadir algún archivo de personalización de solo lectura para todas las estaciones habilitadas SecureEntry, como por ejemplo un archivo de exits de usuario tipo *EDYCUST*, bastará con que lo instale en el directorio SecureEntry apropiado del servidor (p.e, *SGMSHELL\EXEC* de la vía de acceso SecureEntry).

Para los archivos de lectura/escritura, el árbol de lectura/escritura SecureEntry de cada máquina se encuentra a partir de : *x:\IBMLAN\RPLUSER\nombremáquina\SGMSHELL*.

El archivo de arranque protegido *EDYSTART.CMD* debe ponerse en la vía *x:\IBMLAN\RPLUSER\nombremáquina* para que sea procesado por SecureEntry durante el arranque remoto de la máquina cliente. Observe que si antes de la habilitación SecureEntry de una máquina existiese en dicha vía un archivo *STARTUP.CMD*, éste será migrado por el proceso de habilitado de la estación a *EDYSTART.CMD*.

Qué componentes SecureEntry funcionan en los clientes WSOD

Vd. puede utilizar toda la funcionalidad que SecureEntry provee en entornos WorkSpace on Demand, con las siguientes salvedades y restricciones :

El componente WarpCenter No se soporta este componente en clientes WSOD, ya que por las características del mismo, y según la filosofía WSOD, solamente sería viable usarlo como lanzador de aplicaciones, por lo que sugerimos utilice un perfil de barra de herramientas personal (Launchpad) en su lugar.

El objeto de autoarranque EdyStart Dado que en clientes WSOD el lugar de trabajo (WorkPlace Shell) se rearranca cada vez que un usuario se conecta, SecureEntry ignora los contenidos de dicho objeto para no causar una carga de los mismos en cada conexión. Si vd. desea ejecutar ciertos procesos automáticamente en tiempo de arranque de la máquina, le sugerimos utilice el archivo EDYSTART.CMD, o que lo haga vía la exit de usuario apropiada en su lugar. Si vd. desea ejecutar ciertos procesos en cada conexión, deberá entonces utilizar una carpeta personal configurada como de autoarranque y asignada a los usuarios/grupos apropiados.

Los componentes relacionados con el escritorio (desktop) Específicamente hablando, los escritorios restringidos, barras de herramientas y las carpetas personales están soportados en entornos WSOD, pero deberá vd. tener en cuenta que en este entorno, su funcionalidad estará además acotada y restringida por el propio WorkSpace On Demand. Así por ejemplo, no será posible borrar o arrastrar nuevos objetos sobre la barra de herramientas o la carpeta personal, ni hacer un objeto 'borrable' para usuarios no administradores.

Además, y con objeto de facilitar la configuración de SecureEntry, podrá vd. crear una carpeta de *Herramientas de administración* en una máquina cliente de WSOD siempre que :

1. Se haya conectado como administrador
2. Tenga vd. acceso a una línea de comandos o al objeto 'Unidades'
3. Esté vd. utilizando la versión de WSOD 2.0 como mínimo

Para crear dicha carpeta, ejecute el programa EDYCRWRK que se encuentra en su vía de acceso SecureEntry, subdirectorio INSTALL.

De este modo, podrá configurar de una forma fácil y cómoda los perfiles de seguridad y personalización SecureEntry deseados y asignarlos a los usuarios y/o grupos requeridos, tomando como base el escritorio y entorno de trabajo real de las estaciones cliente. Hacerlo así es especialmente importante para configurar perfiles SecureEntry relacionados con el escritorio, dado que puede resultar imposible el configurar exactamente el mismo entorno en el servidor de WorkSpace on Demand que en las estaciones.

Uso de SecureEntry

Una de las virtudes de SecureEntry es que éste es un producto que trabaja de modo transparente, y por lo tanto el usuario no observará cambio alguno en su hábito de trabajo. Tan solo las funciones de control de sesión pondrán en evidencia el hecho de que se está en un entorno protegido, al requerir una identificación por parte de los usuarios para trabajar.

Conexión

Desbloqueo

Desconexión

Ctl-Alt-Supr

Conexión

Después del arranque, o cuando la sesión de trabajo anterior haya finalizado, se presentará el siguiente diálogo :

Simplemente entre su identificador y palabra clave, pulse *Bien*, y se iniciará su sesión de trabajo. En caso de que desee cambiar la palabra clave, marque el botón de cambio y entre la nueva palabra clave en ambos campos.

Desbloqueo

La sesión de trabajo puede bloquearse por varios motivos :

Solicitud explícita vía el botón de bloqueo de la barra de herramientas (launchpad o smartcenter)

Solicitud explícita vía el menú emergente del escritorio

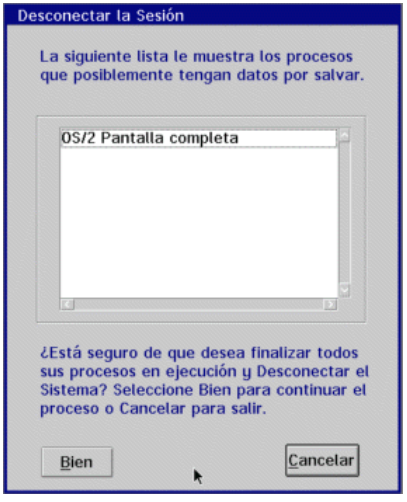
Bloqueo automático de la sesión por periodo de inactividad detectado

En caso de que esto suceda, verá el siguiente diálogo :

Entre su palabra clave (la que utilizó para conectarse), pulse *Bien* y la sesión de trabajo continuará.

Desconexión

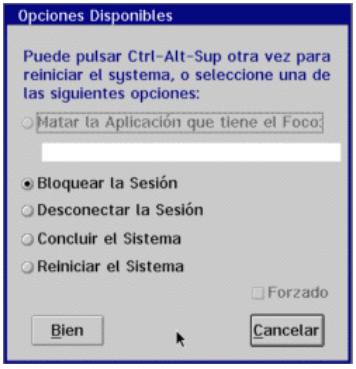
En cualquier momento vd. puede desconectar la sesión o cerrar el sistema vía el menú emergente del escritorio, o el botón apropiado del launchpad o smartcenter. La diferencia entre ambas funciones es evidente. Mientras la desconexión de sesión volverá a presentar el diálogo de conexión para que un nuevo usuario se identifique, *Concluir* preparará el sistema para ser desconectado físicamente. En cualquiera de los dos casos, el sistema puede presentar un diálogo similar a :



Éste diálogo le recuerda las aplicaciones que se están ejecutando y pueden tener datos por salvar. Acepte la lista presionando sobre *Bien* para proseguir la desconexión, o cancele la operación presionando *Cancelar* para poder cerrar las aplicaciones manualmente.

Ctl-Alt-Supr

Ésta combinación de teclas, usada normalmente para rearrancar el sistema, puede ser configurada con SecureEntry para que desconecte la sesión, cierre el proceso en curso, o concluya el sistema. Opcionalmente, vd. puede tenerla configurada de tal modo que le pregunte sobre la acción a tomar, presentando el siguiente diálogo :



Vd. puede escoger entre :

Terminar la applicación que tenía el foco

Desconectar la sesión

Concluir

Bloquear el sistema

Rearrancar. Debe ser considerada como la opción de cierre de emergencia.

Escoja una de las opciones y pulse *Bien* para continuar.

Componentes de seguridad - Base y PM

Si vd. acaba de instalar SecureEntry, y es el responsable de la definición y administración del mismo, necesitará planear las siguientes tareas :

1. Definir una política de seguridad para su instalación. Puede empezar identificando grupos de usuarios con necesidades similares (p.e, cajeros, interventores, desarrolladores, ...). Esto le dará una idea de qué roles asignar y qué grupos de usuarios SecureEntry deberá definir.
2. Definir, grupo a grupo, qué tipo de interacciones con el sistema les serán permitidas a sus usuarios, a nivel de componente. Esto es :

   Qué aplicaciones son necesarias en cada grupo para poder trabajar, y el grado de libertad y flexibilidad con que deben ser tratadas a nivel de escritorio : opciones del menú emergente, si el usuario podrá mover sus iconos representativos, etc.. (componente de restricción de escritorio).

   Cual debe ser el contenido de la barra de herramientas (launchpad o warpcenter) para cada grupo, p.e, cual es el conjunto de aplicaciones/objetos más frecuentemente usados. (componentes launchpad o warpcenter).

   Grado de libertad requerido para el manejo de las aplicaciones, desde dentro de las mismas. p.e, si se desea restringir alguna entrada de menú, o fijar la posición de sus ventanas (componente de restricción del comportamiento de las ventanas).

   Aspecto general y ciclo de control de sesión, por ejemplo, qué imágenes deben verse al bloquearse la máquina, qué hacer cuando el usuario pulse Ctrl-Alt-Supr,... (componente SES).

   Política de acceso a la disquetera. ¿ Va a dejar vd. a sus usuarios que accedan a la misma ?. ¿ En qué modo ? (componente de restricción de acceso a la disquetera).

   Definir, a nivel de gestor de archivos, a qué directorios/archivos se debe permitir o prohibir el acceso, y desde qué aplicaciones. (componente treelock)

   ¿ Deben haber combinaciones de teclas aceleradoras ?, ¿ cuales y para qué grupos ? (componente de combinaciones de acceso rápido)

   ¿ Habrán objetos con acceso restringido por palabra clave u otro ?, ¿ cuales y para qué grupos ? (componente de objetos con activadores)

   ¿ Qué aspecto deberá tener la lista de tareas ?, ¿ qué tipo de interacción estará soportada ? (componente lista de tareas)

   ¿ Es necesario definir carpetas personales o con memoria de posicionamiento ? (componente de escritorio personal)
3. Extraiga, de las respuestas anteriores, los perfiles de seguridad comunes para todos los grupos, así como las excepciones, que deberán ser asignadas a nivel de usuario. Descarte a priori la utilización de aquellos componentes para los cuales no se requiera un comportamiento específico en ningún grupo.
4. Construya una tabla de descripción de necesidades, como la siguiente :

Grupo	Requisitos	Componente
Defecto	Bitmaps estándar, ctl-alt-supr debe preguntar	SES
ADMINS	Sin restricciones, Launchpad especial con herramientas de ADMIN.	Launchpad
CAJEROS	Acceso a terminal financiero. Iconos fijos.	Escritorio,

	Permitir acceso a AMIPRO. disquetera modo lectura encriptada. ctl-alt-supr desactivado. Launchpad con terminal financiero. Impedir manipulacion de fuentes en emuladores.	Treelock, disquetera, SES, Launchpad, Comp. Ventanas.
DESARROLLO	Acceso no restringido. Launchpad con herramientas desarrollo	Escritorio, Launchpad
Casos especiales	Algunos desarrolladores necesitan acceso a disquetera R/W ENCRIPTADA	disquetera

5. Cree y pruebe los diferentes perfiles de seguridad utilizando la carpeta de definición de perfiles de cada componente, asignando nombres a los perfiles ya identificados.
6. Cree una tabla como la siguiente :

Componente	Defecto	ADMINS	CAJEROS	DESARROLLO	Excepciones
ESCRITORIO	All invisible	All visible	DESK1.INI	DESK2.INI	
LAUNCHPAD		LP1.INI	LP2.INI	LP3.INI	
VENTANAS			WB1.INI		
SES	SES1.INI		SES2.INI		
FLOPPY			FLOP1.INI		FLOP2.INI (*)
TREELOCK			TLK1.INI		

```
(*) Para desarrolladores con acceso a disquetera encriptado.
```

7. Utilice la herramienta interactiva o batch de administración para crear los diferentes usuarios y grupos de usuarios. Tenga en cuenta que, en caso de operar en entornos Lan Server, el identificador para los grupos SecureEntry debe empezar por los carácteres *'SG'*.
8. Utilice las herramientas de administración para asignar los perfiles de seguridad ya creados a los diferentes grupos y/o usuarios. Esta operación se realiza con la herramienta interactiva arrastrando y soltando el perfil seleccionado dentro del contenedor de componentes del grupo/usuario deseado.
9. Copie en la carpeta *NOUSER* los perfiles de seguridad comunes a todos los usuarios, cuyas restricciones y características desea que actúen como valor por defecto a nivel de máquina. Recuerde darles como nombre el nombre por defecto para los perfiles, según su tipo. El nombre por defecto es aquel que ya tiene el modelo del mismo tipo en la carpeta *TEMPLATE*.
10. Decida si es necesario, y en su caso active, cualquiera de las otras funciones de seguridad suministradas con SecureEntry, como por ejemplo :

    Protección de arranque

    Chequeo de la integridad de los archivos

    Proceso de arranque

    Exits de usuario
11. Compruebe su solución
12. En cualquier momento, si vd. desea cambiar algún perfil de seguridad, es posible hacerlo directamente desde la herramienta interactiva de administración de usuarios y grupos, haciendo doble-click sobre el icono que representa el componente a cambiar.

A continuación se describe como configurar y trabajar con cada uno de los componentes SecureEntry, detallados en el presente y siguiente capítulos :

Componentes relacionados con los servicios base y de presentación :

- Restricciones de la disquetera
- Características del SES
- Restricciones de las ventanas
- Restricciones de la lista de tareas
- Restricciones del treelock
- Proceso de arranque protegido
- Protección de arranque
- Chequeo de la integridad de archivos
- Componente de procesos auditables

Componentes relacionados con el escritorio :

- Restricciones del escritorio
- Definición de escritorios personalizados
- Definición de objetos con activadores
- Definición de características del launchpad
- Definición de WarpCenters
- Definición de combinaciones de acceso rápido
- Definición de Aplicaciones Públicas

Restricciones de la disquetera

Ya que este es uno de los componentes más sencillos de utilizar, lo describiremos en primer lugar.

El componente de restricción de acceso a la disquetera permite configurar el modo en el que se desea ver la misma, con varias opciones :

- Sin acceso
- Acceso de lectura/escritura
- Lectura/escritura con encripción
- Acceso en modo de sólo lectura
- Acceso de solo lectura con encripción

Cuando se seleccione un modo de acceso con encripción, esta puede a su vez establecerse con tres algoritmos distintos :

- La encripción genérica, ofrece un nivel de protección básico.

La encripción mejorada, ofrece un nivel de protección complejo, aunque sigue siendo genérica en tanto que cualquier máquina SecureEntry que use este modo podrá acceder a los disquetes.

La encripción dependiente de la institución, tiene un coste equivalente al modo anterior, pero utiliza como semilla el identificador de su institución, de tal modo que los disquetes grabados de esta forma solamente serán accesibles por máquinas SecureEntry de su organización.

Para trabajar con este componente, abra la carpeta de *definición de restricciones de la disquetera*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*.

Vd. puede crear un perfil para este componente mediante el modelo de perfiles de la misma carpeta (*EDYFLOPP.INI*).

Arrastre y suelte el perfil creado sobre el objeto *editor de restricciones de la disquetera*, para editar los valores de dicho perfil. El editor tiene el siguiente aspecto :

Una vez satisfecho con la opción seleccionada, guarde el perfil y salga del editor. Para probarlo, arrástrelo y suéltelo sobre el objeto *Test de las restricciones de la disquetera*.

Por último, vd. puede traducir disquetes de un modo a otro utilizando el objeto *Traductor de disquetes*, que se encuentra también en la misma carpeta. Ejecute el programa y consulte la ayuda disponible en caso de duda. Observe como esta utilidad es particularmente eficiente, por cuanto tan solo traduce de cada disquete el espacio utilizado por los archivos, sin necesidad de leer/escribir todas las pistas. SecureEntry proporciona además una versión de línea de comandos para efectuar esta operación. Así pues, los programas traductores pueden invocarse como sigue :

EDYTFLOP.EXE Para el traductor PM (gráfico), y

TRANDISK.EXE Para la versión en modo texto.

Ambos residen en el directorio *EXEC*, de su vía de acceso SecureEntry.

Descripción de los módulos y API

Descripción de los módulos y API

A continuación se describen los módulos que se integran en este componente:

Filtro de acceso a la disquetera

Se carga vía el *CONFIG.SYS* con la sentencia :

```
BASEDEV=EDYFLPY.FLT
```

Observe que para evitar problemas con el filtro **XDF**, EDYFLPY debe ser cargado después del filtro OS/2 XDFLOPPY.FLT.

Mensajes:

Carga correcta:

```
IBM SecureEntry Floppy Disk Filter V 1.00
```

Códigos de retorno : Ninguno. En caso de fallo de carga no se interrumpe el arranque.

EDYFLINI

Este es el programa editor de perfiles. Tiene la siguiente sintaxis :

```
EDYFLINI.EXE [Perfil]
```

Donde *Perfil* es la vía de acceso y nombre de archivo del perfil deseado. En caso de que el filtro esté cargado, el programa permite probar un modo de acceso directamente.

EDYFLPY

El programa activador de perfiles, tiene la siguiente sintaxis :

```
EDYFLPY.EXE [/I:[disco:][vía][archivo][.INI]] | [/V:valor]
```

Si se especifica un nombre de archivo, activará el modo de acceso indicado en el perfil.

Si se suministra un *valor*, activará el modo de acceso según el valor.

Mensajes:

Correcto:

```
Ok
```

Errores:

```
Usage: EDYFLPY [/I:[drive:][pathname]filename.[.INI]]  | [/V:Value]]
               Value in [10,20,21,22,30,40,41,42,50]

System Error (hex)=__ (dec)=__ querying for file ________

The Floppy Disk Filter API returned  (hex)=__ (dec)=__
See EDYFLAPI.ERR for more information
```

El archivo EDYFLAPI.ERR se escribirá con, para cada error encontrado, la siguiente información :

```
Error produced on WEEKDAY, DATE AND TIME
----------------------------------------
 Source Module Name: SOURCE MODULE NAME
 Compilation Date  : COMPILATION DATE
 Compilation Time  : COMPILATION TIME
 Source Line Number: SOURCE LINE NUMBER
 Logged Error      :  (hex)=RC (dec)=RC
```

Códigos de retorno : 0 para operación correcta. En otro caso, el código del error encontrado.

Interfície del filtro de acceso a la disquetera

El filtro exporta las siguientes rutinas, tal como se define en *EDYFLAPI.H*:

```
ULONG _System EDYFloppyAccessFromIni(PSZ  FileName);
```

Si *FileName* no es NULL, entonces se espera que apunte a un nombre válido de perfil de acceso, para activar el modo especificado en él. Si *FileName* tiene valor NULL, entonces se activará el perfil existente en *%SGM_SHELL%\NOUSER\EDYFLOPP.INI* y en caso de que no existiese, se activaría el modo de no acceso a la disquetera.

```
ULONG _System EDYFloppyAccessFromValue(LONG  Value);
```

Value debe ser alguno de los cinco modos de acceso válidos.

```
ULONG _System EDYGetIniValue(PSZ  FileName, PLONG Value);
```

Esta función solamente obtiene el modo de acceso especificado en el perfil indicado, sin activarlo.

```
ULONG _System EDYSetIniValue(PSZ  FileName, LONG Value);
```

Actualiza el perfil especificado con el valor proporcionado en *Value*.

Códigos de retorno : Operación realizada : 0. Un error devolverá el código de error del sistema operativo.

Características del SES

El componente de características SES permite configurar el comportamiento básico de SecureEntry en las funciones de control de sesión (conexión, desconexión, bloqueo,...), así como ciertos aspectos estéticos de la misma :

Imágenes a presentar durante el proceso de arranque protegido

Imágen de fondo del escritorio

Aspecto y temporizador para el diálogo de desbloqueo

Función salvapantallas (imágenes y temporizadores)

Combinaciones de teclas de sistema (inhibir/llamar a código de usuario)

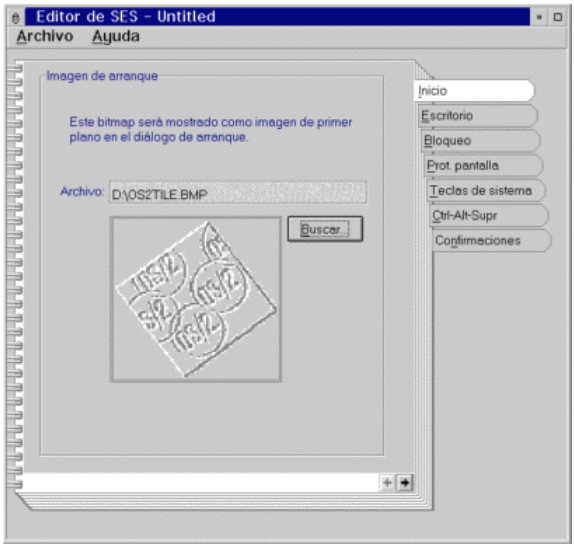
Comportamiento durante el proceso de Ctl-Alt-Supr

Diálogos de confirmación en desconexión de sesión o conclusión del sistema.

Para trabajar con este componente, abra la carpeta de *definición de características del SES*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Para crear un perfil de seguridad de características de SES, utilice el objeto modelo suministrado (*EDYSES.INI*).

Para editar el perfil, haga doble click sobre el mismo, o bien arrastre y suelte el perfil sobre el *editor de características de SES*. Este editor presenta una libreta con páginas para la configuración de las diferentes funciones :



Cuando configure perfiles de características SES, tenga en cuenta :

Las imágenes que configure para el arranque protegido solamente se utilizarán si el perfil se halla en la carpeta *NOUSER* durante el arranque de la máquina, pues ese es el perfil activo antes de la conexión del primer usuario. Estas imágenes serán las definidas como fondo para el bloqueo (imágen de fondo usada en el arranque), y la imágen definida en la página de arranque, (imágen de primer plano).

En la página de *confirmaciones*, vd. puede configurar aquellas aplicaciones que vd. desea de un modo fijo se pida o no se pida confirmación de cierre al concluir o desconectar la sesión estando éstas activas. Dichas aplicaciones pueden configurarse tanto por título (especificándolo entre comillas) como por nombre de proceso, con la posibilidad de especificar carácteres de sustitución ('*' y '?'). Las sesiones DOS serán todas consideradas la misma, sin diferenciación, como una aplicación con nombre de proceso *VDM* o *SYSINIT*, indistintamente.

Para comprender cual será la lógica de confirmación, se enumera a continuación el proceso a seguir :

1. Al desconectar la sesión o concluir el sistema, SecureEntry preparará una lista con los procesos a matar. Esta lista contendrá todos los procesos en activo de la máquina, excepto :

   Los procesos ejecutando en contexto de superusuario, si se está desconectando la sesión. (ver Procesos y contextos de ejecución)

   Procesos que ya estén muriendo.

   Procesos ejecutando en contexto de superusuario, detachados (no interactivos).

   Procesos reservados, como PMSPOOL, PMSHELL o los propios de SecureEntry.

   Todos los procesos pertenecientes a la sesión de pantalla 0 como HARDERR.EXE.

2. Entonces, y uno a uno, todos los procesos restantes en la lista serán filtrados según el perfil de características de SES activo, marcando cada uno como 'a enseñar' , 'a no enseñar', o 'no especificado'.

3. Aquellos procesos marcados como 'no especificado' en la lista anterior se resolverán como sigue :

   Procesos de VDM (emulación DOS) se enseñarán.

   Los procesos PM y los no interactivos no se enseñarán.

   Los procesos de línea de comandos OS/2 enseñarán solamente su proceso descendiente más profundo.

A la hora de configurar las aplicaciones, vd. puede configurar un perfil que pida confirmación para todos los procesos, y en dicho diálogo, tomar nota de los títulos presentados. Puede también hacer doble-click sobre la lista para que esta muestre el nombre de los procesos en lugar de los títulos.

Si vd. no especifica imágen por defecto para el arranque protegido en su perfil de características de SES, y **si** tiene configurada una imágen móvil para la función salvapantallas, se usará esta durante el arranque.

El objeto *Test de características del SES* puede usarse para activar un perfil y comprobar así su funcionamiento. Arrastre y suelte el perfil sobre el objeto testeador.

Por último, tenga en cuenta que **toda** la funcionalidad de este componente está soportada, independientemente de si se usan los servicios de seguridad SES del OS/2, o solamente el emulador SES de SecureEntry.

Restricciones de las ventanas

El **componente de restricción del comportamiento de las ventanas** le permite configurar perfiles de seguridad que restrinjan el comportamiento y la funcionalidad de las ventanas principales de las aplicaciones con las que vd. trabaje. Entre otras cosas, vd. puede prefijar el tamaño y la posición inicial de las mismas, y restringir alguna o todas las opciones del menú de sistema de éstas, así como deshabilitar ciertas opciones de los menús de su aplicación, especificando el nombre de dichas opciones.

Para trabajar con este componente, abra la carpeta de *definición de restricciones de las ventanas*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Para crear un perfil de seguridad para este componente, utilice el objeto modelo suministrado (*EDYWIN.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor del comportamiento de las ventanas*, o bien haga doble click sobre el mismo. Haga las modificaciones pertinentes, y después salve el perfil modificado.

Para verificar el comportamiento de un perfil antes de asignarlo a un usuario o grupo, puede vd. activarlo arrastrándolo sobre el objeto *test del comportamiento de las ventanas*.

Hay una serie de detalles a tener en cuenta cuando trabaje con este componente :

1. El parámetro de retardo configurable para el posicionamiento/tamaño inicial de las ventanas debe ser usado para aquellas aplicaciones que rechazan el posicionamiento inicial utilizando retardo 0. Esto es debido a que ciertas aplicaciones reposicionan sus ventanas un tiempo después de crearlas, con lo que SecureEntry deberá esperar un intervalo de tiempo mayor antes de efectuar el ajuste final.
2. Vd. puede configurar restricciones por título de ventana o por nombre de proceso :

   Para configurar por título de ventana, entre el título tal y como se muestra en la ventana, entre comillas dobles.

   Para configurar por nombre de proceso, deberá vd. entrar el nombre del proceso 'dueño' de la ventana. Utilice esta opción sólo como último recurso, si la configuración por título resulta inviable. Observe que todas las ventanas de comandos DOS y OS/2 son propiedad del proceso *PMSHELL.EXE* (*SESSHELL.EXE* si está usando los servicios de seguridad SES de OS/2).
3. Tanto los nombres de las ventanas, procesos, como las opciones de menú pueden configurarse con carácteres de sustitución ('*' y '?') y no son sensibles a mayúsculas/minúsculas al hacer las pertinentes comparaciones.
4. La lista de ventanas configuradas se procesa de forma ordenada, en el mismo orden en que aparecen en el editor. Tan solo la primera restricción cuyo título de ventana o nombre de proceso concuerde con la configurada será utilizada.
5. Solamente se pueden configurar restricciones al cambio de tamaño o posicionamiento inicial de aquellas ventanas cuyo tamaño sea modificable por el usuario, es decir, que tengan borde de cambio de tamaño.
6. Al configurar opciones de menú a deshabilitar, tenga en cuenta :

   El alcance de las restricciones sobre los menús afectados :

1. Para ventanas especificadas por título de ventanas, se restringirán todos los menús y submenús cuya ventana propietaria sea una ventana con el mismo título.
2. Para ventanas configuradas por nombre de proceso, todos los menús cuyo procedimiento de proceso de mensajes ejecute en el contexto del proceso indicado (mismo identificador de proceso).

La ventana principal con nombre 'Escritorio' es propietaria de todos los menús de primer nivel del escritorio, mientras que el proceso *PMSHELL.EXE* es el propietario de todos los menús del escritorio, incluyendo aquellos menús de objetos incluidos en carpetas abiertas.

Vd. puede configurar opciones de menú a inhabilitar en todos los casos de ventanas no indicadas explícitamente, configurando la entrada especial <*DEFAULT*>.

Como ejemplos de lo anterior :

Para deshabilitar la opción *Desconectar* del menú de sistema del escritorio :

```
Configure la opción Concluir como entrada de menú a deshabilitar
para una ventana con nombre "Desktop"
```

Para deshabilitar la opción *Buscar* de todos los menús del escritorio, incluyendo objetos de carpetas abiertas :

```
Configure la opción *Buscar* como entrada de menú a deshabilitar
para las ventanas del proceso *PMSHELL.EXE
```

Observe los asteriscos '*', incluídos para inhabilitar también aquellas opciones donde 'B' sea una tecla aceleradora, así como las opciones de tipo 'Buscar..'.

Para inhabilitar **todas** las opciones de menú del tipo *Buscar* :

```
Configure la opción *Buscar* como entrada de menú a deshabilitar
para la entrada <DEFAULT>
```

7. Cuando configure restricciones para aplicaciones WINOS2, tenga en cuenta :

   Vd. puede prefijar la posición inicial para las ventanas de este tipo de aplicaciones, así como restringir el cambio de tamaño y movimiento de sus ventanas (siempre que se ejecuten como sesión conjunta al Shell), aunque el efecto aparente de estas restricciones será algo distinto al observado con aplicaciones OS/2 nativas, ya que en este caso las restricciones solamente se pueden forzar *a posteriori*, es decir, una vez la ventana se ha movido, o ha cambiado a un estado inválido, SecureEntry volverá a restituir el estado inicial.

   No se pueden deshabilitar opciones de menú de las aplicaciones WINOS2.

   Recuerde marcar la aplicación como de tipo 'DOS'.

8. Por último, una breve descripción sobre los botones de selección del estado inicial :

   Si vd. prefija la posición y tamaño inicial de una ventana y selecciona el botón de estado inicial a 'restaurado', entonces SecureEntry forzará dicho estado, posición y tamaño una vez transcurrido el tiempo de retardo desde la creación de la ventana indicada.

   Si vd. prefija la posición y tamaño inicial de una ventana y selecciona el botón de estado inicial a 'maximizado', entonces SecureEntry forzará dicho estado, una vez transcurrido el tiempo de retardo desde la creación de la ventana indicada, pero el tamaño y la posición de la ventana resultante serán el correspondiente al estado maximizado estándar.

Si vd. prefija la posición y tamaño inicial de una ventana y selecciona el botón de estado inicial a 'minimizado', entonces SecureEntry forzará dicho estado, en la posición de minimización asignada por el sistema una vez transcurrido el tiempo de retardo desde la creación de la ventana indicada. Cuando la ventana sea subsecuentemente restaurada o maximizada, SecureEntry forzará entonces la posición y el tamaño configurados, a no ser que :

El estado nuevo (restaurado o maximizado) no esté permitido, o

El tamaño configurado sea de 1 x 1 (valor mínimo)

Resulta evidente por tanto, que para poder configurar un estado inicial determinado, este debe estar permitido en el perfil como estado válido. Por ejemplo, vd. no podrá seleccionar estado inicial 'minimizado' y a la vez impedir la opción del menú de sistema de *minimizar*.

Cuando restrinja el posicionamiento y tamaño inicial de una ventana, tenga especial cuidado con aquellas aplicaciones que hacen sus propios ajustes al mismo, pues podrían provocarse ciclos de reajuste indefinidos. Así por ejemplo, las sesiones del emulador 3270 del Communications Manager, cuando están configuradas para trabajar con fuentes de tamaño variable, detectan el cambio de tamaño de la ventana y fuerzan el calculado, según la fuente que se deba usar. En este caso se deberán configurar los emuladores para que trabajen con fuentes de tamaño fijo.

Tenga cuidado de forzar estados iniciales en ventanas de aplicación que de por sí no los soportan. Probablemente no funcionarán.

Y por último, tenga en cuenta que este componente trabaja basado en asunciones de comportamiento obtenidas por observación, que no se hallan documentadas. En principio se trata de una pieza extremadamente intrusiva, y que puede fácilmente hacer procesar a las aplicaciones casos que pudieran no estar previstos en el diseño de las mismas. El objetivo del mismo no ha sido ni podrá nunca ser el cubrir el 100% de necesidades en este área, si no el mayor porcentaje posible.

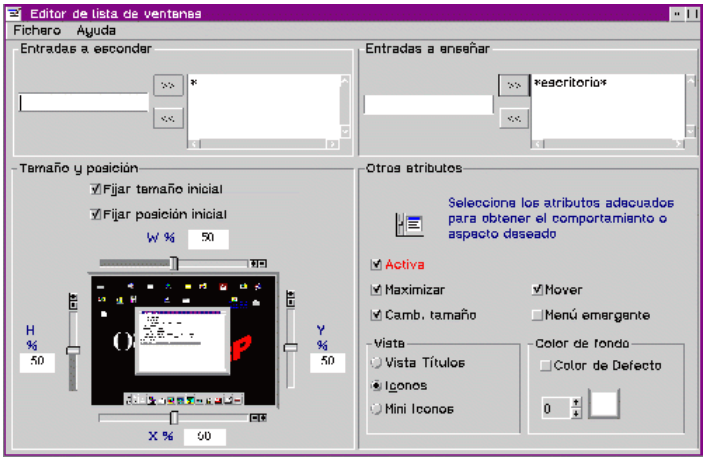
Restricciones de la lista de tareas

El componente de restricción de la lista de tareas permite configurar un perfil de personalización que, cuando se active, modifique el comportamiento estándar de la misma, tanto en cuanto a aspectos estéticos se refiere, como estableciendo un filtro en el cual se indica qué entradas deben ser visibles y cuales no, de tal modo que no se permita al usuario interactuar nada más que con las aplicaciones deseadas a través de la lista de tareas.

Para trabajar con este componente, abra la carpeta de *definición de restricciones de lista de tareas*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Para crear un perfil de seguridad para este componente, utilice el objeto modelo suministrado (*EDYWDLST.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor de restricciones de lista de tareas*, o bien haga doble click sobre el mismo. Haga las modificaciones pertinentes, y después salve el perfil modificado :



Para verificar el comportamiento de un perfil de seguridad de restricciones de lista de tareas, arrástrelo y suéltelo sobre el objeto *Test de restricciones de lista de tareas*, o bien active la función de prueba vía el menú emergente del perfil. Las restricciones y características definidas se activarán, y vd. podrá comprobar que el comportamiento de la lista de tareas sea el deseado.

Cuando configure perfiles para este componente, tenga en cuenta que :

Las listas de **procesos a esconder** y **procesos a enseñar** se utilizan para especificar cuando una nueva entrada en la lista de tareas debe ser visible o invisible. Se aplicarán las siguientes reglas:

1. Se permiten los carácteres de sustitución '*' y '?', sin importar mayúsculas/minúsculas al hacer la comparación.
2. La cadena con la que se compara puede no ser exactamente aquella que se ve en la lista de tareas, ya que la lista de tareas puede añadir información adicional a los títulos almacenados para visualizarlos. Se utiliza para establecer el filtro el título de la entrada de lista de tareas tal y como se guarda internamente. Use la utilidad EDYSWL2 para ver los verdaderos títulos almacenados.
3. En caso de que la entrada nueva **no** esté especificada en ninguna de las listas de restricciones, se dejará sin modificar (visible o invisible dependiendo de la propia aplicación).
4. En caso de que la entrada nueva esté especificada en la lista de 'entradas a enseñar', pero no en la de 'entradas a esconder', se forzará el estado de la misma a visible en la lista de tareas.
5. En caso de que la entrada nueva esté especificada en la lista de 'entradas a esconder', pero no en la de 'entradas a enseñar', se forzará el estado de la misma a invisible en la lista de tareas.
6. Si la entrada nueva está especificada en ambas listas, entonces mandará aquella lista cuya cadena sea mayor. Así por ejemplo :

```
Entradas a esconder   Entradas a enseñar
     *                   *CMD*

                         *Escrito*
```

   Esconderá todo excepto aquellas entradas que cuadren con '*CMD*' o '*Escrito*'. De igual modo :

```
Entradas a esconder   Entradas a enseñar
```

```
*CMD*                    *
*Communic*
```

Enseñará todas las entradas excepto aquellas de aplicaciones cuyos títulos cuadren con '*CMD*' o '*Communic*'.

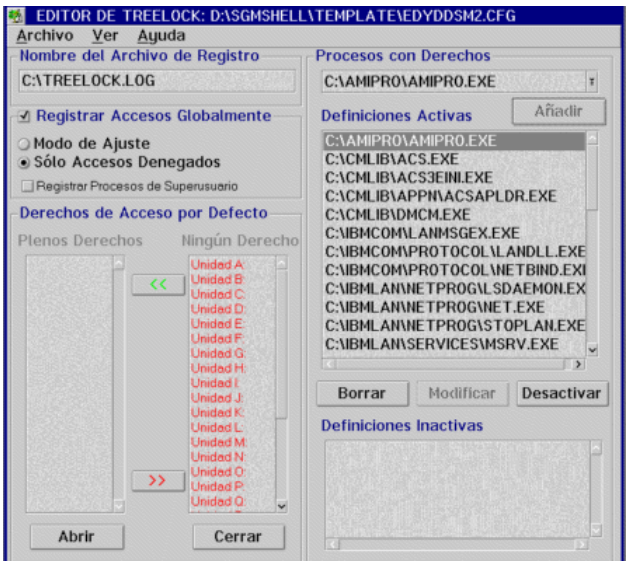
Debido a que la lista de tareas no tiene previsto el no tener ninguna entrada visible, vd. debe asegurarse de que como mínimo una entrada de la misma esté siempre visible al trabajar con este componente. En caso contrario, la tecla <ESC> no le permitirá esconder la lista de tareas. Tal vez una buena opción en caso de no desear entradas visibles sea inhibir completamente esta función del sistema, vía un perfil de restricciones que así lo especifique.

El botón 'menú emergente' le permite restringir las operaciones del usuario con las entradas de la lista de tareas, de tal modo que solo se pueda usar ésta como medio para dar control a las aplicaciones disponibles, sin poder cerrar o alterar la presentación de las mismas (mover, minimizar,...) vía el menú emergente de las entradas.

Restricciones del Treelock

El componente Treelock permite definir, a través de un perfil de control de accesos, las partes de las unidades lógicas y/o dispositivos que serán accesibles o no, una vez se haya activado el componente con un determinado perfil.

Para poder trabajar con este componente, abra la carpeta de trabajo de Treelock que está ubicada dentro de la carpeta de herramientas de SecureEntry.



Dentro de la carpeta de Treelock, encontrará:

Sombras para abrir los dos perfiles ejemplo.

Modelos para crear perfiles de Treelock y archivos de auditoría.
Un objeto programa para invocar el editor de Treelock y poder editar perfiles.
Un objeto programa para poder invocar el activador de Treelock y poder activar perfiles.

El Editor de Treelock permite editar perfiles de Treelock. Un perfil de Treelock es básicamente una lista de derechos de acceso que especifica qué recursos del sistema de archivos serán accesibles o no, una vez el perfil haya sido activado.

Observe que el archivo de auditoría de Treelock se maneja como cualquier otra componente, y, por lo tanto, puede ser asignado a un usuario o grupo a través de las herramientas de administración de grupos y usuarios.

Perfil, Introducción

Un perfil de Treelock especifica:

Qué recursos del sistema de archivos serán accesibles y cuales no.

Qué accesos al sistema de archivos serán registrados y cuales no.

El control sobre los recursos del sistema de archivos se consigue especificando una sección que define unos Derechos de Acceso por Defecto junto con otra sección que define unos Derechos de Acceso Explícitos en forma de listas de derechos de acceso para cada proceso. **Una vez el perfil se ha activado, cada vez que un proceso intenta un acceso al sistema de archivos, primero se comprueban sus derechos de acceso explícitos, y, si tiene y es posible aplicarlos, se aplican, si no, se usan los derechos de acceso por defecto del perfil.**

El control sobre la actividad de registro se consigue a través de una definición global y/o varias definiciones por proceso llamadas definiciones privadas de registro. El modo global de registro es el modo de registro por defecto, y se aplica a todos los procesos de usuario que no tengan definido un modo privado de registro, y, opcionalmente, a todos los procesos de superusuario. Tanto las definiciones globales como las privadas pueden especificar que se **registren todos los intentos de acceso al sistema de archivos, o bien, sólo aquellos que hayan sido denegados.**

Nota: un perfil de Treelock es, de hecho, un archivo de texto que debe ajustarse a una sintaxis determinada. Por lo tanto, un perfil puede contener errores sintácticos. El Editor de Treelock los detecta en tiempo de carga del perfil, y puede mostrarlos en cualquier momento a petición del usuario, facilitando la línea errónea y un mensaje de error indicativo de la posible causa.

Nota: un proceso ejecutándose en modo superusuario no está sujeto a las restricciones de Treelock.

Perfil, Procesos de Superusuario

Los procesos de superusuario son procesos lanzados fuera de sesión de usuario, y, por lo tanto, no deben verse afectados por las restricciones que especifiquen los perfiles de Treelock (los cuales siempre están relacionados con una sesión de usuario determinada). Para poder cumplir este requisito, cada vez que un proceso intenta acceder a un recurso, el Dispositivo de Treelock averigua si este proceso se está ejecutando en modo superusuario o no. Si lo está, siempre concede el acceso, independientemente de lo que el perfil activo de Treelock pueda especificar para este proceso; si no, concede o no el acceso dependiendo de lo que especifique el perfil de Treelock activo.

Así pues, los procesos de superusuario tienen siempre derechos plenos sobre todos los recursos del sistema de archivos. Esto no puede cambiarse, pero si se puede configurar el perfil de Treelock para que registre todos los accesos que hayan sido realizados por procesos de superusuario, permitiendo así monitorizar qué procesos se están ejecutando en modo de superusuario durante una sesión de usuario determinada. Vea la ayuda en línea del Editor de Treelock para saber como habilitar esta opción desde el editor de Treelock.

Perfil, Derechos de Acceso por Defecto

Puede especificar los Derechos de Acceso por Defecto de un perfil de Treelock de dos maneras distintas:

Una definición de derechos de acceso explícita asignada al nombre de proceso reservado: EXES.

Una lista de unidades lógicas, desde A hasta Z, que clasifica cada unidad como accesible o no.

Cuando un proceso P intenta acceder a un recurso R y sus derechos explícitos no son aplicables, entonces se consultan los derechos explícitos del proceso EXES, si son aplicables se aplican, si no, se consulta la lista de unidades lógicas y el acceso es concedido sólo si R está ubicado en una unidad especificada como accesible.

Perfil, Derechos de Acceso Explícitos

La **sección de derechos de acceso explícitos de un perfil de Treelock** permite definir derechos de acceso específicos de cada proceso. Es una **lista de definiciones de derechos de acceso**.

Una **definición de derechos de acceso** es una asignación de los mismos derechos de acceso a un determinado conjunto de procesos.

Los derechos de acceso se definen en dos pasos. Primero se definen los **derechos mínimos garantizados** y luego los **derechos de acceso específicos**. Los derechos mínimos garantizados son los derechos de acceso por defecto del conjunto de procesos, y se aplican sólo si los derechos específicos no pueden ser aplicados. Los derechos específicos no pueden ser más restrictivos que los mínimos garantizados, y toman la forma de una lista de derechos de acceso los elementos de la cual especifican derechos para un determinado conjunto de recursos.

El conjunto de procesos afectados por una definición de derechos de acceso se especifica a través de una ruta completa del sistema de archivos eventualmente con metacarácteres. Todos los procesos que coincidan con esa ruta pertenecen al conjunto de procesos. **Por lo tanto, un proceso P tiene derechos de acceso explícitos, si y sólo si, P pertenece a un conjunto de procesos especificado por al menos una de las definiciones de derechos de acceso (excepto EXES) del perfil.**

Derechos Mínimos Garantizados

Los derechos mínimos garantizados son los derechos de acceso por defecto del conjunto de procesos especificado por la definición de derechos de acceso. Se aplican siempre que alguno de estos procesos intenta acceder a un recurso no especificado en la lista de derechos específicos de la definición de derechos de acceso. Pueden tomar los siguientes valores:

PLENOS : los procesos tendrán derechos de acceso plenos (abrir, ejecutar, borrar, mover y creación y borrado de subdirectorios) **sobre todos los recursos** y podrán arrancar líneas de comandos.

ABRIR/EJECUTAR : los procesos tendrán derechos para abrir y ejecutar (pero no borrar, ni mover, ni crear ni borrar subdirectorios) **sobre todos los recursos que no estén mencionados en la lista de derechos específicos**, y podrán arrancar líneas de comandos.

NULOS : los procesos no tendrán derechos mínimos garantizados, y **los accesos sobre los recursos no mencionados en la lista de derechos específicos se resolverán usando la lista de unidades lógicas de los derechos de acceso por defecto** del perfil

Derechos de Acceso Específicos

La sección de derechos de acceso específicos de una definición de derechos de acceso permite definir los derechos de acceso que el conjunto de procesos afectados tendrá sobre recursos particulares, es una lista de argumentos, <**R**,**D**,**T**>, especificando el tipo de acceso que tienen los procesos sobre un conjunto de recursos determinado:

R es una ruta completa del sistema de archivos, eventualmente con metacarácteres.

Los procesos tendrán derechos de acceso, **D**, sobre todos los recursos que coincidan con esta ruta.

D son los derechos de acceso.

Los procesos tendrán derechos de acceso **D** sobre los recursos definidos por **R**. Estos derechos de acceso no pueden ser más restrictivos que los mínimos garantizados.

T es el tipo de recurso.

Se usa para modificar el conjunto de recursos especificado por **R**. Puede tomar tres valores:

archivo

El conjunto de recursos no se modifica.

Directorio

Los procesos tienen también derechos de acceso **D** sobre todos los recursos ubicados dentro de el(los) directorio(s) especificado(s) por **R**.

Subárbol

Es equivalente a especificar la ruta **R***. Los procesos tendrán también derechos de acceso **D** sobre todos los recursos contenidos en el(los) subárbol(es) que cuelguen de **R**

Nota: todas las rutas que identifican procesos o recursos en un perfil de Treelock aceptan los metacarácteres ('*' ,'?') , y pueden ser parametrizadas para independizarlas de una ubicación fija en el sistema de archivos .

Nota: vea la ayuda en línea del Editor de Treelock para saber como definir definiciones de derechos de acceso desde el Editor de Treelock .

Perfil, Definiciones Inactivas

El Editor de Treelock permite desactivar cualquier definición de derechos de acceso y cualquier definición de derechos de acceso específica.

Una definición inactiva se comporta como si no estuviera definida, sin embargo, el Editor de Treelock la reconoce y la muestra dentro del grupo de las definiciones inactivas del perfil.

Perfil, Parametrización

Todas las rutas que identifican procesos o recursos en un perfil de Treelock pueden ser parametrizadas para independizarlas de una ubicación fija en el sistema de archivos. Si se hace, un perfil se convierte también en un modelo que puede ser usado para generar fácilmente nuevos perfiles que se adapten a otras configuraciones del sistema de archivos.

La parametrización consiste en sustituir alguna subcadena de la ruta con un nombre de parámetro arbitrario.

```
c:\os2 podría ser sustituido por %os_dir%
```

```
c:\sgmshell podría ser sustituido por %sgm_shell%
```

Nota: para evitar ambigüedades, una cadena parametrizada no puede estar contenida completamente en otra cadena ya parametrizada.

Después de ser parametrizado, un perfil es todavía un perfil, la diferencia es que ahora también se puede comportar como un modelo, es decir, puede ser cargado como un modelo en el que las cadenas parametrizadas han sido sustituidas por los nombres de sus parámetros asociados, y a estos se les puede asignar nuevos valores para generar nuevos perfiles.

Nota: vea la ayuda en línea del Editor de Treelock para saber como parametrizar un perfil desde el editor de Treelock

Perfil, sintaxis ASCII

El editor de Treelock detecta los errores de sintaxis en tiempo de carga del perfil. Una vez el perfil ha sido cargado, los errores de sintaxis pueden ser visualizados en cualquier momento: se muestran las líneas erróneas y para cada error se da un mensaje orientativo del problema.

Un perfil con errores de sintaxis no es fiable: el editor de Treelock no salva perfiles con errores de sintaxis, por lo tanto, ante un perfil sintácticamente erróneo, cabe suponer que el perfil ha sido modificado y editado a mano.

A continuación se da la gramática a la que se debe ajustar un perfil de Treelock, junto con algunos apuntes semánticos para cada construcción sintáctica:

```
; Esto es un comentario, y llega hasta el final de línea

; Sección de parámetros GLOBALES
; ------------------------------

[Set Debug=d:\rutacompleta\mobrearchivo]

; "set debug" establece el nombre del archivo de registro. Este archivo se
; recrea cada vez que se carga el sistema o se activa un perfil de Treelock.
; Contiene todas las acciones que el dispositivo de Treelock registra. Si no se especifica,
; no se registra nada.

[Set Globdebug={a|d}]
```

```
   ; "set globdebug" permite especificar el modo de registro global: todos los accesos o sólo
los denegados

   ;           ZYXWVUTSRQPONMLKJIHGFEDCBA
   [Set Drives=00000011011011001001010111]

   ; "set drives" es la lista de unidades lógicas que especifica cuales son
   ; accesibles (1) y cuales no (0). Esta variable es consultada por el dispositivo de
Treelock
   ; cuando el acceso a un recurso no puede ser resuelto por ninguna otra vía.

   [Set Mode={s|c}]

   ; "set mode" establece el acceso por defecto para los procesos no especificados,
   ; ningún derecho (STRICT), todos los accesos serán denegados; o plenos derechos
   ; (CALCULATED), todos los accesos serán concedidos. El dispositivo de Treelock
   ; consulta ésta variable sólo si la variable global "set drives" no ha  sido declarada.
   ; NOTA : el Editor de Treelock no utiliza ésta variable porque siempre salva los perfiles
   ; con la variable global DRIVES  definida.
   ; NOTA : esta línea NO deshabilita las restricciones implícitas de Treelock
   ; (i.e, acceso al archivo config.sys para usuarios normales).

   ; Sección específica POR PROCESO
   ; ------------------------------

   [A|D] {F|O|Y|N} <ejecutable|EXES|VDMS> [args]*
   [args] = [A|R|N] {F|D|S} <rutaarchivo>

   ; A = flag de análisis para esta línea: todos los accesos realizados por este proceso
   ;     serán registrados y siempre concedidos.
   ; D = flag de ajuste para esta línea: todos los accesos realizados por este proceso
   ;     que hayan sido denegados serán registrados.
   ; F = este <ejecutable> tiene plenos derechos de acceso: abrir, ejecutar, borrar, mover y
creación
   ;     y borrado de subdirectorios.
   ; O = este <ejecutable> tiene derechos de abertura y ejecución, pero no para borrar, ni
   ;     mover,  ni crear ni borrar subdirectorios.
   ; N = este <ejecutable> no podrá arrancar líneas de comandos.
   ; Y = este <ejecutable> podrá arrancar líneas de comandos.
   ;     Este es el valor por defecto.
   ; <ejecutable> = ruta completa del archivo ejecutable (puede contener
   ;                los metacarácteres '*' y '?').
   ; <VDMS>       = nombre reservado que designa cualquier proceso que se ejecute en modo Real
   ; <EXES>       = nombre reservado que designa todos los ejecutables que no hayan sido
mencionados
   ;                     (incluidos los que se ejecutan en modo Real).

   ; Cada proceso puede tener ninguno o algún recurso especificado. Cada recurso tiene
   ; dos o tres argumentos:
   ; o Opcionalmente el tipo de acceso a un <rutaarchivo>:
   ;   o A significa que todos los accesos están permitidos
   ;   o R significa que sólo los accesos de lectura están permitidos
   ;   o X significa que sólo los accesos de ejecución están permitidos
   ;   o N significa que ningún acceso está permitido
   ;   A es el valor por defecto si el parámetro anterior no se especifica.
   ; o Como interpretar <rutaarchivo>:
   ;   o F significa acceso a un archivo.
   ;   o D significa acceso a un directorio.
   ;   o S significa acceso a todos los archivos del directorio y sus subdirectorios.
   ; o El <rutaarchivo> que puede contener los metacarácteres '*' y '?'.
   ;
   ; Puede partir una línea en más líneas usando el carácter '/'
```

Perfil, Configuración de la Actividad de Registro

A través de un perfil de Treelock se puede configurar la actividad de registro que debe llevarse a cabo una vez el perfil se haya activado. Puede especificar qué procesos quiere monitorizar y cuales de sus accesos quiere registrar.

Dado un proceso, existen dos posibles modos de registro:

Registrar sólo los accesos denegados.

Registrar todos los accesos (y concederlos, sin importar lo que el perfil diga al respecto)

Un modo de registro puede ser definido global o privadamente. Un modo de registro privado asigna un modo de registro a una definición de derechos de acceso y es válida para todos los procesos de **usuario** afectados por la definición; un modo de registro global asigna un modo de registro a todos los procesos de **usuario** que no tengan un modo privado de registro definido, y, opcionalmente, a todos los procesos de superusuario.

Nota: una definición privada de registro no se aplica a un proceso ejecutándose en contexto de superusuario. Los procesos de superusuario sólo pueden ser monitorizados si ello se especifica en la definición global de registro del perfil.

Nota: vea la ayuda en línea del editor de Treelock para saber como configurar la actividad de registro desde el editor del Treelock.

Diseñando Perfiles de Treelock

Para asignar derechos de acceso a los recursos del sistema de archivos, el administrador del sistema debe editar un perfil de Treelock. Este perfil es salvado como un archivo ASCII por el editor de treelock que el dipositivo de Treelock es capaz de leer e interpretar al ser cargado, o al activar/desactivar un perfil a través de la API de Treelock.

Debe ser consciente de que el proceso de cerrar el sistema a accesos no privilegiados se basa en el ajuste de los perfiles mediante el método de "ensayo y error". Por ejemplo, si quiere que el usuario pueda ejecutar el programa Amipro/2, pero permitiéndole acceder sólo a algunos directorios de trabajo , tendrá que testear repetidamente su perfil hasta que esté seguro de que:

1. Ha identificado todos los recursos que Amipro/2 utiliza internamente, y le ha dado a este programa derechos de acceso plenos sobre esos recursos que crea o actualiza, y derechos de acceso de sólo lectura sobre aquellos que no necesita crear ni actualizar, pero sí leer.
2. Ha identificado todos los recursos que Amipro/2 utiliza como resultado de que el usuario acceda a diferentes directorios o archivos. Debe dar a Amipro/2 los derechos de acceso apropiados para que pueda gestionar esos recursos y a la vez su sistema quede protegido.

Puede configurar las aplicaciones dándoles derechos de acceso específicos a éstas, y luego estableciendo los derechos de acceso para el resto de aplicaciones no especificadas (todas tendrán los mismos derechos de acceso).

Los programas que se ejecutan en VDMs, incluso los que se ejecutan en el subsistema Windows, no pueden ser distinguidos el uno del otro ya que el Kernel del OS/2 Warp tan sólo ve instancias diferentes del mismo proceso ejecutándose en modo real. Por lo tanto, los programas que se ejecutan en modo real se identifican con el nombre reservado de proceso **VDMS**. Para estos programas, si el dispositivo de Treelock no puede resolver un acceso basándose en la definición de derechos de acceso asociada a VDMS, tratará de resolverlo vía la definición de derechos de acceso asociada a EXES.

El proceso de cerrar el sistema depende fuertemente de sus necesidades. Puede necesitar un sistema relativamente cerrado en el que se especifican restricciones sobre algunos procesos concretos y el resto de procesos se dejan sin casi ninguna restricción; o puede necesitar un sistema más cerrado, en el que se especifican restricciones sobre la mayoría de procesos, y no se dejan puertas abiertas para casi ningún proceso. El primer caso lleva a un sistema fácil de configurar; el segundo, requiere más tiempo para ser ajustado correctamente. Para facilitar esta tarea **el editor de Treelock le permite activar los perfiles que edita y visualizar los archivos de registro resultantes, de tal manera que la información de registro puede ser utilizada para completar el perfil.**

En cualquier caso, el mejor método que puede seguir para ajustar un perfil, es:

1. Especifique un nombre de archivo de registro para el perfil.

2. Especifique el modo global de registro para que registre sólo los accesos denegados.
3. Especifique todas las unidades lógicas como accesibles (sistema abierto).
4. Especifique, para el proceso que quiere ajustar, un modo privado de registro que registre todos los accesos y los conceda.
5. Quítele al proceso que quiere ajustar los derechos mínimos garantizados (que sean los por defecto del perfil)
6. Active el perfil y use extensivamente el programa que quiere ajustar.
7. Edite el archivo de log desde el editor de Treelock y observe los recursos que han sido accedidos por el proceso que está ajustando.
8. Añada estos recursos a la definición de derechos de acceso asociada al proceso que está ajustando con los derechos específicos que más le convengan (puede hacerlo directamente desde el editor del archivo de registro)
9. Cambie los derechos mínimos garantizados del proceso que ajusta a los que más le convengan.
10. Vuelva al paso 6 hasta que esté seguro de haber ajustado correctamente el programa.

Testeando Perfiles de Treelock

El editor de Treelock le permite activar y desactivar perfiles de Treelock sin necesidad de salir de él. Activar un perfil significa aplicar todas las restricciones que especifica, por lo tanto hay que ir con cuidado si se está probando un perfil de un sistema cerrado.

Para garantizar una operativa normal, el editor de Treelock se da a sí mismo plenos derechos en todos los perfiles que activa (añade la línea "F <rutadirectorio>\tlcked.exe"). Esta es la única diferencia entre una activación real y una hecha desde el editor de Treelock.

Por otro lado, el perfil activo de Treelock, sólo puede ser desactivado mediante la activación de otro perfil, por lo tanto, el editor de Treelock desactiva los perfiles activando el perfil que estaba activo antes de ellos. Así, desactivar un perfil desde el editor de Treelock es, de hecho, restaurar el perfil de Treelock que se había asignado al usuario actual en tiempo de conexión.

Vea la ayuda en línea del editor de Treelock para saber como activar/desactivar perfiles desde el editor de Treelock.

Perfil, Ejemplo 1

La configuración de EDYDDSM1.CFG no impone restricciones en ningún acceso, y usa como archivo de registro c:\treelock.log:

```
set debug=c:\treelock.log
set globdebug=a
set mode=c
```

Perfil, Ejemplo 2

La configuración de EDYDDSM2.CFG impone algunas restricciones en los accesos, y registra sólo los accesos denegados en el archivo c:\treelock.log. Los procesos no especificados se resuelven según la definición EXES; y si ésta no es aplicable, como el modo es estricto, el acceso es denegado:

```
set debug=c:\treelock.log
set globdebug=d
set mode=s

; ========================
```

```
   ; OS/2 Base (imprescindible)
   ; ========================

   ; Dar a c:\os2\pmshell.exe derechos de abrir/ejecutar sobre cualquier recurso en c:\spool,
   ; k:\post and h:\ . Dar derechos plenos a c:\os2\os2.ini, c:\os2\os2.###,
   ; c:\os2\os2.!!!, c:\os2\os2sys.ini, c:\os2\os2sys.###, c:\os2\os2sys.!!!,
   ; c:\os2\pmdiary.###, c:\os2\pmdiary.!!!, c:\os2\pmdiary.ini,
   ; c:\os2\install\reinstal.ini, c:\os2\install\reinstal.### and
   ; c:\os2\install\reinstal.!!!

   O c:\os2\pmshell.exe            s c:\spool           s k:\post     s H:   /
     f c:\os2\os2.ini              f c:\os2\os2.###     f c:\os2\os2.!!!     /
     f c:\os2\os2sys.ini           f c:\os2\os2sys.###  f c:\os2\os2sys.!!!  /
     f C:\OS2\PMDIARY.###          f C:\OS2\PMDIARY.!!! f C:\OS2\PMDIARY.INI /
     f c:\os2\install\reinstal.ini f c:\os2\install\reinstal.###             /
     f c:\os2\install\reinstal.!!!

   ; Dar a c:\os2\harderr.exe, c:\os2\chkdsk.com and c:\os2\pmspool.exe
   ; derechos plenos.

   F c:\os2\system\harderr.exe
   F c:\os2\chkdsk.com
   F c:\os2\pmspool.exe



   ; ======================
   ; OS/2 Base (opcionales)
   ; ======================

   ; No permitir que c:\os2\apps\pmdcalc.exe ejecute líneas de comando, dándole plenos
   ; derechos sobre c:\os2\apps\dll\pmdiary.dll, c:\os2\pmdiary.###,
   ; c:\os2\pmdiary.ini, c:\os2\pmdiary.!!!, c:\os2\help\pmdiary.hlp and
   ; c:\os2\help\hmhelp.hlp

   n C:\OS2\APPS\PMDCALC.EXE  f C:\OS2\APPS\DLL\PMDIARY.DLL         /
     f C:\OS2\PMDIARY.### f C:\OS2\PMDIARY.INI f C:\OS2\PMDIARY.!!! /
     f C:\OS2\HELP\pmdiary.hlp f C:\OS2\HELP\HMHELP.HLP

   ; No permitir que c:\os2\apps\pmsticky.exe ejecute líneas de comandos, dándole
   ; plenos derechos sobre c:\os2\apps\dll\pmdiary.dll, h:\os2\pmdiary.###,
   ; h:\os2\pmdiary.ini, h:\os2\pmdiary.!!!, c:\os2\help\pmdiary.hlp,
   ; c:\os2\help\hmhelp.hlp and h:\pmsticky.$$p

   n C:\OS2\APPS\PMSTICKY.EXE f C:\OS2\APPS\DLL\PMDIARY.DLL         /
     f H:\OS2\PMDIARY.### f H:\OS2\PMDIARY.INI f H:\OS2\PMDIARY.!!! /
     f C:\OS2\HELP\pmdiary.hlp f C:\OS2\HELP\HMHELP.HLP f H:\PMSTICKY.$$P

   ; No permitir que c:\os2\more.com ejecute líneas de comandos, dándole
   ; plenos derechos sobre c:\os2\system\oso001.msg and c:\oso0001.msg

   N c:\os2\MORE.COM f C:\OS2\SYSTEM\OSO001.MSG f c:\oso0001.msg

   ; La siguiente línea impediría que cmd.exe arrancará otra cmd.exe,
   ; le negaría todos los accesos sobre el programa format.com, le daría plenos derechos
   ; sobre cualquier otro .exe y .com en c:, derechos de sólo lectura sobre treelock.log
   ; y plenos sobre la unidad d:.
   ; Con esta línea, los exes y coms distintos de format.com que estuvieran en c: podrían
   ; ser creados y borrados, pero no se podrían crear ni borrar ningún otro tipo de archivos
ni
   ; directorios. Para mantenter las mismas restricciones, pero permitiendo la ejecución de
   ; líneas de comandos, sólo debería cambiar la "n" inicial por una "y"

   ;n c:\os2\cmd.exe n f c:\os2\format.com                    /
   ;  a s c:\*.exe a s c:\*.com r f c:\treelock.log a s d:

   ; La siguiente línea permitiría que cmd.exe pudiera arrancar, abrir o crear cualquier
   ; archivo, incluso aunque añadiera algunas restricciones específicas de recursos. No podría
   ; borrar ni mover archivos, ni tampoco crear ni borrar directorios.

   ;o c:\os2\cmd.exe

   ; La siguiente línea daría a la cmd plenos derechos sobre la unidad d:. Como no se dice
nada
   ; sobre otras unidades lógicas, no se daría acceso a ellas. (modo estricto)
```

```
   ;n c:\os2\cmd.exe a s d:

   ; La siguiente línea hace que cmd.exe se comporte como en la línea anterior, pero podría
arrancar
   ; otra línea de comandos.

   ;y c:\os2\cmd.exe a f c:\os2\cmd.exe a s d:

   ; La siguiente línea no impone ninguna restricción a la línea de comandos:

   f c:\os2\cmd.exe



   ; ==============
   ; Sentencia VDMS
   ; ==============

   ; Dar a cualquier programa ejecutándose en modo real derechos de sólo lectura sobre
C:\CONFIG.SYS y
   ; C:\STARTUP.CMD, plenos derechos sobre C:\DOSUTILS y todos sus subdirectorios,
   ; plenos derechos sobre C:\OS2\MDOS\DOSKRNL y C:\OS2\BOOT\VIOTBL.DCP, etc.
   ; Obsérvese que no se da acceso a la unidad A:,
   ; que se usan metacarácteres,
   ; y que esta sentencia afecta al programa Anitvirus de IBM para DOS y DW4.

   N VDMS R F C:\CONFIG.SYS              R F  C:\STARTUP.CMD                      /
      S  C:\DOSUTILS                     F  C:\OS2\MDOS\DOSKRNL                   /
     A F  C:\OS2\BOOT\VIOTBL.DCP          F  C:\OS2\SYSTEM\COUNTRY.SYS             /
     A F  C:\OS2\MDOS\COMMAND.COM         F  C:\OS2\MDOS\APPEND.EXE                /
     A F  C:\OS2\MDOS\WINOS2\WINOS2.COM    F C:\OS2\MDOS\WINOS2\SYSTEM\OS2K386.EXE  /
     A F  C:\OS2\MDOS\SYSTEM\*.DRV        F  C:\OS2\MDOS\WINOS2\*.INI              /
     A F  C:\OS2\MDOS\SYSTEM\*.FON                                                /
     A F  C:\OS2\MDOS\WINOS2\*.GRP                                                /
     A F  C:\OS2\MDOS\WINOS2\SYSTEM\SETUP.INF                                     /
     A D  C:\OS2\MDOS                                                             /
     N S A:                                                                      /
     a s  c:\ibmav                                                               /
     N F  C:\DW4\*.doc                                                           /
     N F  C:\DW4\*.rft                                                           /
     A F  C:\DW4\*.LST                                                           /
     A F  C:\DW4\*.PG1                                                           /
     A F  C:\DW4\*.PRF                                                           /
     A F  C:\DW4\DW4ODIR.BAT                                                     /
     A F  C:\*.$$P                                                               /
     R S C:

   ; ==============
   ; Sentencia EXES
   ; ==============

   ; Dar a los EXES no especificados acceso a una línea de comandos, y ningún acceso sobre
   ; C:\CONFIG.SYS, derechos de sólo lectura sobre C:\STARTUP.CMD, plenos derechos
   ; sobre el directorio C:\TOOLS, etc.
   ; Nótese que se usan metacarácteres.

   N EXES N F C:\CONFIG.SYS   R F C:\STARTUP.CMD          N F  C:\AUTOEXEC.BAT  /
     A D C:\TOOLS             R F  C:\OS2\HELP\EPM.HLP       S  C:\OS2\APPS     /
     A D C:\OS2\APPS\DLL        S  C:\OS2\DLL                S  C:\OS2UTILS     /
     N S A:                   N F  C:\OS2\MDOS\WINOS2\*.INI

   ; ==========
   ; Lan Server
   ; ==========

   F c:\os2\epw.exe
   F C:\IBMLAN\NETPROG\LSDAEMON.EXE
   F C:\IBMLAN\NETPROG\STOPLAN.EXE
   F C:\IBMLAN\NETPROG\NET.EXE
   F C:\IBMLAN\SERVICES\WKSTA.EXE
   F C:\IBMLAN\SERVICES\MSRVINIT.EXE
   F c:\IBMLAN\SERVICES\MSRV.EXE
   N C:\MUGLIB\MUGLRQST.EXE  S C:\MUGLIB S C:\IBMLAN
```

```
;====================================================================
; Communications Manager
;====================================================================

F c:\ibmcom\lanmsgex.exe
F c:\ibmcom\protocol\netbind.exe
F c:\ibmcom\protocol\LANDLL.EXE
n c:\CMLIB\DMCM.EXE          S C:\CMLIB
n C:\CMLIB\ACS.EXE           S C:\CMLIB F C:\IBMLVL.### F C:\IBMLVL.INI F C:\IBMLVL.!!!
n C:\CMLIB\APPN\ACSAPLDR.EXE S C:\CMLIB
N C:\CMLIB\ACS3EINI.EXE      S C:\CMLIB F C:\OS2\HELP\HMHELP.HLP

; ==========
; OS2 AmiPro
; ==========

N C:\AMIPRO\AMIPRO.EXE          A D C:\AMIPRO                          /
A F C:\AMIPRO\ICONS\*.BMP                                             /
A F C:\AMIPRO\ICONS\*.TBL       A F C:\AMIPRO\ICONS\*.SMI              /
A F C:\AMIPRO\MACROS\*.DLG      A F C:\AMIPRO\MACROS\*.SMM             /
A F C:\AMIPRO\STYLES\*.STY      A F C:\AMIPRO\DRAWSYM\*.SDW            /
A F C:\OS2\AMI*.*               A D C:\OS2\DLL                         /
A F C:\OS2\*.BIN                A S C:\SPOOL                           /
A F C:\OS2\HELP\HMHELP.HLP      A D C:\PSFONTS                         /
A F C:\OS2\INSTALL\SYSLEVEL.OS2 A F C:\OS2\SYSTEM\COUNTRY.SYS          /
A F C:\OS2\MDOS\WINOS2\*.INI    A F c:\amipro\teller\*.sam              /
N S C:

; ============
; OS2 IbmWorks
; ============

n c:\ibmworks\ibmworks.exe   a f c:\ibmworks\ibmworks.ini               /
                            a f  c:\ibmworks\ibmworks.hlp              /
                            a f  c:\os2\help\hmhelp.hlp                /
                            a f  c:\os2\dll\*.drv                      /
                            a f  c:\os2\dll\*.dev                      /
                            a f  c:\os2\dll\*.prf                      /
                            a f  c:\ibmworks\*.def                     /
                            a f  c:\ibmworks\*.tmp                     /
                            a s  c:\delete                             /
                            a f  c:\ibmworks\*.ctn                     /
                            a s  c:\psfonts                            /
                            a s d:

N c:\ibmworks\fpwpim.exe     a f c:\ibmworks\ibmworks.ini               /
                            a f  c:\ibmworks\fpwpim.*                  /
                            a f  c:\os2\help\hmhelp.hlp                /
                            a f  c:\ibmworks\*.tmp                     /
                            a s  c:\delete                             /
                            a s  c:\ibmworks\DATA                      /
                            a s  c:\psfonts                            /
                            a s d:

N c:\ibmworks\fpwmon.exe     a f c:\ibmworks\ibmworks.ini               /
                            a f  c:\ibmworks\fpwpim.*                  /
                            a f  c:\os2\help\hmhelp.hlp                /
                            a f  c:\ibmworks\*.tmp                     /
                            a s  c:\delete                             /
                            a s  c:\ibmworks\DATA                      /
                            a s  c:\psfonts                            /
                            a s d:


; =============
; OS2 Lotus 123
; =============

n C:\LOTUS\123G\123G.EXE  S C:\LOTUS\123G S D:\DADES\123 D C:\PSFONTS     /
F C:\OS2\SYSTEM\OSO001.MSG

; ========
; FaxWorks
; ========

N c:\PBA\FXSVIEW.EXE   s c:\PBA f M:\FAXWORKS\FAX.LOG
```

```
N G:\FAXWORKS\FAXWORKS.EXE  S G:\FAXWORKS  S C:\FAXWORKS                  /
 F M:\FaxWorks\Fax.log  F M:\FaxWorks\User.Spl

; =====================
; Other  OS2 applications
; =====================

n c:\os2\view.exe  a s c:\*.inf a f c:\os2\viewdoc.exe

N C:\OS2\VIEWDOC.EXE  a s c:\*.inf a s c:\*.cp S C:\OS2\HELP             /
  f C:\OS2\SYSTEM\COUNTRY.SYS   f C:\OS2\VIEWDOC.EXE


f m:\tools\inie.exe
f m:\tools\inimaint.exe
```

Resolución de la Ambigüedad

Un perfil de treelock puede ser ambiguo por dos razones:

Existe un proceso que pertenece a más de una definición de derechos de acceso.

Existe un recurso que pertenece a más de un elemento de la lista de derechos específicos de una definición de derechos de acceso.

El problema proviene del hecho de que dos rutas del sistema de archivos (con metacarácteres) pueden tener intersección no nula. Todos los procesos o recursos pertenecientes a este conjunto estarán sujetos a ambigüedad porque más de una definición puede ser aplicada para resolver sus accesos.

La mejor solución sería aplicar la definición que se asociará a la ruta más específica, pero debido a la inherente complejidad de ésta solución, se ha implementado la siguiente aproximación: Siempre que un proceso trata de acceder a un recurso, el dispositivo de Treelock empieza a recorrer secuencialmente la lista de definiciones de derechos de acceso (en el orden en que aparecen en el perfil ASCII). La primera definición en la que coinciden la ruta de la definición con la ruta del proceso que accede es la que se aplica. De la misma forma se recorre la lista de derechos específicos de una definición de derechos de acceso, pero en este caso, lo que debe coincidir es la ruta del recurso que es accedido.

Sabiendo esto, todo lo que se necesita es saber que método de ordenación utiliza el editor de Treelock para salvar el perfil ASCII.

La ordenación se realiza sobre la ruta asociada a la definición de derechos de acceso, y el algoritmo de ordenación es el que sigue:

Las rutas sin metacarácteres se guardan primero.

Las rutas con metacarácteres se guardan luego siguiendo el siguiente esquema:

Las más largas se guardan primero.

Para las que tienen igual longitud, se aplica la ordenación alfabética especial: x<?<* (donde x es cualquier carácter que no sea '?' ni '*')

Modelos

Un modelo es simplemente un perfil de Treelock que el editor de Treelock ha cargado como modelo. En tiempo de carga el editor sustituye todas las cadenas parametrizadas del perfil por los nombres de parámetros asociados a ellas , y asigna valores por defecto a cada uno de estos parámetros. Habitualmente el valor por defecto de un parámetro es la propia subcadena que el parámetro ha sustituido en tiempo de carga; pero si el

nombre del parámetro coincide con el nombre de una variable de entorno definida en tiempo de carga, el valor por defecto asignado es el valor de ésta variable de entorno. Esto permite asociar parámetros con variables de entorno.
Nota: un perfil no parametrizado es de hecho un modelo, pero un modelo sin parámetros

Puede asignar nuevos valores a los parámetros para adaptar el perfil a múltiples configuraciones del sistema de archivos. Observe que si el valor asignado a un parámetro es igual al nombre de una variable de entorno, el valor que finalmente se le asigna no es el nombre de la variable, sino el valor de la misma.

Para generar perfiles a partir de modelos debe
fusionar el modelo con un perfil de Treelock. La operación de fusión añade las definiciones de derechos de acceso del modelo a las del perfil con los parámetros sustituídos por sus valores actuales, pero sin modificar ningún otro dato del perfil. A través de esta operación puede crear nuevos perfiles (si el perfil con el que se fusiona está vacío) o actualizar fácilmente perfiles ya existentes.

Nota: vea la ayuda en línea del editor de Treelock para saber como trabajar con modelos desde el editor.

El archivo de Registro

El archivo de registro asociado a un perfil de Treelock es especialmente útil para poder ajustar el perfil. Tiene el siguiente formato de línea:

Resultado: puede ser :

Ok: el acceso ha sido concedido.

Nok: el acceso ha sido denegado.

Nombre del Proceso: ocho carácteres como máximo especificando el nombre del proceso que ha realizado el intento de acceso:

Información sobre la resolución del acceso: puede ser :

La ruta asociada a la definición de derechos de acceso del perfil que se ha usado para resolver el acceso.

SUPERUSER: el proceso se estaba ejecutando en contexto de superusuario (por lo que el acceso se concedió).

VACÍO: se aplicaron los derechos de acceso por defecto del perfil para resolver el acceso.

Tipo de Acceso intentado: puede ser:

DEL: borrar.

REN: renombrar.

EXECP: crear un proceso.

OPEN: abrir.

MKDIR: crear un directorio.

RMDIR: borrar un directorio.

CHDIR: cambiar de directorio.

FINDF: ejecutar un FindFirst.

FINDN: ejecutar un FindNext.

FINDV: ejecutar un Find desde una DOS Box.

Flags: puede ser una combinación de los siguientes (y son posicionales):

AN: el proceso tenía el flag de análisis especificado.

DB: el proceso tenía el flag de ajuste especificado.

BX: el proceso se estaba ejecutando en modo Real.

DA: debe ignorar este flag.

OE: el proceso tenía derechos mínimos garantizados de abertura

NC: el proceso no podía arrancar líneas de comandos.

FA: el proceso tenía plenos derechos

NA: el proceso no tenía derechos mínimos garantizados

Nombre completo de recurso: el nombre completo del recurso que se ha intentado acceder.

Vea el siguiente ejemplo:

```
Nok CMD  C:\OS2\*     OPEN  '  DB      NA' A:\
Nok E                 OPEN  '  DB      NA' C:\CONFIG.SYS
ok  E   SUPERUSER     EXECP '  DB      NC' C:\OS2\CMD.EXE
```

El ejemplo dice:

A una línea de comandos se le denegó un acceso a la unidad A:, y se usó la definición de derechos de acceso asociada a "c:\os2*" para resolver el acceso.

Al programa E se le denegó un acceso al archivo C:\CONFIG.SYS, y se usaron los derechos por defecto del perfil para resolver el acceso.

Al programa E, se le permitió arrancar una línea de comandos porque se ejecutaba en modo de superusuario.

El editor de Treelock le permite visualizar cualquier archivo de registro como un archivo de texto o como un archivo estructurado. Como archivo de texto, el archivo de registro se visualiza tal cual es y no puede ser modificado; como archivo estructurado, los contenidos son interpretados de manera que pueda usar la información para poder ajustar el perfil actualmente cargado por el editor de Treelock. El visualizador de archivos de registro muestra toda la información clasificando los accesos registrados según el proceso que los realizó, y según fueron concedidos o no, y le permite usar las rutas de los procesos y recursos visualizados para poder añadirlos directamente al perfil actualmente cargado por el editor de Treelock.

Nota: vea la ayuda en línea del editor de Treelock para saber como visualizar y usar los archivos de registro desde el editor de Treelock.

El archivo de Auditoría

El archivo de auditoría registra sólo los accesos denegados. Este archivo contiene lo siguiente:

Cabecera (opcional):

La palabra reservada TLOCK_AUDIT: especifica que este archivo es un archivo de auditoría de Treelock.

La palabra reservada MAX_LINES: especifica el número máximo de líneas que el archivo puede contener. El archivo se purga cada vez que se abre. Si no se especifica, se mantendrán las 1000 líneas más recientes.

Datos de cada acceso:

TimeStamp: fecha y hora del acceso denegado.

UserID: identificador del usuario que realizó el acceso.

Administrador: si el usuario que realizó el acceso era administrador o no.

Nombre de Proceso: ocho carácteres como máximo especificando el nombre del proceso que realizó el acceso.

Tipo de Acceso: puede ser:

DEL: borrar.

REN: renombrar.

EXECP: crear un proceso.

OPEN R/O: abrir para sólo lectura.

OPEN W/O: abrir para escritura.

OPEN R/W: abrir para lectura/escritura.

OPEN DLL: abrir una DLL.

MKDIR: crear un directorio.

RMDIR: borrar un directorio.

CHDIR: cambiar de directorio.

FINDF: ejecutar un FindFirst.

FINDN: ejecutar un FindNext.

FINDV: ejecutar un Find desde una DOS Box.

Nombre Recurso: el nombre completo del recurso que se intentó acceder.

Vea el siguiente ejemplo:

```
MAX_LINES 100
07-08-1996 16:25:42 USER_A    No Admin E        OPEN R/W C:\CONFIG.SYS
07-08-1996 16:25:42 USER_A    No Admin TEDIT    OPEN R/O C:\CONFIG.SYS
07-08-1996 16:25:43 USER_A    No Admin CMD      FINDF    C:\CONFIG.SYS
```

La cabecera dice que este archivo será purgado cada vez que se abra, dejando sólo las 100 líneas más recientes.

Los datos dicen que al usuario USER_A, que no es administrador, se le denegó el acceso al archivo C:\CONFIG.SYS por tres veces:

La primera, intentando abrirlo para lectura/escritura desde el programa E

La segunda, intentando abrirlo para sólo lectura desde el programa TEDIT

La tercera, intentando averiguar si existía o no desde una línea de comandos (probablemente con un comando DIR).

Ejemplos de Utilización

Esta sección muestra como construir tres perfiles habituales de Treelock:

1. **Esconder un directorio a un usuario**

2. **Restringir un usuario a un directorio de trabajo**
3. **Dar a un usuario derechos de sólo ejecución sobre un directorio de aplicaciones**

Para **esconder un directorio a un usuario** debe:

1. Dar acceso a todas las unidades lógicas
2. Especificar la definición de derechos de acceso asociada a EXES sin derechos mínimos garantizados
3. Añadir a la lista de definiciones específicas de la definición EXES el directorio que quiere esconder, con:

   Derechos de acceso = ninguno

   Tipo de Recurso = subárbol

Veamos por qué funciona: cualquier intento de acceder un recurso ubicado fuera del directorio escondido se resuelve usando la lista de acceso de unidades lógicas porque la definición EXES no tiene derechos mínimos garantizados y su lista de derechos específicos no incluye al recurso accedido. Como todas las unidades se han especificado accesibles el acceso se concede. Sin embargo, si un proceso intenta acceder al directorio escondido, la definición EXES puede ser aplicada para resolver el acceso, y como especifica derechos nulos sobre el recurso, el acceso se deniega.

Nota: el recurso debe ser de tipo "subárbol" para asegurar que todos los subdirectorios también se esconderán. Se podía también haber especificado el tipo de recurso como "archivo" y la ruta de recurso como "dir_a_esconder*"

Para **restringir un usuario a un directorio de trabajo** debe:

1. Cerrar los accesos a las unidades lógicas (excepto la A si quiere que el usuario pueda usar disquetes)
2. Especificar la definición EXES sin derechos mínimos garantizados
3. Añadir a la lista de definiciones específicas de la definición EXES el directorio de trabajo, con:

   Derechos de acceso = plenos

   Tipo de Recurso = subárbol

De nuevo, cualquier intento de acceso fuera del directorio de trabajo se resuelve usando la lista de acceso de las unidades lógicas porque la definición EXES no tiene derechos mínimos garantizados y su lista de definiciones específicas no incluye el recurso accedido. Como la lista de unidades lógicas especifica que las unidades no son accesibles, el acceso se deniega. Sin embargo, si un proceso intenta acceder a un recurso dentro del subdirectorio de trabajo, la definición EXES si puede ser aplicada para resolverlo, y como especifica plenos derechos sobre el recurso, el acceso es concedido.

Nota: el recurso debe ser de tipo "subárbol" para permitir que el usuario pueda trabajar con subdirectorios dentro de su directorio de trabajo.

Dar derechos de sólo ejecución sobre un directorio de aplicaciones

Se supone que se quiere un sistema cerrado (la unidad c: no accesible por defecto) y que el nombre del directorio donde residen las aplicaciones es "c:\exes". Se quiere que el usuario pueda ejecutar esas aplicaciones, pero que no pueda borrarlas. Por lo tanto, se debe:

1. Establecer la unidad c: como no accesible por defecto.
2. Especificar la definición EXES sin derechos mínimos garantizados.
3. Añadir "c:\exes" a la lista de definiciones específicas de EXES con:

   Derechos de acceso = ejecución

Tipo de Recurso = Directorio

Ahora el usuario podría ejecutar cualquier aplicación ubicada en el directorio "c:\exes" y no podría borrarla, pero no es suficiente. Se debe también ajustar cada aplicación que el usuario va a poder ejecutar. Por ejemplo, la aplicación "my_app.exe" podría necesitar modificar un archivo INI ubicado en el directorio "c:\exes". Ahora no podría hacerlo porque "my_app.exe" resolvería sus accesos vía la definición EXES que le daría sólo ejecución sobre los archivos contenidos en "c:\exes". Por lo tanto se debería:

4. Añadir "c:\exes\my_app.exe" a la lista de definiciones de derechos de acceso del perfil sin derechos mínimos garantizados.
5. Añadir "c:\exes\my_app.ini" a la lista de derechos específicos de la definición anterior, con:

   Derechos de acceso=plenos

   Tipo de Recurso=archivo

La API de Treelock

La API de Treelock tiene tres puntos de entrada definidos en EDYDDAPI.H:

Activar un perfil de Treelock, o desactivar la verificación de accesos:

```
ULONG _System EDYPDDSetAccessToFiles(PSZ  FileName);
```

Si FileName es NULL el dipositivo de Treelock verificará los accesos utilizando el perfil %SGM_SHELL%\NOUSER\EDYDD32.INI; si este archivo no existe, no se verificará ningún acceso. Si FileName no es NULL, se activa el perfil especificado por FileName; si no existe se retorna un error.

Activar/Desactivar un archivo de Auditoría:

```
ULONG _System EDYPDDSetAuditFile(PSZ  FileName);
```

Si FileName es NULL se activa la auditoría sobre el archivo %SGM_SHELL%\NOUSER\EDYDD32.AUD; si este archivo no existe, la auditoría se desactiva. Si FileName no es NULL, se activa la auditoría sobre el archivo especificado ; si no existe se devuelve un error.

Cerrar los archivos de registro y de auditoría:

```
ULONG _System EDYPDDCloseLogDebugFile(VOID);
```

Si la llamada se ejecuta con éxito se devuelve un 0. Si hay algún problema se devuelve un código de error. Sólo se soportan llamadas de 32 bits.

El programa EDYDDUTL.EXE utiliza la API de Treelock:

```
EDYDDUTL { {/F|/A}[drive:][pathname][filename][.ext]  | /C }
```

Donde:

/Ffilename activa el perfil *filename*.

/F desactiva el perfil actual.

/Afilename activa la auditoría sobre *filename*.

/A desactiva la auditoría.

/C cierra los archivos de registro y de auditoría.

Restricciones Implícitas

Para poder proporcionar un entorno suficientemente seguro, el componente de Treelock incorpora un conjunto de restricciones de seguridad implícitas que garantizan que un usuario no administrador no pueda jugar con las interfícies y herramientas de SecureEntry, y así no pueda poner en entredicho la seguridad y la integridad de todas las funcionalidades que este producto proporciona.

Estas restricciones son:

- Los administradores no tienen ninguna restricción.
- Los usuarios no administradores tienen las siguientes restricciones:
  - Derechos nulos sobre los recursos ubicados dentro de la ruta apuntada por la variable de entorno RUNWORKPLACE excepto SES\PSSDMON.EXE, e.g. los accesos a C:\OS2\SECURITY serán denegados.
  - Derechos nulos sobre los recursos:
    - OS2\BOOT\SESDD32.SYS
    - OS2\BOOT\EDYDD32.SYS
    - OS2\BOOT\EDYFLPY.FLT
  - Derechos de sólo lectura y de abertura de DLLs sobre el subdirectorio DLL del directorio apuntado por la variable de entorno SGM_SHELL.
  - Derechos plenos sobre todos los recursos dentro de los subdirectorios WORK y TEMP contenidos en el directorio apuntado por la variable de entorno SGM_SHELL.
  - Derechos de lectura y ejecución sobre todos los recursos dentro del subdirectorio TOOLS contenido en el directorio apuntado por la variable de entorno SGM_SHELL.
  - Derechos de ejecución sobre los módulos de traceado y sobre el archivo EDYUTIL.EXE contenido en el subdirectorio EXEC del directorio apuntado por la variable de entorno SGM_SHELL.
  - Derechos de sólo lectura sobre:
    - EDYSTART.CMD
    - CONFIG.SYS
    - STARTUP.CMD
    - todos los recursos contenidos en el directorio apuntado por la variable de entorno SGM_SHELL exceptuando aquellos que estén sujetos a derechos menos restrictivos.

Observe que puede eliminar estas restricciones usando un perfil de Treelock que incluya explícitamente sus preferencias, aunque no se recomienda. Por ejemplo, suponiendo que quisiera que los usuarios no administradores pudieran modificar el archivo config.sys, podría incluir la siguiente línea en el perfil de Treelock:

```
set mode=c
Y EXES A F C:\CONFIG.SYS
```

que permitiría a todos los procesos no especificados hacer cualquier cosa con el config.sys, además de poder arrancar líneas de comandos.

Proceso de arranque

El proceso de arranque OS/2 estándar no es seguro por que puede ser interrumpido, dejando la estación en un estado inestable, sin garantías de que se haya instalado completamente el software de blindaje. El objetivo del proceso de arranque protegido suministrado con SecureEntry es garantizar la completa inicialización de la máquina de un modo que, sin permitir interrupciones, sea a su vez informativo y capaz de garantizar la integridad de la misma. Para ello, el archivo de arranque estándar OS/2 *STARTUP.CMD* se reemplaza por el archivo de arranque protegido *EDYSTART.CMD* en el directorio raíz de la partición de arranque, y la carpeta de autoarranque del OS/2 se sustituye a su vez por la pseudo carpeta (lista de sombras) *EdyStart*, con el mismo propósito y localizada en la vía de acceso SecureEntry, directorio *NOUSER*.

El proceso de arranque protegido provee además de ciertos comandos, con los cuales se puede informar al usuario del progreso del mismo en una ventana modal de sistema mientras se procesa *EDYSTART.CMD*.Basta con codificar las llamadas pertinentes a dichos comandos en el mismo archivo *EDYSTART.CMD*. Todos los mensajes mostrados serán además añadidos al archivo *EDYLKINI.LOG*, para su posterior análisis por si el arranque fuera desatendido y hubiese algún problema. Dicho archivo de log se puede encontrar también en el directorio raíz de la partición de arranque de la estación.

EDYLKINI.EXE

EDYLKSLD.EXE

EDYLKMSG.EXE

EDYLKBLK.EXE

EDYLKSWT.EXE

EDYWFWPS.EXE

Ejemplo de proceso de arranque

EDYLKINI.EXE

Descripción

Este comando puede usarse para comprobar el funcionamiento del proceso de arranque manualmente, sin necesidad de rearrancar la máquina.

Sintaxis

```
EDYLKINI [/NOMODAL]
```

donde /NOMODAL hace que la ventana informativa del arranque protegido no sea modal de sistema, permitiendo al usuario interactuar con el mismo.

Códigos de retorno

Ninguno.

EDYLKSLD.EXE

Descripción

Ejecutable utilizado para mover la barra de progreso del diálogo de arranque protegido.

Sintaxis

```
EDYLKSLD [número]
```

donde *número* indica la posición deseada de la barra. Por defecto, ésta se mueve a la siguiente posición.

Códigos de retorno

Ninguno.

EDYLKMSG.EXE

Descripción

Ejecutable utilizado para mostrar un mensaje informativo en la ventana de arranque protegido.

Sintaxis

```
EDYLKMSG mensaje
```

donde *mensaje* es el mensaje a mostrar.

Códigos de retorno

Ninguno.

EDYLKBLK.EXE

Descripción

Este comando puede usarse para bloquear la estación cuando ocurra algún error controlado en el proceso de arranque.

Sintaxis

```
EDYLKBLK mensaje
```

donde *mensaje* es el mensaje a mostrar en la ventana de arranque protegido informando de la circunstancia causante del bloqueo.

Códigos de retorno

Ninguno.

EDYLKSWT.EXE

Descripción

Este comando se mantiene por compatibilidad con versiones antiguas de SecureEntry, y permite especificar un nombre de proceso que se lanzará una vez se haya procesado completamente *EDYSTART.CMD*

Sintaxis

```
EDYLKSWT parámetros

parámetros:

-D:directorio de trabajo
-P:nombre programa
-A:argumentos
-T:título de sesión
-U:x retardo de arranque en segundos (por defecto 0 segundos)
-F:x foco
                        0=primer plano (defecto)
                        1=segundo plano
-S:x tipo de sesión
                        1=línea de comandos OS/2
                        2=línea de comandos OS/2 en ventana
                        3=Aplicación Presentation Manager (PM)
                        4=Aplicación DOS VDM (DOS o WINOS2)
                        7=Aplicación DOS VDM en ventana
-X:x posición X de la ventana
-Y:x posición Y de la ventana
-W:x anchura de la ventana
-H:x altura de la ventana
```

Códigos de retorno

Ninguno.

EDYWFWPS.EXE

Este comando permite esperar, durante el proceso de arranque, por la inicilización del WorkPlace Shell (escritorio). Está diseñado para ser usado **exclusivamente** durante el proceso de EDYSTART.CMD. Una vez invocado, no devolverá control hasta que el Shell se haya cargado y el escritorio esté inicializado. No dispone de parámetros adicionales, de modo que la sintaxis de llamada es :

```
EDYWFWPS
```

Utilice este comando solamente si la variable de entorno SES **RESTARTUSERSHELL** tiene el valor *NO* (valor por defecto). En caso contrario, y puesto que el arranque del escritorio se retrasaría a tiempo de conexión, su procedimiento de arranque no terminaría nunca.

Este ejecutable reside en la vía de instalación SecureEntry, directorio EXEC.

Ejemplo de proceso de arranque

Éste es un ejemplo de archivo de arranque *EDYSTART.CMD*

```
rem mover la barra a la primera posición
edylksld
rem mostrar mensaje
edylkmsg "Arrancando los servicios del servidor"
rem mover la barra a la tercera posición
edylksld 3
rem arrancando la red
net start requester
rem mover la barra a la cuarta posición
edylksld
rem mostrar mensaje
edylkmsg "Arrancando comunicaciones"
rem arrancar CM
cmstart
rem mover la barra a la sexta posición
edylksld 6
rem mostrar mensaje
edylkmsg "Arrancando procesos de segundo plano"
start myserver.exe
rem mover la barra a la octava posición
edylksld 8
edylkmsg "Arrancando daemon"
rem  La siguiente instrucción arrancará un proceso secundario cuando acabe
rem  el proceso de éste archivo, dejando visible ventana de arranque 10 segs.
edylkswt -P:C:\MYAPPS\MYDAEMON.EXE  -S:3 -D:C:\MYAPPS  -U:10
rem mover la barra a la novena posición
edylksld 9
rem asignar recursos
net use J:  MyAlias
rem mover la barra a la última posición
edylksld
rem  finalizar
@exit
```

Protección de arranque

Las herramientas de protección de arranque SecureEntry permiten proteger al sistema frente a intentos de arranque con otro sistema operativo desde disquete. Hay básicamente tres maneras de conseguir este objetivo :

1. Utilizando directamente los menús de configuración de la máquina (BIOS), para definir una secuencia de arranque que no pase por la disquetera, y definir una clave de administrador de tal modo que solo este último puede cambiar la secuencia de arranque. Esta opción no requiere ayuda por parte de SecureEntry, pero desafortunadamente no todas las máquinas permiten este tipo de configuración, además de que el manejo de las claves de administrador puede hacerse muy engorroso para una gran corporación.
2. Cambiando la secuencia de arranque vía BIOS, en máquinas que dispongan de una copia de los programas de sistema en el disco duro, de modo que, modificando estos debidamente, solamente los usuarios administradores puedan llegar a los menús de configuración BIOS de la máquina. Esta opción es llamada también *Control de arranque BIOS* y solo es válida en ciertos modelos de PS/2 (los más modernos).
3. Protegiendo el sector de arranque del disco duro de tal modo que, aunque no se evite el arranque con otro sistema operativo, este no sea capaz de ver el disco, con lo que la máquina mantendrá su integridad. Este es el método menos seguro, pero tiene la ventaja de que puede aplicarse a prácticamente cualquier máquina. Se denomina *Control de arranque vía software*

Vd. debe decidir cual de los tres métodos usar, sopesando las ventajas e inconvenientes de cada uno.

Control de arranque BIOS

Control de arranque vía software

Por último, y a pesar de no estar directamente relacionado con el control de arranque, cabe observar que SecureEntry provee de la utilidad de Salvaguarda del sector de arranque, por si vd. desea obtener protección adicional frente a programas que, de forma intencionada o no, sobreescriban dicho sector, crítico para el arranque.

Control de arranque BIOS

Descripción

La función SecureEntry de control de arranque BIOS impide que los usuarios puedan arrancar el sistema a través de la disquetera y/o accedan a los menús de configuración del mismo. Esta función es aplicable **solamente** a aquellos modelos de PS/2 que disponen de los programas de sistema en una partición independiente del disco.

Esta función se consigue cambiando la secuencia de arranque vía los menús de configuración y controlando el acceso a los menús de configuración, siguiendo los pasos que se detallan :

Obtener los *disquetes de instalación* a ser usados en las máquinas de producción para instalar el control de arranque.

Preparar las máquinas de producción, cambiando la secuencia de arranque e instalando la función de control de arranque.

Generar los *disquetes clave* para ser usados por los administradores de sistema. Cuando se entre la clave correcta, entonces el usuario podrá acceder a los menús de configuración del sistema.

Obteniendo los *disquetes de instalación*

Los disquetes de instalación de la función de *control de arranque BIOS* se obtienen a partir del *disquete de referencia* de la máquina deseada. Utilice los menús de configuración de la máquina (opción *Salvar la partición de sistema*) para obtener una copia del disquete de referencia deseado.

Para generar el disquete de instalación, haga lo siguiente :

Desde la vía de acceso SecureEntry, directorio *TOOLS*, ejecute EDYSREFD. Esta utilidad le pedirá que inserte el disquete de referencia previamente creado en la disquetera.

Una vez el proceso completo, el contenido del disquete habrá sido modificado y será ahora un disquete de instalación para la función de *control de arranque BIOS*.

Preparando las máquinas de producción

Para modificar la secuencia de arranque y prevenir el arranque desde disquete, siga el siguiente proceso en las máquinas de producción :

Acceda a los menús de configuración del sistema.

Escoja las siguientes opciones :

Establecer características

Establecer secuencia de arranque.

Seleccione el disco duro como primer dispositivo de arranque, y la disquetera como dispositivo secundario.

Grabe la secuencia de arranque modificada.

Para instalar la función de control de arranque, inserte el disquete de instalación previamente creado en la disquetera, y reinicialice el sistema.

Una vez el proceso completo, la protección de arranque BIOS estará operativa. A partir de este momento, para acceder a los menús de configuración BIOS será necesario un disquete *clave*, que debería ser propiedad del usuario administrador.

Generando los disquetes clave

Para generar los disquetes clave, siga el proceso :

Inserte un disquete vacío y formateado en la disquetera.

Desde la vía de acceso SecureEntry, directorio *TOOLS*, ejecute EDYSETPW.

Entre una clave de hasta 8 carácteres de longitud.

Entre la misma clave para verificación.

Una vez completo, el disquete contendrá la clave encriptada, y será necesario para acceder al menú de configuración de las máquinas donde esté instalada la función de protección de arranque BIOS.

Accediendo a los menús de configuración

Para arrancar las utilidades de configuración del sistema, siga el proceso :

Inserte el disquete *clave* en la disquetera.

Arranque el sistema.

Acceda a los menús de configuración. (pulse Ctrl-Alt-Ins cuando el cursor esté en el borde superior derecho de la pantalla).

Entre la clave correspondiente al disquete insertado, cuando se le pregunte. El máximo número de reintentos es de 3.

Si la clave es correcta, dispondrá vd. de las siguientes opciones :

1. Acceder a los menús de configuración
2. Cambiar la clave del disquete clave
3. Operación restringida

   Esta opción le permite desactivar el proceso de protección BIOS.

Control de arranque vía software

Descripción y procedimientos

La función de control de arranque vía software SecureEntry impide que se pueda acceder a las particiones del disco duro cuando se haya arrancado el sistema a través de otra partición/disquete de arranque no controlados por SecureEntry.

Existen dos iconos para instalar y desinstalar esta función que están disponibles en la carpeta de *herramientas de instalación* SecureEntry. A continuación se describe el proceso para hacerlo manualmente :

Para **habilitar la protección de arranque**, vd. puede también ejecutar el siguiente comando desde una ventana de línea de comandos OS/2 :

```
EDYNOTA.EXE /Pclave
```

Donde *clave* se la clave para desinstalar posteriormente la protección de arranque.

Añada a continuación la siguiente línea en el archivo *CONFIG.SYS*:

```
CALL=x:\SGMSHELL\EXEC\EDYNOTA.EXE  /R
```

Donde *x* es el identificador de la partición donde SecureEntry esté instalado.

A partir de este momento, se impedirá el acceso al disco cuando el sistema se arranque desde disquete.

Para **desactivar la protección de arranque**, deberá vd. borrar o comentar la línea anterior del archivo *CONFIG.SYS*, y ejecutar el siguiente comando desde una sesión OS/2 :

```
EDYYESA.EXE /Pclave
```

Donde *clave* es la clave entrada durante la instalación de la protección de arranque.

Si vd. ejecuta *EDYYESA* o *EDYNOTA* en un sistema con la protección de arranque instalada, suministrando una clave diferente de la usada para la instalación, no se grabará ningún cambio en el disco duro.

Observe que, con la protección de arranque instalada, cualquier programa que acceda al sector de arranque del disco (incluyendo FDISK) presentará datos falsos sobre el mismo. Si vd. desea definir o borrar particiones, etc.. deberá primero desinstalar la protección de arranque.

Mensajes

EDYNOTA.EXE (run-time)

Operación satisfactoria :

```
Ok
```

Mensajes de aviso :

```
Boot protection already installed on disk X - Password ignored
Protección de arranque ya instalada para el disco X -  Clave ignorada

Password ignored
Clave ignorada

Boot protection not installed on disk X
La protección de arranque no está instalada para el disco X

Boot protection already installed on disk X
La protección de arranque ya está instalada para el disco X
```

Error:

```
Error produced on WEEKDAY, DATE AND TIME
----------------------------------------
 Source Module Name: SOURCE MODULE NAME
 Compilation Date  : COMPILATION DATE
 Compilation Time  : COMPILATION TIME
 Source Line Number: SOURCE LINE NUMBER
 Logged Error      :  (hex)=RC (dec)=RC
```

Esta información será copiada también en el archivo *EDYLOGA.ERR*.Contacte con el servicio de soporte SecureEntry.

EDYYESA.EXE (run-time)

Operación satisfactoria :

```
Ok
```

Mensajes de aviso :

```
Boot protection not installed on disk X
La protección de arranque no está instalada para el disco X

Invalid password
Clave inválida
```

Error: igual que para EDYNOTA.EXE.

EDYBOOT.SYS (en tiempo de arranque)

Errores:

```
Cannot read partition
No se pudo leer la partición

Invalid partition
Partición inválida
```

Compatibilidad con la utilidad de volcado estándar OS/2

Si vd. utiliza la sentencia **TRAPDUMP** estándar de OS/2 para grabar volcados de memoria en el disco duro (partición SADUMP) en caso de errores del sistema, entonces y si la protección de arranque SecureEntry está instalada, dicha utilidad no reconocerá el disco duro, con lo que no será capaz de producir el archivo de volcado requerido. Para evitar esta situación, puede vd :

Desinstalar la protección de arranque SecureEntry antes de reproducir la situación que produce el error e inicia el volcado, o

Utilizar el comando SecureEntry suministrado *EDYPDUMP.CMD* con objeto de modificar la utilidad de volcado OS/2 de modo que reconozca las particiones del disco protegidas por SecureEntry. Dicha utilidad se encuentra en la vía de acceso SecureEntry, subdirectorio *EXEC*. Para ejecutar esta utilidad, teclee :

```
EDYPDUMP SET
```

si desea modificar el código de volcado para reconocer particiones SecureEntry, o

```
EDYPDUMP RESET
```

para eliminar dicha modificación. En caso de que desee implementar esta solución en máquinas de producción, deberá vd. primero probarla concienzudamente en su hardware, ya que existe la posibilidad de que ni siquiera así funcionen los volcados de memoria, para ciertos tipos de controladoras de disco SCSI.

Códigos de retorno

La operación de un comando correcta devuelve 0. En caso de error, se devuelve 1.

En tiempo de arranque, si se encuentra algún error, el programa entrará en un ciclo de ejecución sin fin, después de mostrar el mensaje de error.

Chequeo de la integridad de archivos

La función de chequeo de integridad de archivos SecureEntry consta de una serie de comandos con los cuales se puede verificar la integridad de los programas y datos estáticos deseados, en tiempo de arranque o antes de su utilización. La idea es calcular previamente un número de verificación para cada archivo deseado, que dependa del contenido del mismo, de tal modo que se pueda comprobar que un archivo no haya sido modificado recalculando dicho número y comparándolo con el número de verificación (checksum) original. Las utilidades suministradas por SecureEntry permiten utilizar dos algoritmos de suma diferentes :

XOR binario en bloques de 64 bits. Es el método más rápido.

Algoritmo MD4 de proceso de mensajes. Es el método más seguro.

Módulos

Para calcular el número de verificación de un archivo:

```
SAF2INGN.EXE <Método> <Archivo>

donde: <Método> es 1 para XOR 64 bits, o 3 para MD4
       <Archivo> es el nombre de archivo a procesar
```

Mensajes:

Correcto :

```
Calculated checksum: xxxxxxxx
Número de verificación xxxxxxxx
```

Error:

```
Usage: SAF2INGN Method Filename
Utilización: SAF2INGN Método Archivo

Invalid method
Método inválido

Open file error
Error abriendo el archivo

Invalid Checksum
Número de verificación inválido
```

Códigos de retorno: 0 para ejecución correcta. Código de retorno de error OS/2 en otro caso.

Para verificar una serie de archivos:

```
SAF2INCK.EXE <ArchivoEntrada> <CheckID> <ArchivoSalida> [<Programa>]
```

Donde:

<ArchivoEntrada> Es el nombre del archivo que contiene la lista de archivos y números de verificación.

<CheckID> Es el identificador de grupo de archivos a verificar. Solamente se procesarán los archivos de la lista con el mismo identificador

<ArchivoSalida> Es el nombre de archivo a escribir con el resultado. Por defecto se usará la consola en caso de que no se pueda abrir.

<Programa> Es un nombre de programa a ejecutar en caso de verificación correcta.

El <*ArchivoEntrada*> debe seguir el siguiente formato :

```
 <CheckID> <Método> <NúmeroVerif> <Archivo>
     |        |         |             |
     |        |         |            +->  Archivo a verificar
     |        |         +--------------->  Número de verificación hexadecimal
     |        +-------------------------> 00001:  XOR 64 bits
     |                                    00003:  MD4
     +---------------------------------->  Identificador de grupo de archivos
```

En el ejemplo que sigue, los archivos C:CONFIG.SYS y C:AUTOEXEC.BAT serán verificados contra un número de verificación 77 y 40 respectivamente, mediante el algoritmo de XOR binario de 64 bits si SAF2INCK.EXE es llamado con CheckID 10000; y los archivos C:OS2\SYSTEM\CONFIG.DOS y C:OS2\SYSTEM\AUTOEXEC.DOS serán verificados contra los números 7F89AA02751EA8908348C4C38D9D390A y 680A5CA3E0F9B8A5372B39EB856CE268 respectivamente, usando MD4 si SAF2INCK.EXE es lanzado con CheckID 1000A.

```
10000 00001 77                                C:CONFIG.SYS
10000 00001 40                                C:AUTOEXEC.BAT
1000A 00003 7F89AA02751EA8908348C4C38D9D390A  C:OS2\SYSTEM\CONFIG.DOS
1000A 00003 680A5CA3E0F9B8A5372B39EB856CE268  C:OS2\SYSTEM\AUTOEXEC.DOS
* Vd. puede añadir comentarios si el primer carácter de la línea es '*'
```

Mensajes:

Correcto :

Check OK !!!!

Verificación correcta !!!!

Error:

Wrong usage
Error de sintaxis de llamada

Unable to open configuration file
Imposible abrir archivo de entrada

Error(s) found during check
Errores encontrados durante la verificación

Invalid method
Método inválido

Open file error

```
Error de apertura de archivo

Invalid Checksum
Número de verificación inválido

Unknown checkid
Identificador de grupo desconocido

System stopped
Sistema detenido
```

Códigos de retorno: 0 para ejecución correcta. Código de retorno de error OS/2 en otro caso.

Para calcular una serie de números de verificación:

```
SAF2GEN.CMD <CheckID> <FileSpec[+Filespec..]> <Método> [/S] [/H] [/R] [/T]
Donde:
<CheckID> es el identificador de grupo de archivos a generar.
<Método>  es 1 para XOR-64, 3 para MD4
<FileSpec> son los nombres de archivos para los cuales se debe calcular el número
de identificación. Los carácteres de sustitución están permitidos.
/S  opcionalmente, buscar archivos recursivamente en los subdirectorios
encontrados.
/H         incluir archivos ocultos
/R         incluir archivos de sólo lectura
/T         incluir archivos de sistema
```

Este programa produce su salida en el mismo formato que es preciso para poder ejecutar SAF2INCK, de modo que es posible redireccionarla a un archivo y utilizar este directamente para la verificación (parámetro <*ArchivoEntrada*>). Cualquier error encontrado será indicado como comentario (primer carácter '*'); por ejemplo, cuando el número de verificación de un archivo no pueda calcularse por estar siendo usado por otro proceso.

Códigos de retorno:

0 Ejecución correcta.

1 Falló el cálculo del número de verificación para algún archivo.

2 No se pudo ejecutar el programa por algún error grave.

En el ejemplo que sigue, se calculará el número de verificación de todos los archivos de C:\OS2\DLL y C:\CMLIB\DLL, y al resultado se añadirán los números de verificación para todo el subárbol C:\MYDIR con CheckID 00001 usando el método MD4. El archivo para la posterior llamada a SAF2INCK será PARMFILE.DAT.

```
SAF2GEN 1 C:\MYDIR\* 3 /S >PARMFILE.DAT
SAF2GEN 1 C:\OS2\DLL\*+C:\CMLIB\DLL\*  3 /S >>PARMFILE.DAT

Observe que el CheckID se rellenará con 0's en la salida.
```

Componente de procesos auditables

El Componente Auditor de Procesos SecureEntry le permite obtener respuestas a preguntas tales como:

¿Hay procesos acaparando el procesador? ¿Cuáles?

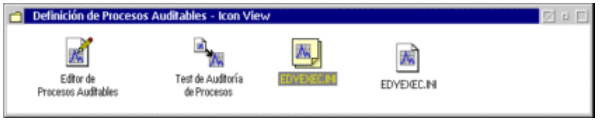
¿Usan los usuarios realmente las herramientas que la Corporación para la que trabajo pone a su disposición? ¿Cuáles de ellas tienen mayor aceptación?

¿Hay realmente usuarios a los que el procesador se les queda "corto"?

¿Hay usuarios que pierden parte de su tiempo en tareas repetitivas?

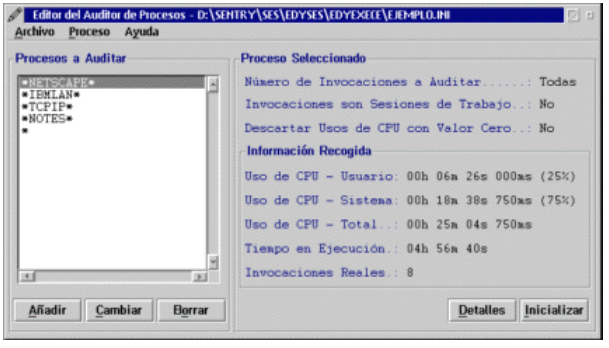
¿Se estan utilizando programas explícitamente prohibidos por la Corporación?

Para trabajar con este componente, abra la carpeta de *Definición de Procesos Auditables*, que se encuentra a su vez en la carpeta *Herramientas de Administración SecureEntry*.



Para crear un perfil de personalización para este componente, utilice el objeto modelo suministrado (*EDYEXEC.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor de Procesos Auditables*, o bien haga doble click sobre el mismo. Efectúe las modificaciones pertinentes y después salve el perfil modificado. Para cualquier duda, consulte la ayuda interactiva del editor.



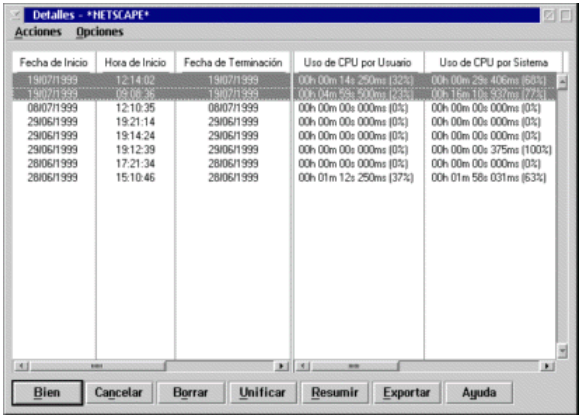
Para verificar el comportamiento del perfil, arrástrelo y suéltelo sobre el objeto *Test de Auditoría de Procesos*, o bien active la función de prueba vía la barra de menú del editor. El perfil definido se activará.

Una vez configurado, asocie el perfil al usuario o grupo deseado, arrastrándolo y soltándolo sobre el contenedor adecuado de la herramienta de administración de usuarios y/o grupos, o bien establezca el mismo como defecto de máquina, copiándolo con su nombre por defecto (EDYEXEC.INI) en la carpeta *NOUSER*.

Cuando un usuario realize una conexión, se activará el perfil que tenga asociado, ya sea el suyo propio o el del grupo SecureEntry al que pertenezca en caso de no tenerlo. Si el usuario no tiene ningún perfil de procesos auditables asociado, entonces se activará el perfil que pudiera haber en la carpeta *NOUSER*. Si en la

carpeta *NOUSER* tampoco existe un perfil de procesos auditables para la máquina, entonces no se auditará ningún proceso.

Dado que este es uno de los Componentes SecureEntry que realimenta el perfil con información de salida, dicho perfil no sólo se baja en tiempo de conexión, sino que además también se sube en tiempo de desconexión. Puede usted usar el mismo Editor para visualizar la información recogida por SecureEntry.



El Editor también proporciona extensiones adicionales para la exportación a o importación desde un archivo externo sobre la información recogida en detalle.

Remítase a Códigos y Mensajes de Error para la descripción de los códigos de error que el Editor de Procesos Auditables puede devolver.

La información recogida

Descripción de los módulos y API

Herramienta de Volcado de Procesos Auditables: EDYEXEDM

La información recogida

La **Información Recogida** por el componente Auditor de Procesos de SecureEntry se compone de:

Uso de CPU por Usuario Por definición, este es el tiempo acumulado cuando un proceso se ejecuta en Ring 2 o Ring 3. En la práctica, se puede ver como la cantidad de tiempo que un proceso ha estado ejecutándose, probablemente como consecuencia de una *acción de usuario*, utilizando recursos **propios** de la aplicación.

Uso de CPU por Sistema Por definición, este es el tiempo acumulado cuando un proceso se ejecuta en Ring 0. En la práctica, se puede ver como la cantidad de tiempo que un proceso ha estado ejecutándose utilizando recursos y código del **sistema**, i.e., a nivel de controlador de dispositivo y Kernel.

Uso de CPU Total Es la suma de los tiempos de uso de Usuario y de Sistema, y mide la cantidad de "tiempo de tarea" (task time) durante el que un proceso concreto ha estado ejecutándose.

Tiempo en Ejecución Mide la cantidad de tiempo transcurrido desde que el proceso empezó a ejecutarse hasta que completó su ejecución.

Invocaciones Reales El número de veces que una instancia distinta del proceso seleccionado se ha encontrado en ejecución.

Como regla general, y debido a que el uso de CPU total refleja la cantidad de tiempo que un proceso ha estado ejecutándose en "tiempo de tarea" (task time), la diferencia entre el tiempo en ejecución y esta cantidad proporciona el tiempo durante el cual el proceso ha estado interrumpido y deshabilitado.

La granularidad del reloj del sistema, que es de 31.25ms por "tick de reloj" (timer tick), hace que los tiempos de uso de CPU por Usuario y por Sistema sirvan de bien poco a no ser que sean mediciones extensas, por lo que debe usted tener en cuenta que puede hacer una interpretación de resultados errónea si inspecciona la información recogida en un perfil que haya estado activo durante un período de tiempo relativamente corto.

Descripción de los módulos y API

A continuación se describen los módulos que se integran en este componente:

EDYEXECE

Este es el programa editor de perfiles. Tiene la siguiente sintaxis:

```
EDYEXECE.EXE [Perfil]
```

Donde *Perfil* es la vía de acceso y nombre de archivo del perfil deseado. El editor permite probar un perfil directamente.

EDYEXECT

Este es el programa activador de perfiles. Tiene la siguiente sintaxis:

```
EDYEXECT.EXE /F[Perfil]
```

/F*Perfil* activa el perfil descrito en *Perfil*. Si *Perfil* no existe, no se activará ningún perfil.

/F activa el perfil EDYEXEC.INI descrito en *NOUSER*. Si dicho perfil no existe, no se activará ningún perfil

Interfície del componente de procesos auditables

El componente exporta la siguiente rutina, tal como se define en *EDYEXECD.H*. La rutina se ejecuta correctamente si devuelve cero; en caso contrario devuelve el error obtenido:

```
APIRET _System ActivateExecsAuditor(PSZ  pszFileName);
```

Activa el perfil descrito en pszFileName. Si el contenido de pszFileName está vacío, entonces no se audita ningún proceso.

Si pszFileName apunta a "", entonces se activará el perfil de NOUSER.

Si el arhivo no existe, entonces se develve un error y no se auditará ningún proceso.

Herramienta de Volcado de Procesos Auditables: EDYEXEDM

La herramienta *EDYEXEDM* permite extraer y/o reinicializar la información recogida por el componente auditor de procesos. La información extraida se almacenará en un fichero de texto con el mismo formato que el utilizado por el *Editor de Procesos Auditables* para importar y exportar la información recogida en detalle.

La sintaxis del comando es como sigue:

```
EDYEXEDM ? | /Help | [/Outfile:f] [/Users:{mask[+mask...]|@file.lst}]
         [/Groups:{mask[+mask...]|@file.lst}]
         [/Process:{process[+process...]|@file.lst}]
         [/Cpu:{U|S}ratio] [/Reset | /ONLYReset]
         [/Info:{[U|G] [M|S] [D|D[..]date{[..]|[..date...]}|D@file.lst]
                 [OCU|OCS|OCT]}]


    /Help y ?    : Ayuda.
    /Outfile     : Vía de acceso y nombre del fichero de salida.
                   Por defecto, EDYEXEDM.TXT.
    /Users       : Sólo extraer la información de los procesos pertenecientes
                   a los usuarios que coinciden con las máscaras especificadas.
    /Groups      : Sólo extraer la información de los procesos pertenecientes
                   a los usuarios de los grupos que coinciden con las
                   máscaras especificadas.
    /Process     : Sólo extraer la información de los procesos que se especifican.
    /Cpu         : Sólo almacenar la información extraida de los procesos
                   con:
                   U   un porcentaje de uso de Cpu por usuario mayor o igual
                       que el porcentaje especificado (0-100).
                   S   un procentaje de uso de Cpu por sistema mayor o igual
                       que el procentaje especificado (0-100).
    /Reset       : Además reinicializar en el perfil la información
                   extraida de los procesos.
    /ONLYReset   : Reinicilizar y no extraer la información de los
                   procesos.
    /Info        : Determina como se almacena en el fichero de salida la
                   información extraida. Al menos uno de los siguientes valores
                   debe ser especificado:
                   U   juntar la información de los procesos de todos los usuarios.
                   G   juntar la información de los procesos de todos los usuarios
                       pertenecientes al mismo grupo.
                   M   fundir todas las invocaciones pertenecientes al mismo proceso.
                   S   resumir todas las invocaciones pertenecientes al mismo proceso.
                   D   fundir todas las invocaciones pertenecientes al mismo proceso
                       que comienzan el mismo dia.
                   D[..]date{[..]|[..date...]}  y D@file.list
                        fundir las invocaciones pertenecientes al mismo proceso
                        que comienzan en el mismo intervalo de tiempo.
                        Las fechas límite de intervalo tienen el formato "dd-mm-yyyy".
                   OCU  ordenar las invocaciones por uso de cpu por usuario.
                   OCS  ordenar las invocaciones por uso de cpu por sistema.
                   OCT  ordenar las invocaciones por uso de cpu total.
                      (por defecto las invocaciones se ordenan por fecha de inicio)
```

Así por ejemplo: `EDYEXEDM /U:EDYADMIN+U* /G:@GROUP.LST /C:U30 /INFO:G S OCT`

Extrae la información de proceso para el usuario *EDYADMIN*, los usuarios que coinciden con *U** y los usuarios de los grupos que coinciden con las mascaras especificadas en el fichero *GROUP.LST*. Además, sólo los procesos con un procentaje de uso de cpu por usurio mayor o igual que *30* serán considerados. La información extraida se almacenará por grupos, resumiendo las invocaciones y ordenandolas por uso de cpu total.

```
EDYEXEDM /U:* /R /INFO:D..12-09-1999..12-10-1999..
```

Extrae y reinicializa la información de proceso para todos los usuarios. La información se almacena fundiendo todas las invocaciones que comienzan antes del *12-09-1999* ; entre el *12-09-1999* (éste inclusive) y el 12-10-1999 ; y después del *12-10-1999* (éste inclusive).

```
EDYEXEDM /U:@USER.LST /P:* /ONLYR
```

Reiniciliza la información del proceso * para los usuarios que coinciden con las máscaras especificadas en el fichero *USER.LST*.

Observe que los valores *M* y *S* del parámetro */INFO* realizan exactamente la misma operación que los comandos *Unificar* y *Resumir* del *Editor de Procesos Auditables*.

Componentes de seguridad - WPS

Restricciones del escritorio

El componente de restricciones del escritorio permite establecer restricciones a los estilos y características de los objetos del escritorio. Así por ejemplo, puede vd. hacer que ciertos objetos sean invisibles, o impedir las operaciones de arrastre con los mismos. También puede vd. eliminar por completo o parcialmente el menú emergente de los objetos deseados.

Para trabajar con este componente, abra la carpeta de *definición de restricciones del escritorio*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Los perfiles de este componente pueden definirse de dos modos : Perfiles de tipo binario y perfiles de tipo texto editable. Estos últimos requieren un paso adicional de conversión a binario para poder ser activados o asignados a usuarios y/o grupos de usuarios.

```
*************************************************************************
*  NOTA: El soporte de perfiles de tipo texto tan solo se mantiene     *
*        por razones históricas y de compatibilidad, dado que no       *
*        son estrictamente necesarios, resultando mucho mas sencillo   *
*        partir de un perfil de tipo binario para conseguir el mismo   *
*        resultado.                                                    *
*************************************************************************
```

Vd. puede crear un perfil texto para este componente mediante el modelo de perfiles de texto de la misma carpeta (*Perfil de texto*).

Vd. puede crear un perfil binario para este componente mediante el modelo de perfiles de la misma carpeta (*Perfil Binario*)., o a través del modelo residente en el directorio *TEMPLATE* de su vía de acceso SecureEntry (*EDYDESK.INI*).

Las herramientas suministradas por SecureEntry para la administración de perfiles de restricción de escritorio son :

Un **capturador** de escritorios, para capturar los valores existentes de los estilos de los objetos de su escritorio. Capture un escritorio arrastrando y soltando un perfil de tipo texto sobre el objeto *Captura de las restricciones del escritorio*

Dos **compiladores**, para traducir perfiles binario a texto y viceversa. Arrastre y suelte el perfil deseado sobre el objeto compilador adecuado (*Traducción de binario a texto* o *Traducción de texto a binario*) para efectuar la conversión.

El objeto **activador** de perfiles binarios, para verificar el comportamiento de las restricciones establecidas (Arrastre y suelte el perfil binario adecuado sobre el objeto *Test de restricciones del escritorio*).

El objeto **editor** de perfiles binarios. Arrastre y suelte un perfil binario sobre el objeto *Editor de restricciones del escritorio* para poner al escritorio en modo edición. Configure entonces las restricciones necesarias de los objetos existentes a través de la nueva entrada *Editar restricciones* del menú emergente de los mismos. La ventana principal del editor permite también establecer restricciones por defecto para los objetos del escritorio, fuera de él, e incluso de los trabajos de impresora.

La función de edición directa le permite editar las restricciones de un objeto sin necesidad previa de abrir el editor, simplemente arrastrando y soltando el objeto deseado sobre el perfil binario deseado.

Configurando perfiles de escritorio a partir de perfiles de texto

Para configurar un perfil de restricciones de escritorio, vd. puede empezar directamente por un perfil de tipo binario, o definir las mismas en modo texto y después traducirlas. En este último caso, siga los pasos que se detallan a continuación :

1. Edite el perfil de restricciones
2. Compile el perfil de restricciones

Edición del perfil de restricciones de tipo texto

Siga el siguiente procedimiento :

1. Cree una instancia del objeto *Perfil de texto* a partir de su modelo.

   Vd. puede también utilizar las restricciones activas en un momento dado como punto de partida, en cuyo caso deberá arrastrar y soltar el perfil de texto recién creado sobre el objeto *Captura de las*

restricciones del escritorio, o bien activando la opción de captura a través del menú emergente del perfil de tipo texto.

Por último, vd. puede traducir a texto un perfil binario ya existente, y configurar sus restricciones en modo texto. Arrastre y suelte el perfil binario sobre el objeto *Traductor de binario a texto* para conseguirlo. Este proceso creará un perfil de texto con el mismo nombre, y extensión *TXT*. Vd. deberá cerrar la sesión creada por el programa compilador.

2. Abra el perfil de restricciones de tipo texto haciendo doble-click sobre su icono, y edítelo. En caso de utilizar otro editor, asegúrese de usar uno que preserve los atributos extendidos OS/2 de los archivos.
3. Especifique en el archivo los objetos y propiedades que desee restringir o configurar.
4. Guarde el perfil de texto modificado.

Compilación del perfil de tipo texto

Para traducir un perfil de restricciones de tipo texto y obtener un perfil equivalente de tipo binario, arrastre y suelte el objeto sobre el *Traductor de texto a binario*.

Se creará un archivo con el mismo nombre, y extensión *INI*, de tipo binario. Si el archivo ya existiera, sería actualizado.

En caso de que vd. suelte dos perfiles, uno binario y otro de tipo texto sobre el traductor, el perfil binario será actualizado con la nueva información suministrada en el perfil de tipo texto, añadiendo nuevas restricciones y/o modificando las antiguas.

También existe la posibilidad de invocar al traductor de perfiles desde el menú emergente de los mismos, o vía línea de comandos. En cualquier caso, Vd. deberá cerrar la sesión creada por el programa compilador.

El perfil binario resultante contendrá las restricciones especificadas y estará listo para ser probado.

Probando perfiles de restricción del escritorio

Para probar el comportamiento del escritorio con un perfil determinado, siga el siguiente proceso :

1. Capture las restricciones actuales del escritorio para poder reactivarlo con posterioridad. Alternativamente, vd. podrá reconectar la sesión para reestablecer las restricciones del escritorio.

   Vd. puede arrastrar y soltar un perfil de texto vacío sobre el objeto de *Captura de restricciones del escritorio* y después compilar el mismo soltándolo sobre el *Traductor de texto a binario*

2. Active el perfil de escritorio a probar.

   Haga esto arrastrando el icono que representa su perfil de restricciones de tipo binario sobre el objeto *Test de restricciones del escritorio*, o bien seleccionando la opción adecuada del submenú *abrir* del menú emergente del mismo.

   Verifique entonces que la apariencia y comportamiento del escritorio son los deseados.

Para restaurar las restricciones originales del escritorio una vez finalizada la prueba, puede vd. activar el perfil previamente capturado y guardado, o desconectar la sesión y volver a conectarse.

Modificando perfiles de restricción del escritorio

Para modificar un perfil de restricción del escritorio en formato binario, haga lo siguiente :

1. Entre en modo edición para los objetos deseados :

   Arrastre y suelte los objetos sobre los que desea establecer restricciones sobre el perfil binario, o

Abra el editor de perfiles explícitamente arrastrando el perfil binario sobre el objeto *Editor de restricciones del escritorio*, y entonces :

Seleccione *Editar restricciones* vía el menú emergente de los objetos a restringir, o

Haga doble-click sobre el objeto a modificar en la ventana principal del editor.

Se abrirá entonces una libreta de valores para establecer las restricciones de cada uno de los objetos deseados. Los valores mostrados para cada estilo serán los previamente definidos en el perfil, o los actualmente activos en su defecto.

2. Use la libreta de valores para especificar :

   Un subconjunto de los parámetros de la cadena de inicialización (pestaña inicio).

   La cadena de inicialización del OS/2 se utiliza para especificar parámetros que definen el comportamiento del objeto. SecureEntry permite además modificar la característica de *link* y permitir o denegar la creación de sombras del objeto, opcionalmente a carpetas de usuario.

   Las opciones seleccionables desde el menú emergente del objeto (pestaña menú).

   Las páginas de valores que podrán ser modificadas de la libreta de valores del objeto (pestaña Valores).

   Recuerde que la mayoría de restricciones se especifican por medio de botones de tres estados :

   Botón ensombrecido : Dejar el valor original (tal y como se encontrase antes de activar el perfil).

   Botón marcado : Habilitar la opción (forzar el valor a 'permitir').

   Botón desmarcado : Inhabilitar la opción (forzar el valor a 'no permitir')

   Para más información sobre como navegar a través de las páginas de la libreta y especificar restricciones concretas, acceda a la ayuda interactiva accesible desde la misma, bien pulsando el botón de ayuda, o la tecla *F1*.

3. Cierre la libreta de edición de restricciones pulsando *Bien*, y en su caso, cierre también la ventana principal del editor.

Alternativamente, vd. siempre tiene la posibilidad de traducir el perfil binario a otro de tipo texto, y editar las restricciones en este último, que una vez traducido de nuevo a binario, contendrá las restricciones especificadas.

Formato de los perfiles de tipo texto

A continuación se muestra la gramática aceptada para perfiles de tipo texto.

Vd. puede replicar la definición de restricciones de objeto básicas tantas veces como objetos deban ser definidos.

Se han utilizado las siguientes convenciones:

MAYÚSCULAS representan valores que vd. puede especificar directamente, sin cambios.

minúsculas representan variables a sustituir por el valor adecuado.

```
[nombreobjeto]|[DEFAULT]

  ATRIBUTO_SUPRIMIR=SI|S|1|NO|N|0
  ATRIBUTO_COPIAR=SI|S|1|NO|N|0
```

```
ATRIBUTO_MOVER=SI|S|1|NO|N|0
ATRIBUTO_SOMBRA=SI|S|1|NO|N|0
ATRIBUTO_SOMBRA_RESTRINGIDA=SI|S|1|NO|N|0
ATRIBUTO_VISIBLE=SI|S|1|NO|N|0
ATRIBUTO_IMPRIMIR=SI|S|1|NO|N|0
ATRIBUTO_RENOMBRAR=SI|S|1|NO|N|0
ATRIBUTO_ARRASTRAR=SI|S|1|NO|N|0
ATRIBUTO_SOLTAR=SI|S|1|NO|N|0
ATRIBUTO_VALORES=SI|S|1|NO|N|0

EMERGENTE_ABRIR=SI|S|1|NO|N|0
EMERGENTE_VALORES=SI|S|1|NO|N|0
EMERGENTE_VISTA_ICONOS=SI|S|1|NO|N|0
EMERGENTE_VISTA_ARBOL=SI|S|1|NO|N|0
EMERGENTE_VISTA_DETALLES=SI|S|1|NO|N|0
EMERGENTE_PROGRAMA=SI|S|1|NO|N|0
EMERGENTE_PALETA=SI|S|1|NO|N|0
EMERGENTE_AYUDA=SI|S|1|NO|N|0
EMERGENTE_CREAR_OTRO=SI|S|1|NO|N|0
EMERGENTE_COPIAR=SI|S|1|NO|N|0
EMERGENTE_MOVER=SI|S|1|NO|N|0
EMERGENTE_CREAR_SOMBRA=SI|S|1|NO|N|0
EMERGENTE_CREAR_PARTICION=SI|S|1|NO|N|0
EMERGENTE_SUPRIMIR=SI|S|1|NO|N|0
EMERGENTE_BUSCAR=SI|S|1|NO|N|0
EMERGENTE_IMPRIMIR=SI|S|1|NO|N|0
EMERGENTE_SELECCIONAR=SI|S|1|NO|N|0
EMERGENTE_BLOQUEAR_AHORA=SI|S|1|NO|N|0
EMERGENTE_CONCLUIR=SI|S|1|NO|N|0
EMERGENTE_CONFIGURACION_SISTEMA=SI|S|1|NO|N|0
EMERGENTE_CLASIFICAR=SI|S|1|NO|N|0
EMERGENTE_ORDENAR=SI|S|1|NO|N|0
EMERGENTE_RENOVAR_AHORA=SI|S|1|NO|N|0
EMERGENTE_MODIFICAR_ESTADO=SI|S|1|NO|N|0
EMERGENTE_ESTABLECER_POR_OMISION=SI|S|1|NO|N|0
EMERGENTE_INHABILITAR_SPOOL=SI|S|1|NO|N|0
EMERGENTE_COMPROBAR_DISCO=SI|S|1|NO|N|0
EMERGENTE_DAR_FORMATO_DISCO=SI|S|1|NO|N|0
EMERGENTE_COPIAR_DISCO=SI|S|1|NO|N|0
EMERGENTE_ABRIR_PADRE=SI|S|1|NO|N|0
EMERGENTE_RECOGER=SI|S|1|NO|N|0

VALORES_GENERAL=SI|S|1|NO|N|0
VALORES_VENTANA_SISTEMA=SI|S|1|NO|N|0
VALORES_VISTA1_RELOJ_SISTEMA=SI|S|1|NO|N|0
VALORES_VISTA2_RELOJ_SISTEMA=SI|S|1|NO|N|0
VALORES_FECHA_PAIS=SI|S|1|NO|N|0
VALORES_NUMEROS_PAIS=SI|S|1|NO|N|0
VALORES_PAIS_PAIS=SI|S|1|NO|N|0
VALORES_HORA_PAIS=SI|S|1|NO|N|0
VALORES_BLOQUEAR1_ESCRITORIO=SI|S|1|NO|N|0
VALORES_BLOQUEAR2_ESCRITORIO=SI|S|1|NO|N|0
VALORES_BLOQUEAR3_ESCRITORIO=SI|S|1|NO|N|0

VALORES_DETALLES_DISCO=SI|S|1|NO|N|0
VALORES_MENU=SI|S|1|NO|N|0
VALORES_TIPO=SI|S|1|NO|N|0
VALORES_ARCHIVO1=SI|S|1|NO|N|0
VALORES_ARCHIVO2=SI|S|1|NO|N|0
VALORES_ARCHIVO3=SI|S|1|NO|N|0
VALORES_FONDO=SI|S|1|NO|N|0
VALORES_INCLUIR=SI|S|1|NO|N|0
VALORES_CLASIFICAR=SI|S|1|NO|N|0
VALORES_VER1=SI|S|1|NO|N|0
VALORES_VER2=SI|S|1|NO|N|0
VALORES_VER3=SI|S|1|NO|N|0
VALORES_DISTRIBUCION_TECLADO=SI|S|1|NO|N|0
VALORES_NEC_ESPEC_TECLADO=SI|S|1|NO|N|0
```

```
VALORES_TIEMPOS_TECLADO=SI|S|1|NO|N|0
VALORES_DISTRIBUCION_RATON=SI|S|1|NO|N|0
VALORES_TIEMPOS_RATON=SI|S|1|NO|N|0
VALORES_CONFIGURACION_RATON=SI|S|1|NO|N|0
VALORES_ALARMA_RELOJ_SISTEMA=SI|S|1|NO|N|0
VALORES_ALIMENTACION_ALIMENTACION=SI|S|1|NO|N|0
VALORES_VER_ALIMENTACION=SI|S|1|NO|N|0
VALORES_PROGRAMA_PROGRAMA=SI|S|1|NO|N|0
VALORES_ASOCIACION_PROGRAMA=SI|S|1|NO|N|0
VALORES_SESION_PROGRAMA=SI|S|1|NO|N|0
VALORES_AVISO_SONIDO_BEEP=SI|S|1|NO|N|0
VALORES_CONFIRMACION_SISTEMA=SI|S|1|NO|N|0
VALORES_LOGOTIPO_SISTEMA=SI|S|1|NO|N|0
VALORES_FECHA_HORA_RELOJ_SISTEMA=SI|S|1|NO|N|0
VALORES_CONTROLADOR_IMPRESORA=SI|S|1|NO|N|0
VALORES_IMPR_PANT_SISTEMA=SI|S|1|NO|N|0
VALORES_IMPRESION_IMPRESORA=SI|S|1|NO|N|0
VALORES_PRIORIDAD_IMPRESION_SPOOL=SI|S|1|NO|N|0
VALORES_SALIDA_IMPRESORA=SI|S|1|NO|N|0
VALORES_COLA_IMPRESORA=SI|S|1|NO|N|0
VALORES_PANTALLA_SISTEMA=SI|S|1|NO|N|0
VALORES_PANTALLA_SISTEMA2=SI|S|1|NO|N|0
VALORES_TITULO_SISTEMA=SI|S|1|NO|N|0
VALORES_VIA_ACCESO_SPOOL=SI|S|1|NO|N|0
VALORES_VER_IMPRESORA=SI|S|1|NO|N|0
VALORES_GENERAL2=SI|S|1|NO|N|0
VALORES_VENTANA_SISTEMA2=SI|S|1|NO|N|0
VALORES_VENTANA_SISTEMA3=SI|S|1|NO|N|0
VALORES_ARCHIVADOR=SI|S|1|NO|N|0
VALORES_ESCRITORIO=SI|S|1|NO|N|0
VALORES_CURSOR_COMETA_RATON=SI|S|1|NO|N|0
VALORES_PUNTEROS_RATON=SI|S|1|NO|N|0
VALORES_ENTRADA_SISTEMA=SI|S|1|NO|N|0
```

Note: Las siguientes palabras clave son aplicables solamente para sistemas con OS/2 3.0 (WARP) o superior :

```
ATRIBUTO_VALORES
EMERGENTE_ABRIR_PADRE
EMERGENTE_RECOGER
VALORES_GENERAL2
VALORES_VENTANA_SISTEMA2
VALORES_VENTANA_SISTEMA3
VALORES_ARCHIVADOR
VALORES_ESCRITORIO
VALORES_CURSOR_COMETA_RATON
VALORES_PUNTERO_RATON
VALORES_ENTRADA_SISTEMA
```

El valor del parámetro *nombreobjeto* puede ser el título del objeto o su identificador (object-ID).

El identificador de objeto y su título se pueden especificar en la *cadena de inicialización* (setup string) del objeto, que es usada para definir los parámetros que caracterizan el comportamiento del objeto como parte del proceso de creación. El identificador de objeto es una cadena única por sistema que acompaña al objeto aún cuando el título del mismo se cambie. Siendo optativo, vd. debe especificarlo de un modo explícito para los objetos que desee tengan identificador asociado.

Cuando identifique los objetos a través de su identificador, escriba vd. este **exactamente** tal y como esté definido, prestando especial atención en los carácteres en mayúscula/minúscula, así como en los carácteres en blanco. No deje blancos adicionales entre los símbolos <, > y el valor de identificador.

Cuando identifique objetos a través de su título, puede vd. especificar títulos de más de una línea usando la cadena \n.

Si vd. indica como nombre de objeto el identificador *DEFAULT*, las propiedades asociadas se aplicarán a todos los objetos que no aparezcan de un modo explícito en el perfil de restricciones (valor por defecto).

El primer bloque de palabras reservadas corresponde a los parámetros de la *cadena de inicialización*, tal como indica el prefijo ATRIBUTO_, excepto en el caso de ATRIBUTO_SOMBRA_RESTRINGIDA, que restringe el alcance de ATRIBUTO_SOMBRA de tal modo que solo se permita la creación de sombras del objeto dentro de *carpetas de usuario*. Éstas últimas se verán más adelante. Así pues, ATRIBUTO_SOMBRA_RESTRINGIDA tan solo será un atributo válido si la opción ATRIBUTO_SOMBRA está habilitada.

Cuando se active un perfil de restricciones de escritorio, todas las propiedades no definidas a través de la palabra reservada ATRIBUTO_ para un objeto determinado, mantendrán su valor asociado tal y como estuviesen definidas antes de la activación del perfil.

El segundo bloque de palabras reservadas corresponde a opciones que pueden ser seleccionadas vía el menú emergente del objeto (prefijo EMERGENTE_).

El tercer bloque de palabras reservadas corresponde a las diferentes páginas de la libreta de valores del objeto, por ejemplo : VALORES_VISTA1_RELOJ_SISTEMA y VALORES_VISTA2_RELOJ_SISTEMA.

Cuando se active un perfil de restricciones de escritorio, aquellas propiedades del menú emergente o libreta de valores no especificadas, mantendrán su estado original.

Para todas las palabras clave, el valor del parámetro puede ser:

SI, S, o 1

> Para permitir una propiedad, enseñar una opción de menú, o una página en la libreta de valores.

NO, N, o 0

> Para inhibir una propiedad, no enseñar una opción de menú, o esconder una página en la libreta de valores.

Las palabras clave y los valores pueden escribirse en mayúscula o minúscula, indistintamente.

Ejemplo de perfil de restricciones tipo texto

```
/* Hacer todos los objetos invisibles, excepto aquellos */
/* explícitamente reseñados                             */

    [DEFAULT]
    ATRIBUTO_VISIBLE=NO

    [Mi programa]
    ATRIBUTO_VISIBLE=SI
    ATRIBUTO_COPIAR=NO
    ATRIBUTO_MOVER=NO
    ATRIBUTO_SUPRIMIR=NO
    ATRIBUTO_ARRASTRAR=NO
    EMERGENTE_COPIAR=NO
    EMERGENTE_SUPRIMIR=NO

    [Escritorio]
    EMERGENTE_ABRIR=NO
    EMERGENTE_RENOVAR=NO
    EMERGENTE_AYUDA=SI
    EMERGENTE_CREAR_SOMBRA=NO
    EMERGENTE_BLOQUEAR_AHORA=SI
    EMERGENTE_CONCLUIR=SI
    EMERGENTE_CONFIGURACION_SISTEMA=NO
    EMERGENTE_BUSCAR=NO
```

```
EMERGENTE_SELECCIONAR=NO
EMERGENTE_CLASIFICAR=NO
EMERGENTE_ORDENAR=NO
```

Controlando las posiciones de los objetos

Para controlar como manejará SecureEntry la posición de los objetos en el escritorio, hay tres opciones diferentes :

1. La opción 'Guardar posiciones' está marcada en la página *escritorio* de la libreta de valores del escritorio.

   En este caso, el Workplace Shell manejará la posición de los mismos, de modo que cualquier cambio de posición que se haga se mantendrá en las sesiones de trabajo subsiguientes.

2. La opción 'Descartar los cambios en las posiciones de las carpetas al terminar la sesión' está marcada en la página *escritorio* de la libreta de valores del escritorio.

   En este caso, SecureEntry mantendrá la lista de posiciones de los objetos del escritorio y de dentro de las carpetas, de tal modo que, al comenzar cada sesión de trabajo, garantice que estas posiciones sean respetadas. Esto permite a los usuarios modificar las posiciones de los objetos durante su sesión de trabajo sin interferir en el aspecto general del escritorio para otros usuarios.

   Si se usa esta opción, los usuarios administradores tendrán la posibilidad de salvar las posiciones actuales vía una nueva opción del menú emergente del escritorio.

3. La opción 'Descartar los cambios en las posiciones de las carpetas al cerrarlas' está marcada en la página *escritorio* de la libreta de valores del escritorio.

   Con esta opción vd. puede conseguir que las posiciones de los objetos de las carpetas se memoricen y activen cada vez que las carpetas se abran.

   Si se usa esta opción, los usuarios administradores tendrán la posibilidad de salvar las posiciones actuales vía una nueva opción del menú emergente del escritorio.

Nota : Observe que cuando modifique la opción seleccionada de la página *escritorio* de la libreta de valores del escritorio, será necesaria una nueva carga del WorkPlace Shell (escritorio) antes de que el nuevo valor tome efecto. Esto quiere normalmente decir que precisará vd. reinicializar la máquina antes de ver el comportamiento deseado.

Personalización del escritorio

Recapitulando, cuando un usuario SecureEntry inicia una sesión, el Workplace Shell se modifica de acuerdo con las especificaciones y restricciones del perfil de restricciones asignado. Podrá entonces modificar el aspecto y propiedades de las carpetas (incluído el escritorio en si), siempre que le esté permitido, incluyendo :

Posiciones de los iconos en la carpeta

Vía las opciones 'clasificar' u 'ordenar', o la página de reordenación de la libreta de valores de la carpeta, o arrastrando y soltando los iconos en la posición nueva.

Propiedades de la vista de la carpeta

A través de las páginas de 'vista' de la libreta de valores de la carpeta.

SecureEntry puede configurarse para que estas modificaciones sean descartadas al cerrar la carpeta y/o la sesión de trabajo, de modo que el aspecto y posición de los objetos en las carpetas no varíe para el resto de usuarios, siempre que se haya previsto tal y como se explicó en Controlando las posiciones de los objetos.

```
************************************************
NOTA IMPORTANTE

Lo que sigue es la descripción de como crear y
definir carpetas personalizadas (asociadas a
usuarios), así como carpetas con memoria, utilizando
el componente de definición de restricciones del
escritorio. Esta funcionalidad se mantiene por
cuestión de compatibilidad con versiones antiguas
de SecureEntry, pero se desaconseja su uso, ya que
el nuevo componente de Definición de escritorios personalizados
permite conseguir el mismo objetivo de un modo mucho
más flexible y rápido.
************************************************
```

No obstante, SecureEntry permite adicionalmente que el administrador asocie carpetas y valores a un usuario final, de modo que los cambios que este efectúe sobre las mismas sean guardados en tiempo de desconexión, y más tarde reinstaurados, en la misma u otra máquina, cuando decida reanudar su trabajo.

Para definir carpetas con posiciones personalizadas según el usuario, deberá el administrador definir estas carpetas como *carpetas con memoria* asociadas al usuario en su perfil de restricciones.

Adicionalmente, el administrador podrá definir *carpetas de usuario*, que serán recreadas, junto con sus contenidos y valores, en tiempo de conexión del usuario. En estas carpetas el usuario podrá crear objetos de tipo sombra de otros existentes en el sistema, y manejar su contenido de modo que este sea guardado al desconectar la sesión. Estas carpetas son una buena opción para que los usuarios configuren en ella los objetos que utilizan con más frecuencia.

Carpetas con memoria

Si una carpeta se define como carpeta con memoria, ciertos cambios que efectúe un usuario sobre la carpeta serán guardados como atributos asociados al usuario para esa carpeta, de modo que, cuando este se desconecte y después vuelva a reconectarse, no se perderán. Estos cambios incluyen :

Posiciones de los iconos.

Propiedades de las vistas que puedan configurarse vía las páginas de vista de la libreta de valores de la carpeta (vista de iconos, árbol y detalle).

El administrador puede definir cualquier carpeta como carpeta con memoria, incluída la vista del escritorio, a través de un perfil de personalización, como se indica más abajo.

Carpetas de usuario

Las carpetas de usuario son una clase de carpetas SecureEntry donde solamente pueden crearse o borrarse objetos tipo sombra. Así mismo, estas carpetas pueden existir solamente a primer nivel en el escritorio.

Las carpetas definidas como de usuario son creadas en tiempo de conexión a partir de el perfil dinámico asociado al usuario, y destruídas en tiempo de desconexión, no sin antes guardar los eventuales cambios a las mismas para futuras conexiones.

Para poder crear sombras de objetos sobre carpetas de usuario, el objeto debe tener permitida dicha operación (ATRIBUTO_SOMBRA habilitado, y opcionalmente ATRIBUTO_SOMBRA_RESTRINGIDA habilitado) en el perfil de restricciones activo.

El administrador del sistema puede también asignar carpetas de usuario a grupos de usuarios a través del perfil de personalización.

Configurando perfiles de personalización

Los perfiles de personalización pueden configurarse para usuarios individuales o grupos de usuarios. Vd. puede crear un perfil de restricciones de texto con las sentencias de personalización necesarias como punto de partida. Siga el siguiente proceso :

Edite y guarde el perfil de personalización, igual que en el caso de perfil de restricciones de escritorio. De hecho, puede vd. utilizar el mismo perfil de texto para ambos propósitos.

Compile el perfil de personalización. Arrastre y suelte el perfil sobre el objeto 'traductor de texto a binario'. Si el perfil contiene sentencias de personalización, se creará un perfil de personalización binario con la extensión *PER*.

Ya puede vd. asignar dicho perfil a usuarios o grupos, utilizando las herramientas de administración de usuarios y grupos SecureEntry.

Formato de las sentencias de personalización

Vd. puede replicar la estructura básica de definición de una *carpeta con memoria* cuantas veces sea necesario.

Se utilizan las siguientes convenciones: ;p.

MAYÚSCULAS representan valores que vd. puede especificar directamente, sin cambios.

minúsculas representan variables a sustituir por el valor adecuado.

Estructura de palabras reservadas de un perfil de personalización de texto

```
[nombreobjeto]
  SALVAR_POSICION_ICONOS=SI|S|1|NO|N|0

[_SE_CARPETA_USUARIO_]
  CREAR_CARPETA=SI|S|1|NO|N|0
```

El parámetro *nombreobjeto* puede indicar el identificador de objeto de la carpeta, o bien su título.

La palabra reservada SALVAR_POSICION_ICONOS puede estar configurada para que se guarden dinámicamente las posiciones de los objetos contenidos (SI,S o 1), o para que no se guarden (NO, N, o 0).

Cuando la palabra CREAR_CARPETA tenga asignado alguno de los valores SI, S o 1, se creará dicha carpeta al inicio de la sesión.

Las palabras clave y los valores pueden escribirse en mayúscula o minúscula, indistintamente.

Ejemplo de perfil de personalización

```
/* El desktop mantiene su apariencia y la carpeta de */
/* productividad no debe guardar las posiciones, al  */
/* igual que las otras carpetas del sistema          */

       [<WP_DESKTOP>]
         SALVAR_POSICION_ICONOS=SI

       [<WP_TOOLS>]
         SLVAR_POSICION_ICONOS=NO

/* El usuario dispone de una carpeta de usuario      */

       [_SE_CARPETA_USUARIO_]
         CREAR_CARPETA=SI
```

Interfície de activación de los perfiles

Descripción

La interfície de programación del componente de restricciones de escritorio consiste en :

Una librería de carga dinámica (DLL) denominada EDYSHELL.DLL.

El módulo de librería EDYSHELL.LIB.

El archivo de definiciones EDYSHELL.H.

Esta librería proporciona únicamente la función edy_refresh_profile, para activar un perfil de escritorio.

Dicha función refresca los objetos del Workplace Shell según las definiciones del perfil suministrado.

Sintaxis de edy_refresh_profile

```
LONG APIENTRY edy_refresh_profile (CHAR *nombreperfil)
```

Donde *nombreperfil* es la vía de acceso y nombre del archivo de perfil que se desea activar. En caso de pasar el valor NULL, se buscará el archivo VíaDeAccesoSecureEntry\WORK\EDYDESK.INI o, en su defecto, VíaDeAccesoSecureEntry\NOUSER\EDYDESK.INI

Códigos de retorno de edy_refresh_profile

Código	Descripción
0001x	Correcto
0000x	Error refrescando el Workplace Shell
FFFFx	Error al obtener el código de retorno Workplace Shell
Otro	Error básico de OS/2

Sintaxis de los comandos

Esta sección describe los comandos que pueden ser entrados desde una ventana OS/2 para arrancar las herramientas relacionadas con el manejo de perfiles de restricción del escritorio.

Comando de activación de perfiles

El comando EDYREFR tiene como objeto la activación de un perfil de restricciones de escritorio. Entre :

```
EDYREFR [nombreperfil]      o
EDYTEST [nombreperfil]
```

nombreperfil

Vía de acceso y nombre del archivo de perfil a activar.

Si no se proporciona, se activará VíaDeAccesoSecureEntry\WORK\EDYDESK.INI o, en su defecto, VíaDeAccesoSecureEntry\NOUSER\EDYDESK.INI

Comando de traducción de texto a binario

Para iniciar la herramienta de traducción de texto a binario, entre :

```
EDYT2B perfiltexto perfilbinario
```

perfiltexto

Vía y nombre del archivo con el perfil de restricciones en modo texto. Es el archivo de entrada.

perfilbinario

Vía y nombre del archivo binario a crear. Es el archivo de salida.

Comando de traducción de binario a texto

Para iniciar la herramienta de traducción de binario a texto, entre :

```
EDYB2T perfilbinario perfiltexto
```

perfilbinario

Vía y nombre del archivo con el perfil de restricciones en binario a traducir. Es el archivo de entrada.

perfiltexto

Vía y nombre del archivo texto a crear. Es el archivo de salida.

Comando para capturar el perfil actual

Para iniciar la herramienta de captura, entre :

```
EDYSAVEE  [perfiltexto] [/ID:(YES|NO)]
```

perfiltexto

Nombre de archivo donde escribir las restricciones capturadas. Por defecto, se usará **EDYDESK.TXT**.

ID

Especifica si se deben identificar los objetos por identificador de objeto (valor YES), o bien por su título (defecto : valor NO).

Definición de escritorios personalizados

SecureEntry permite que el administrador del sistema asocie ciertas carpetas y los valores de las mismas a un usuario o grupo de usuarios, de modo que los cambios que este efectúe sobre éstas sean guardados en tiempo de desconexión, y más tarde reinstaurados, en la misma u otra máquina, cuando decida reanudar su trabajo. A estas carpetas se les denomina *carpetas con memoria*.

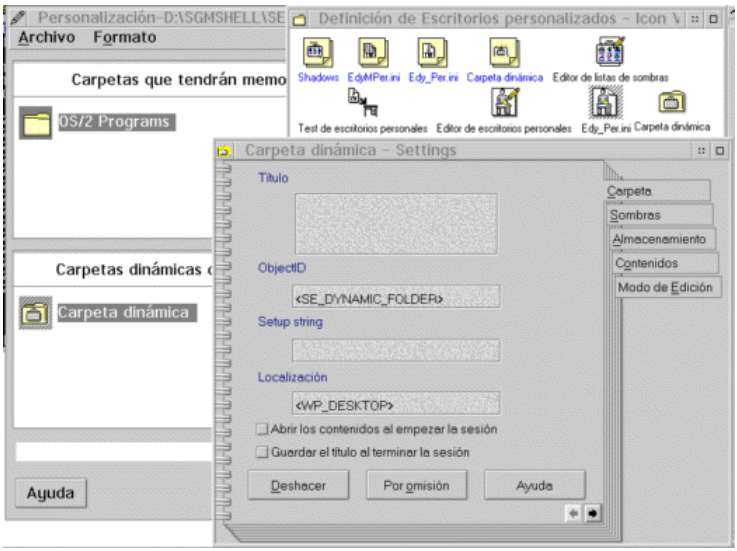
Adicionalmente, el administrador puede definir *carpetas de usuario*, que son creadas, junto con sus contenidos y valores, en tiempo de conexión del usuario. En estas carpetas el usuario final puede crear y/o borrar objetos de tipo sombra de otros existentes en el sistema, y manejar su contenido a su gusto. Al desconectar la sesión, el contenido de estas carpetas se guardará también asociado al usuario para cuando éste se reconecte. Estas carpetas son una buena opción para que los usuarios configuren en ella los objetos que utilizan con más frecuencia.

Originalmente, este tipo de carpetas se configuraban con SecureEntry vía el componente de restricciones del escritorio, y aunque esto puede hacerse todavía, El **componente de definición de escritorios personalizados** permite hacerlo de un modo más sencillo y flexible. Así pues, este componente permite definir las *carpetas con memoria* y *carpetas de usuario* (en adelante llamadas *carpetas dinámicas*)

Al igual que con el resto de componentes, el proceso de configuración consiste en crear un perfil de personalización, asignándolo después al usuario o grupo específico vía las herramientas de administración de usuarios y grupos.

Los perfiles de personalización tienen la característica especial de que son modificados indirectamente por el usuario durante su sesión de trabajo (p.e, al cambiar las posiciones de los iconos de una carpeta con memoria), y por tanto son dinámicos en el sentido de que, en cada desconexión, se recopian en la base de datos de usuarios y grupos reemplazando la instancia antigua existente de los mismos. Es por ello que, aunque vd. puede asignar un perfil de personalización a un grupo de usuarios, este se utilizará solamente como 'modelo' para crear el perfil específico de cada usuario perteneciente al grupo.

Para trabajar con este componente, abra la carpeta de *definición de escritorios personalizados*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:



Utilice los objetos de esta carpeta para :

Definir Carpetas dinámicas

Editar Perfiles y modelos de personalización

Editar Carpetas con memoria

Editar Listas de sombras con el editor de listas de sombras

Carpetas dinámicas

Las **Carpetas dinámicas** (también llamadas carpetas de usuario) son carpetas especiales que :

Tan solo pueden contener objetos de tipo sombra, que se añaden arrastrando y soltando sobre ellas los objetos originales.

Pueden almacenar la lista de sombras contenida en el propio perfil de personalización que las define, para usarse desde distintas estaciones de trabajo.

Se crean en tiempo de conexión y se destruyen en la desconexión.

Pueden ser definidas como carpetas de autoarranque de modo que sus contenidos se abran en la conexión.

La lista de sombras contenidas puede almacenarse, como hemos dicho, en el propio perfil de personalización, o bien en un archivo externo, que se referencia por medio de su vía de acceso en el perfil. En este último caso, es entonces el administrador quien debe decidir si los usuarios pueden o no modificar el contenido de las mismas.

Las carpetas dinámicas son una herramienta útil para :

Permitir a los usuarios disponer de una carpeta personal, donde ellos puedan poner los objetos que deseen.

Asignar a los usuarios carpetas de autoarranque, donde ellos decidan que objetos o aplicaciones abrir al conectarse.

Disponer de carpetas de autoarranque configuradas por el administrador.

Tener carpetas con contenidos dependientes de la estación de trabajo, configuradas por el administrador según el tipo de máquina y aplicaciones instaladas.

Tener carpetas compartidas por grupos de usuarios en la red.

Dado que en las carpetas dinámicas se definen sombras de otros objetos, los objetos referenciados deben estar disponibles en la máquina donde éstas se activen.

Vd. puede crear una carpeta dinámica a partir del modelo suministrado en la carpeta de definición de escritorios personalizados. Esta carpeta puede entonces asignarla a un perfil de personalización determinado, arrastrándola y soltándola sobre el contenedor de carpetas dinámicas que muestra el editor de perfiles de escritorios personalizados.

Perfiles y modelos de personalización

Los perfiles de personalización especifican

Las carpetas dinámicas a crear en tiempo de conexión

Un conjunto de carpetas existentes que deben actuar con memoria durante el periodo en el que el perfil esté activo.

Los **perfiles de personalización** (creados a partir del modelo de objeto *Edy_Per.ini*) contienen normalmente información específica de usuario, que además se modifica dinámicamente durante la sesión de trabajo. Por ello, estos perfiles son almacenados de nuevo en tiempo de desconexión. Si el administrador define un perfil de personalización para un grupo de usuarios o en la carpeta *NOUSER*, este será tomado como un modelo para crear y asignar dinámicamente una copia a los diferentes usuarios a medida que se vayan conectando.

Los **modelos de personalización** (creados a partir del modelo de objeto *Edy_MPer.ini*) tienen el mismo formato que los perfiles de personalización, pero no contienen información dependiente del usuario, y pueden ser usados no solamente para crear los perfiles de personalización iniciales de los usuarios, si no también para actualizar estos con las nuevas definiciones. Estos modelos pueden ser asignados a grupos de usuarios o como defecto de máquina, en la carpeta *NOUSER*

Cuando se conecta un usuario que dispone de modelo de personalización, bien porque éste ha sido definido para los usuarios de su grupo, o por que se halle en la carpeta *NOUSER*, su perfil de personalización se actualizará con las definiciones que se encuentren en el modelo :

Si el usuario **no** dispone de perfil de personalización, se creará uno con las definiciones del modelo, y en tiempo de desconexión, le será asignado al usuario permanentemente.

Cualquier carpeta dinámica o con memoria definida en el perfil y no definida en el modelo será borrada del perfil de personalización.

Cualquier carpeta dinámica o con memoria definida en el modelo y no en el perfil de personalización será añadida al perfil.

Las carpetas dinámicas definidas tanto en el modelo como en el perfil de personalización serán actualizadas en el perfil con los valores hallados en el modelo. No obstante, mantendrán sus contenidos intactos (sombras).

Carpetas con memoria

Cuando se define una carpeta como **carpeta con memoria** en el perfil de personalización de un usuario, los cambios de presentación que el usuario haga sobre el mismo, se almacenarán en el perfil de personalización, de modo que serán reaplicados a la carpeta cuando el usuario se conecte de nuevo en la misma u otra estación de trabajo. La información que se memoriza es la siguiente:

Posición de la ventana.

Posición de los objetos contenidos.

Atributos de la vista y fuentes de presentación.

Vd. tan solo puede definir como carpetas con memoria aquellas carpetas que dispongan de un identificador de objeto asociado.

Listas de sombras

Los archivos de **Listas de sombras** (creados a partir del modelo de objeto *Lista de sombras*) se utilizan para almacenar los contenidos de las carpetas dinámicas, y también para definir el proceso de autoarranque SecureEntry (objeto *EdyStart* en la carpeta *NOUSER*). También pueden usarse para editar modelos de carpeta dinámica.

Los archivos de lista de sombras pueden verse y editarse con el objeto *editor de listas de sombras* o directamente desde la página de contenido de la libreta de edición de los objetos de tipo *carpeta dinámica*.

Las sombras pueden añadirse arrastrando y soltando los objetos deseados sobre el contenedor, y borrarse a través de su menú emergente.

Definición de objetos con activadores

El componente de objetos con activadores permite crear un perfil de seguridad en el que se especifica para qué objetos se debe establecer un *activador*. Un *activador* es una exit de usuario, a través de la que se puede llamar a un programa externo en los momentos de apertura y/o cierre de los objetos deseados. En el caso de la apertura, el programa externo puede entonces decidir si se debe aceptar o rechazar la petición de apertura. Con este esquema resulta extremadamente fácil configurar objetos que requieran, por ejemplo, una palabra clave para abrirse, u otros que abran a su vez en cascada, otros objetos relacionados.

Los objetos para los que se definan activadores deben ser de tipo carpeta o programa, y tener un identificador de objeto asociado.

Para trabajar con este componente, abra la carpeta de *definición de objetos con activadores*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Para crear un perfil de seguridad para este componente, utilice el objeto modelo suministrado (*EDYCUSWP.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor de objetos con activadores*, o bien haga doble click sobre el mismo. Efectúe las modificaciones pertinentes, y después salve el perfil modificado. En caso de duda, consulte la ayuda disponible desde el mismo programa editor.

Para verificar el comportamiento de un perfil de seguridad de objetos con activadores, arrástrelo y suéltelo sobre el objeto *Test de objetos con activadores*, o bien active la función de prueba vía el menú emergente del perfil. El perfil definido se activará.

Este componente proporciona además un programa *activador* de ejemplo, que implementa un algoritmo de claves de un solo uso razonablemente seguro, de tal modo que resulta una tarea muy sencilla el configurar un objeto para que solicite dicha palabra clave en cualquier intento de apertura. La palabra clave será proporcionada por el administrador, ejecutando el programa complementario al activador, es decir, el *generador de claves de un solo uso*. Las claves generadas son válidas para cualquier máquina SecureEntry de la misma institución, y dependen de la fecha/hora del sistema.

Como con cualquier otro componente, una vez definidos los perfiles, puede vd. asignarlos a usuarios o grupos de usuarios utilizando las herramientas de administración. Así mismo, puede establecer perfiles de objetos con activadores como defecto de máquina, copiando el perfil sobre la carpeta *NOUSER* de la vía de acceso donde SecureEntry esté instalado.

Utilidades de claves de un solo uso

Generación de claves

Verificación de claves

Generación/Verificación de claves por defecto

Utilidades de claves de un solo uso

Estas utilidades permiten generar y verificar claves a partir de una fecha/hora determinadas :

La utilidad de generación, **edyotpg.exe**, que se halla en el directorio **<sgm_shell>\exec**, genera una clave a partir de los datos de fecha/hora suministrados.

La utilidad de verificación, **edyotpv.exe**, que se halla también en el directorio **<sgm_shell>\exec**, toma como entrada una clave y la valida para la fecha y hora actual. En caso de que sea correcta, devolverá un 0. En caso contrario un 1.

Vd. puede proporcionar su algoritmo personal de generación y verificación de claves, o bien trabajar con el algoritmo proporcionado por los programas.

Las claves de un solo uso son útiles para restringir el acceso a ciertos recursos a aquellos usuarios que, bajo supervisión del administrador, deban acceder a los mismos. Cuando el usuario intenta acceder a estos, se ejecutará edyotpv.exe, y este se verá forzado a contactar con el administrador para obtener la palabra clave asociada al par fecha/hora presentado. El administrador a su vez ejecutará edyotpg.exe, para generar la clave siempre que el usuario tenga justificado el acceso a los recursos protegidos, y se la transmitirá. Por supuesto, para que este esquema funcione, los usuarios no deben tener permitido el cambio de fecha y hora del sistema.

Generación de claves

Este programa está diseñado para tomar como entrada un par fecha/hora (o cadena semilla aleatoria), y generar como salida una clave que será válida para el programa verificador solamente para esa fecha y hora (o semilla) particular.

La sintaxis es :

```
edyotpg [/G<víageneración>] [/K] [/R(S|D|M|H)] [/M]
```

<víageneración>

Es la vía de acceso y nombre de archivo que implementa el algoritmo alternativo (opcional) de generación de claves.

/K

Use este parámetro para trabajar con cadenas semilla en lugar de pares fecha/hora.

/R

Fija la resolución a (S)egundos, (D)ías, (M)inutos o (H)oras.

/M

Hace que la ventana sea modal de sistema

Si vd. usa un algoritmo alternativo de generación de claves, éste debe seguir ciertas reglas :

Debe ser un módulo ejecutable (.exe).

Este programa recibirá dos parámetros, en caso de trabajar con fecha/hora, siendo el primero la fecha en formato dd/mm/yyyy, y el segundo la hora, en formato hh:mm:ss. En caso de usar cadenas semilla, ésta se recibirá como único parámetro (6 posiciones).

Deberá devolver 0 si la generación es correcta, y 1 en caso contrario.

La clave generada deberá escribirla al dispositivo de salida estándar (stdout), y deberá ser la primera salida que el programa genere.

En caso de no devolver 0, el programa podrá escribir un mensaje de error por el dispositivo de salida, que el programa generador mostrará en pantalla.

Verificación de claves

Este programa valida una clave entrada por el usuario contra el par fecha/hora actual, o la semilla aleatoria suministrada. En caso correcto, puede opcionalmente ejecutar un programa que se suministra como parámetro, y devolverá código de retorno 0. Si la validación no fuese correcta, se devolvería 1. La sintaxis de llamada es :

```
edyotpv [/E<víaprograma>] [/ID<cadena>] [/Dn(S|D|M|H)] [/K] [/R(S|D|M|H)] [/M]
```

<víaprograma>

Es la vía de acceso y nombre de archivo a ejecutar en caso de validación correcta (opcional).

/ID<cadena>

Es un identificador de instancia, en caso de que haya más de un recurso protegido por *edyotpv.exe* Sirve para diferenciar ambos recursos en los perfiles de inicialización de *edyotpv.exe*. Ponga aquí cualquier cadena de carácteres que identifique unívocamente el recurso protegido.

/DnX

Duración de la clave. Si este parámetro se especifica, la misma clave será considerada válida durante el intervalo especificado de duración, una vez entrada por primera vez y para el mismo identificador de recurso (/IDxxx). Así por ejemplo. /D3H indica : 'las claves serán válidas durante 3 horas'.

/K

Use este parámetro para trabajar con cadenas semilla en lugar de pares fecha/hora.

/R

Fija la resolución a (S)egundos, (D)ías, (M)inutos o (H)oras.

/M

Hace que la ventana sea modal de sistema. Use esta opción si desea ejecutar el programa desde una exit de usuario en tiempo de conexión o desbloqueo.

Nota: Si no se especifica parámetro (/E), no se ejecutará ningún programa después de validar una clave.

Vd. puede especificar su propio programa de verificación de claves, llamándolo **edyotpv.exe** y poniéndolo en el directorio **<sgm_shell>\nouser**. En este caso, las reglas de interfície de este programa serán :

El programa deberá llamarse **edyotpv.exe** o **edyotpv.cmd** y estar en el directorio **<sgm_shell>\nouser**.

Este programa recibirá tres parámetros, en caso de trabajar con fecha/hora, siendo el primero la fecha en formato dd/mm/yyyy, y el segundo la hora, en formato hh:mm:ss. El tercero será la clave entrada en mayúsculas, para su verificación. En caso de usar cadenas semilla, ésta se recibirá como primer parámetro (6 posiciones), siendo el segundo la clave a verificar en mayúsculas.

Deberá devolver un 0 en caso de verificación satisfactoria, y un 1 en caso contrario.

Los mensajes que el programa escriba al dispositivo de salida estándar serán presentados al usuario en caso de validación no satisfactoria.

Generación/Verificación de claves por defecto

Las rutinas de generación y verificación de claves trabajan con cadenas de **seis carácteres** sobre el alfabeto **({'A'..'Z'} - {'P','T','V','N'}) U {'0'..'9'}**. Los carácteres 'P','T','V','N' se han excluído por razones fonéticas de similitud con otros, de modo que :

'V' y 'P' se tratan como 'B'.

'T' se trata como 'D'.

'N' se trata como 'M'.

..para evitar confusiones a la hora de transmitir las claves oralmente.

Definición de características del launchpad (barra de herramientas)

El componente de definición de launchpads permite crear perfiles de seguridad que definen barras de herramientas (launchpads) OS/2, con la información necesaria para recrear dicho launchpad en el momento en que el perfil sea activado. Adicionalmente permite restringir ciertas características de la barra de herramientas que pudieran ser peligrosas en un entorno SecureEntry. Este es un ejemplo claro de componente de personalización, en el que el objetivo debe ser adaptar la barra de herramientas a las necesidades de los diferentes usuarios y/o grupos de usuarios que deban utilizarlo.

Para trabajar con este componente, abra la carpeta de *definición de características del launchpad*, que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Para crear un perfil de seguridad para este componente, utilice el objeto modelo suministrado (*EDYPAD.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor de características del launchpad*, o bien haga doble click sobre el mismo. Verá como el color de fondo de la barra de herramientas (launchpad) cambia de color, indicando que está vd. en modo edición. Efectúe las modificaciones pertinentes, editando el lanchpad de forma normal (arrastrando los objetos necesarios) y después salve el perfil modificado, vía la

opción 'salvar' de su menú emergente. Por último cierre el editor por medio de la entrada 'cerrar', también localizada en el menú emergente del launchpad.

Observe que la libreta de valores de una barra de herramientas (launchpad) SecureEntry añade ciertas características al mismo :

Posibilidad de fijar la posición del mismo.

Posibilidad de desactivar los botones de acción.

Para verificar el comportamiento de una barra de herramientas (launchpad) personalizado, arrástrelo y suéltelo sobre el objeto *Test de características del launchpad*, o bien active la función de prueba vía el menú emergente del perfil. El perfil definido se activará y la barra de herramientas activa será el que define el perfil.

Una vez configurado asocie el perfil al usuario o grupo deseado, arrastrando y soltando el perfil sobre el contenedor adecuado de la herramienta de administración de usuarios y/o grupos, o bien establezca el mismo como defecto de máquina, copiando el perfil con su nombre por defecto (EDYPAD.INI) en la carpeta NOUSER.

Definición de WarpCenters

El componente de definición de warpcenters permite crear y configurar perfiles de seguridad SecureEntry que contienen la información necesaria para activar dinámicamente el warpcenter que definen, en tiempo de conexión. Con él puede vd. definir warpcenters personalizados que contengan referencias a los objetos necesarios para sus usuarios o grupos de usuarios, según su perfil de trabajo.

Para trabajar con este componente, abra la carpeta de *definición de warpcenters* , que se encuentra a su vez en la carpeta de *herramientas de administración SecureEntry*:

Para crear un perfil de seguridad para este componente, utilice el objeto modelo suministrado (*EDYSC.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor warpcenter*, o bien haga doble click sobre él mismo. Verá como el color de fondo del warpcenter cambia de color, indicando que está vd. en modo edición. Efectúe las modificaciones pertinentes, editando el warpcenter de forma normal (arrastrando los objetos necesarios) y después salve el perfil modificado, vía la opción 'salvar' de su menú emergente. Por último cierre el editor por medio de la entrada 'cerrar', también localizada en el menú emergente del launchpad.

Observe que la libreta de valores de un warpcenter SecureEntry añade ciertas características al mismo :

Posibilidad de utilizar la lista de tareas OS/2 en lugar de la lista de tareas del warpcenter estándar, cuando se activa ésta desde el warpcenter.

Posibilidad de inhibir el uso del botón *Buscar* del warpcenter.

Posibilidad de deshabilitar la función de búsqueda de los objetos originales vía el menú emergente de los objetos del warpcenter.

Posibilidad de deshabilitar la opción de borrar del menú emergente de los objetos del warpcenter.

Posibilidad de cambiar la funcionalidad del botón de conclusión del warpcenter, haciendo que éste sirva para desconectar la sesión.

Para verificar el comportamiento de un warpcenter personalizado, arrástrelo y suéltelo sobre el objeto *Test WarpCenter*, o bien active la función de prueba vía el menú emergente del perfil. El perfil definido se activará y el warpcenter activo será el que define el perfil.

Una vez configurado asocie el warpcenter al usuario o grupo deseado, arrastrando y soltando el perfil sobre el contenedor adecuado de la herramienta de administración de usuarios y/o grupos, o bien establezca el mismo como defecto de máquina, copiando el perfil con su nombre por defecto (EDYSC.INI) en la carpeta NOUSER.

Nuevas cadenas de inicialización

Variables de entorno SecureEntry - warpcenter

Nuevas cadenas de inicialización

A continuación se detallan las nuevas cadenas de inicialización (setup strings) que SecureEntry añade a la clase SmartCenter. Estas cadenas solamente funcionarán con la instancia del SmartCenter que tenga asociado el identificador de objeto <WP_WARPCENTER>.

EDYSCOPEN=*YES*

Abre la vista por defecto del WarpCenter (igual que hacer doble click).

EDYSCCLOSE=*YES*

Cierra la vista por defecto del WarpCenter.

EDYSCDELETETRAY=*número de bandeja*

Borra la bandeja indicada.

EDYSCTRAYNAME=*nombre de bandeja*

Renombra la bandeja actual.

EDYSCCONFIRMSHUTDOWN=*{YES|NO}*

Habilita/inhibe la confirmación al concluir.

EDYSCLARGEICONS=*{YES|NO}*

Usar iconos grandes/medianos.

EDYSCDISPLAYALWAYS=*{YES|NO}*

Muestra el WarpCenter solamente cuando el ratón está sobre él o siempre.

EDYSCFLOATONTOP=*{YES|NO}*

Hace que WarpCenter flote (o no) por encima de las ventanas maximizadas.

EDYSCTOPPOSITION=*{YES|NO}*

Muestra el WarpCenter en la parte superior/inferior de la pantalla.

EDYSCBUBBLEHELP=*{YES|NO}*

Habilita/inhibe la ayuda de burbuja en el WarpCenter.

ADDTRAY=*nombre bandeja [,ID objeto,...]*

Añade una nueva bandeja con el nombre especificado conteniendo los objetos indicados.

Variables de entorno SecureEntry - warpcenter

A continuación se muestran las variables de entorno que pueden usarse para modificar el comportamiento del WarpCenter:

SCKillFeatureEnabled=*YES*

Permite que se puedan terminar procesos desde la lista de tareas original del WarpCenter. Solamente funciona si vd. no tiene configurada la sustitución de esta función por la lista de tareas OS/2.

SCFindUtility=*VíaArchivo*

El ejecutable especificado en *VíaArchivo* será arrancado siempre que se pulse sobre el botón de búsqueda del WarpCenter. Solamente funcionará cuando dicho botón esté habilitado en el perfil activo de definición de WarpCenter.

SCUsePrettyClock=*YES*

Cambia el reloj del WarpCenter por uno alternativo.

SCCanbeNuked=*1*

Permite borrar las instancias de clase SmartCenter. Tan solo funcionará si SGM_EDYSC_DISABLE está definido.

SGM_EDYSC_DISABLE=*YES*

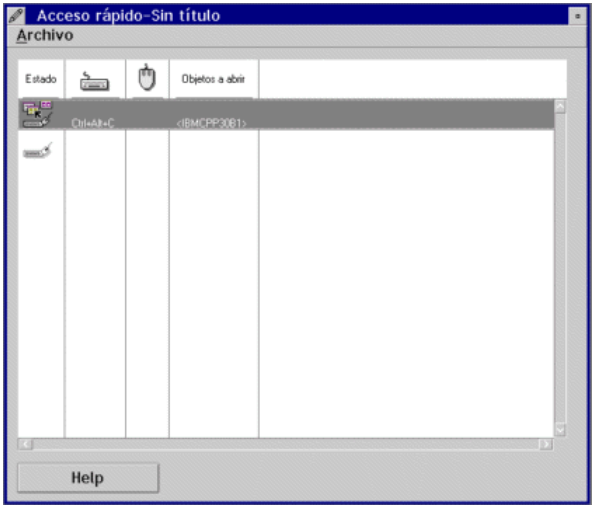
Desactiva toda la funcionalidad SecureEntry añadida a WarpCenter.

Definición de combinaciones de acceso rápido

Este componente permite definir en un perfil de personalización SecureEntry, eventos formados por combinaciones de teclas y/o acciones de ratón, junto con una lista de objetos asociados, que serán abiertos cuando dicho evento sea detectado por el sistema mientras el perfil esté activo.

Para crear un perfil de personalización para este componente, utilice el objeto modelo suministrado (*EDYHOTK.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor de combinaciones de acceso rápido*, o bien haga doble click sobre el mismo. Efectúe las modificaciones pertinentes y después salve el perfil modificado. Para cualquier duda, consulte la ayuda interactiva del editor.



Tenga especial cuidado en no definir combinaciones de teclas que el sistema utilice para otros propósitos.

Para verificar el comportamiento del perfil, arrástrelo y suéltelo sobre el objeto *Test de combinaciones de acceso rápido*, o bien active la función de prueba vía el menú emergente del mismo. El perfil definido se activará y podrá vd. comprobar su funcionamiento.

Una vez configurado, asocie el perfil al usuario o grupo deseado, arrastrándolo y soltándolo sobre el contenedor adecuado de la herramienta de administración de usuarios y/o grupos, o bien establezca el mismo como defecto de máquina, copiándolo con su nombre por defecto (EDYHOTK.INI) en la carpeta NOUSER.

Definición de Aplicaciones Públicas

El componente de aplicaciones públicas permite gestionar, en entornos de LAN Server, la definición de sus aplicaciones públicas. Además, este componente permite definir en un perfil de SecureEntry las aplicaciones públicas de un dominio LAN Server que deben aparecer en la carpeta *Aplicaciones públicas* de un usuario en cuanto este se conecta al sistema.

Para trabajar con este componente, abra la carpeta de *Definición de Aplicaciones Públicas*, que se encuentra a su vez en la carpeta *Herramientas de Administración SecureEntry*.

Para crear un perfil de personalización para este componente, utilice el objeto modelo suministrado (*EDYROAM.INI*), arrastrando y soltando una copia a partir del mismo.

Para modificar un perfil de este tipo, arrástrelo y suéltelo sobre el *Editor de Aplicaciones Públicas*, o bien haga doble click sobre el mismo. Efectúe las modificaciones pertinentes y después salve el perfil modificado. Para cualquier duda, consulte la ayuda interactiva del editor.

El mismo editor puede serle útil a la hora de configurar, no tan sólo el conjunto de aplicaciones públicas que deben aparecer en la carpeta de un usuario en tiempo de conexión, sino también las aplicaciones públicas del propio controlador de dominio del dominio LAN Server en el que esté conectado.

Tenga en cuenta los siguientes puntos:

El editor de este componente obtiene el nombre del servidor controlador de dominio del dominio al que el usuario administrador se ha conectado. Esto significa que si dicho usuario ha realizado una conexión SecureEntry desde el propio controlador de dominio a otro dominio, y luego realiza una desconexión de la LAN no SecureEntry, podrá seguir administrando las aplicaciones públicas del controlador de dominio en el que físicamente se encuentre.

El editor de este componente maneja dos listas de aplicaciones: la lista de la izquierda contiene las definiciones de aplicaciones públicas a asignar a un perfil SecureEntry y usa las definiciones de recursos existentes en el repositorio SecureEntry. La lista de la derecha contiene las definiciones de aplicaciones públicas que deben residir en el controlador de dominio y usa las definiciones de recursos existentes en el controlador de dominio. Esto significa, en entornos corporativos que usen UCM, que los recursos, i.e, los álias, disponibles pueden ser distintos en las dos listas.

El cuaderno de edición de aplicaciones públicas OS/2 contiene una pestaña de nombre *Parámetros*. Usted puede proporcionar información en esta hoja cualquiera que sea el entorno en el que esté trabajando, aunque dicha información sólo será efectiva si está administrando aplicaciones públicas para entornos de WorkSpace On-Demand. Remítase a Consideraciones en entornos de WorkSpace On-Demand para obtener más información.

Para verificar el comportamiento del perfil, arrástrelo y suéltelo sobre el objeto *Test de Aplicaciones Públicas*, o bien active la función de prueba vía la barra de menú del editor. El perfil definido se activará y reconstruirá la carpeta de *Aplicaciones públicas*. Si dicho test se realiza desde el editor, el contenido de la lista de aplicaciones públicas definidas en el controlador de dominio se refrescará. En otro caso, usted deberá seleccionar la opción Refrescar del menú desplegable asociado a la opción Dominio de la barra de menú del editor.

Una vez configurado, asocie el perfil al usuario o grupo deseado, arrastrándolo y soltándolo sobre el contenedor adecuado de la herramienta de administración de usuarios y/o grupos, o bien establezca el mismo como defecto de máquina, copiándolo con su nombre por defecto (EDYROAM.INI) en la carpeta *NOUSER*.

Cuando un usuario realize una conexión, se activará el perfil que tenga asociado, ya sea el suyo propio o el del grupo SecureEntry al que pertenezca en caso de no tenerlo. Si el usuario no tiene ningún perfil de aplicaciones públicas asociado, entonces se activará el perfil que pudiera haber en la carpeta *NOUSER*. Si en la carpeta *NOUSER* tampoco existe un perfil de aplicaciones públicas para la máquina, entonces el conjunto de aplicaciones públicas que pudiera tener asignado el usuario se preservará.

Debe usted tener presente que cuando se realice una conexión SecureEntry de invitado, dicha conexión **no** conllevará la activación del perfil EDYROAM.INI de la carpeta *NOUSER*, en caso de existir.

Descripción de los módulos y API

Los nombres de este componente incluyen la palabra *ROAM*, del concepto inglés *Roaming Desktop*, que significa literalmente *Escritorio Itinerante*, puesto que el conjunto de definiciones de aplicaciones públicas asignadas a un usuario o grupo de usuarios viajan a la estación de trabajo en la que el usuario realiza una conexión. Esto es especialmente significativo en entornos corporativos, donde la gestión de usuarios está centralizada vía UCM.

A continuación se describen los módulos que se integran en este componente:

EDYROAME

Este es el programa editor de perfiles. Tiene la siguiente sintaxis:

```
EDYROAME.EXE [Perfil]
```

Donde *Perfil* es la vía de acceso y nombre de archivo del perfil deseado. El editor permite probar un perfil directamente.

EDYROAMT

Este es el programa activador de perfiles. Tiene la siguiente sintaxis:

```
EDYROAMT.EXE /F[Perfil] [/T]
```

/F*Perfil* activa el escritorio itinerante descrito en *Perfil*. Si *Perfil* no existe, el conjunto de aplicaciones públicas actuales del usuario será preservado.

/F activa el escritorio itinerante EDYROAM.INI descrito en *NOUSER*. Si dicho perfil no existe, el conjunto de aplicaciones públicas actuales del usuario será preservado.

/T indica que el escritorio itinerante debe ser activado en modo de prueba. Este parámetro restaura en el usuario el conjunto de las aplicaciones públicas que tuviera antes de realizar el test.

Interfície del componente de aplicaciones públicas

El componente exporta la siguiente rutina, tal como se define en *EDYROAM.H*. La rutina se ejecuta correctamente si devuelve cero; en caso contrario devuelve el error obtenido:

```
APIRET _System SetRoamingDesktop(PSZ  pszFileName,  BOOL Testing);
```

Activa el escritorio itinerante descrito en pszFileName. Si el contenido de pszFileName está vacío, entonces se borran todas las aplicaciones públicas que pueda tener asignadas el usuario.

Si pszFileName apunta a "", entonces se activará el escritorio itinerante de NOUSER.

Si el fichero no existe, entonces se preservan las aplicaciones públicas que pueda tener asignadas el usuario.

El parámetro Testing debe indicar si se está haciendo una conexión real (FALSE) o si, por el contrario, se está haciendo un test (TRUE).

El archivo de Anotaciones Cronológicas

El archivo de Anotaciones Cronológicas tiene por nombre EDYROAM.LOG y reside en la vía de acceso dada por la variable de entorno SGM_ROAM_LOGPATH. Este archivo contiene los errores y avisos encontrados por el componente durante su ejecución.

```
   Date      Time     Program    Severity   Error           Explanation
---------- -------- ------------ -------- ---------- -------------------------
29/09/1998 16:03:01  EDYROAME.EXE  ERROR    0X0000000D Could not determine  logon domain.
                                                      Probably there's no user logged on.
29/09/1998 16:04:23  EDYROAME.EXE  WARNING  0X00000000  NetServerEnum2 returned 0 entries.
                                                      Retrying with   NetGetDCName.
29/09/1998 16:05:48  EDYROAME.EXE  ERROR    0X00000015  DosQueryPathInfo:  could not get
                                                      file information about   "A:\NOALIAS.INI".
29/09/1998 16:06:32  EDYROAME.EXE  ERROR    0X00000ADF  NetAliasGetInfo:  the alias  "ARBRE"
                                                      is not defined in the Domain Controller.
```

Este ejemplo muestra que el editor de aplicaciones públicas obtuvo tres errores y un aviso durante su ejecución.

El primer error señala que no se pudo determinar el dominio al que se hizo la conexión y propone como posible causa el hecho de que probablemente se realizó una desconexión no SecureEntry desde la sesión de trabajo. Se devolvió al editor el error de OS/2 0X0000000D, que significa que *Los datos son inválidos*.

El único aviso que hay señala que una API de LAN Server devolvió un error y que se utilizó otra API de LAN Server alternativa. Al tratarse de un aviso, no se devolvió ningún error al editor de aplicaciones públicas.

Recuerde que se puede controlar el tamaño de los archivos de anotaciones de SecureEntry, así como cualquier otro archivo ASCII, utilizando la utilidad EDYLOGFS.

Consideraciones en entornos de WorkSpace On-Demand

Como con cualquier componente de SecureEntry, usted puede administrar el conjunto de aplicaciones públicas a asignar a un usuario o grupo desde cualquier estación de trabajo. No obstante, si está usted administrando o probando aplicaciones públicas con parámetros desde una estación de trabajo **no** administradora de WorkSpace On-Demand, entonces la actualización de los parámetros de las aplicaciones públicas **no** podrá realizarse correctamente en la máquina servidora de WorkSpace On-Demand si no hay un usuario administrador conectado en ella.

La mejor recomendación es que administre desde la propia estación definida como Cliente Administrador de WorkSpace On-Demand, o desde el Servidor WorkSpace On-Demand -si se instalaron en él las herramientas de administración de LAN Server-, en caso de que deba usted administrar aplicaciones públicas con parámetros.

En el caso de que un usuario, ya sea administrador o no, que tenga asignado un conjunto de aplicaciones públicas con parámetros realize una conexión desde una estación de trabajo **no** WorkSpace On-Demand, la posible actualización de los parámetros de las aplicaciones públicas **tampoco** podrá realizarse correctamente en la máquina servidora WorkSpace On-Demand si no hay un usuario administrador conectado en ella.

Note usted que, en este caso, la carpeta de aplicaciones públicas asignadas al usuario seguirá conteniendo las aplicaciones asignadas, puesto que en dichas estaciones de trabajo los parámetros de las aplicaciones públicas no tienen sentido.

Parámetros específicos de WorkSpace On-Demand para aplicaciones públicas

A continuación se describen los parámetros específicos de WorkSpace On-Demand que pueden serle útiles a la hora de configurar aplicaciones públicas:

WSOD_LAUNCH_MINIMIZED. Asigne a esta variable de entorno el valor 1 para que la aplicación se arranque minimizada.

WSOD_LAUNCH_NOCLOSE. Asigne a esta variable de entorno el valor 1 para que la ventana DOS o OS/2 VIO no se cierre cuando la aplicación termine. Esta opción puede ser útil a la hora de determinar la causa de un problema con la definición de la aplicación.

WSOD_LAUNCH_SESSION. Este parámetro proporciona al administrador control absoluto acerca del tipo de sesión en que WorkSpace On-Demand lanzará la aplicación. La aplicación puede no funcionar correctamente si usted escoge un tipo erróneo. Estos son los valores que puede tomar esta variable de entorno:

1. Pantalla completa de OS/2
2. Ventana de OS/2
3. PM de OS/2
4. Pantalla completa de DOS
7. Ventana de DOS
10. WinOS2 en modo real
12. WinOS2 en modo automático
15. WinOS2 estándar, transparente (seamless), VDM separada
16. WinOS2 estándar, transparente (seamless), VDM común
17. WinOS2 mejorado, transparente (seamless), VDM separada
18. WinOS2 mejorado, transparente (seamless), VDM común
19. WinOS2 mejorado, pantalla completa
20. WinOS2 estándar, pantalla completa

WSOD_LAUNCH_NODROP. Asigne a esta variable de entorno el valor 1 para que la aplicación se arranque sin desconectarse de los recursos de red en curso.

NCC_SETUP_POST. Esta variable de entorno permite asignar cadenas de inicialización a la aplicación. El valor de este parámetro puede consistir en cualquiera de las cadenas de inicialización especificadas más abajo. Cada cadena consiste de un nombre de llave, inmediatamente seguido por el

signo igual ('=') y un valor. Se pueden asignar distintas cadenas de inicialización separándolas por un punto y coma (';'). A continuación se detallan los nombres de las llaves más usadas:

CCVIEW. Puede tomar los valores *DEFAULT*, *YES* o *NO*.

ICONFILE. Debe tomar como valor el archivo que establece el icono del objeto.

ICONPOS. Debe tomar como valor el par de coordenadas (x,y), en tanto por ciento, sobre las que debe residir el objeto en el escritorio inicialmente.

ICONRESOURCE. Debe tomar como valor el par (id,módulo) que designa el identificador del recurso y el módulo que contienen el icono del objeto.

Por ejemplo, para hacer que el objeto aparezca inicialmente a un diez por ciento desde el inicio de las coordenadas asigne a la variable **NCC_SETUP_POST** el siguiente valor:

```
ICONPOS=10,10;
```

Si está usted configurando aplicaciones públicas que deban ejecutarse en clientes de WorkSpace On-Demand 2.0, puede usted disponer además de los siguientes parámetros:

NCC_PREFITS. Asigne a esta variable un nombre de archivo FIT. Las entradas contenidas en este archivo FIT se anteponen a las entradas por defecto del archivo FIT del usuario conectado. Utilice este archivo para forzar que las entradas del archivo FIT se coloquen antes que otras entradas similares en el archivo FIT por defecto del usuario, o para añadir nuevas entradas en el archivo FIT.

NCC_POSTFITS. Asigne a esta variable un nombre de archivo FIT. Las entradas contenidas en este archivo FIT se añaden por el final a las entradas por defecto del archivo FIT del usuario conectado. Utilice este archivo para forzar que las entradas del archivo FIT se coloquen después de otras entradas similares en el archivo FIT por defecto del usuario, o para añadir nuevas entradas en el archivo FIT.

NCC_FOLDER. Esta variable de entorno permite proporcionar cadenas de inicialización a la aplicación. Utilice este parámetro para situar un objeto programa dentro de una carpeta del escritorio. Usted puede utilizar cualquier cadena de inicialización de objetos WPFolder y WPObject. Por ejemplo, para hacer que la aplicación resida dentro de la carpeta *Directores*, asigne el siguiente valor valor a la variable **NCC_FOLDER** :

```
NCC_FOLDER=TITLE=Directores;
```

Como WorkSpace On-Demand 2.0 soporta carpetas multinivel, usted puede usar la cadena de inicialización **NCC_CHILD_SETUP**, que es parte del parámetro **NCC_FOLDER**, para especificar la carpeta hija. Por ejemplo, si **NCC_FOLDER** contuviera la siguiente cadena de inicialización:

```
NCC_FOLDER=TITLE=Secretarias;NCC_CHILD_SETUP=BOOKKEEP;
```

y otro parámetro BOOKKEEP también existiera y contuviera el siguiente valor:

```
BOOKKEEP=TITLE=Librería;
```

entonces en el Escritorio se crearía una carpeta llamada *Secretarias*, en la carpeta *Secretarias* se crearía otra carpeta de nombre *Librería*, y el objeto programa para la aplicación se crearía en la carpeta *Librería*.

Para obtener más información acerca de los parámetros de WorkSpace On-Demand para aplicaciones públicas, remítase a las publicaciones *WorkSpace On-Demand HandBook* y *WorkSpace On-Demand Administrator's Guide*.

Para obtener más información acerca de las cadenas de inicialización, remítase a la publicación *Workplace Shell Programming Reference*.

IDs de Objetos de Aplicaciones Públicas

En entornos de LAN Server convencionales, las aplicaciones públicas asignadas a un usuario residen en la carpeta *Aplicaciones públicas* Esta carpeta tiene asignado el ID de objeto **<\NETAPPS\NETAPPFLDR>**. Cada objeto programa dentro de esta carpeta se crea con el ID de objeto *<\NombreServidor\IdAplicación>*, donde *NombreServidor* es el nombre del servidor del dominio al que el usuario se ha conectado, y *IdAplicación* es el identificador con el que se creó la aplicación pública.

En entornos de WorkSpace On-Demand, cada objeto programa asociado a una aplicación pública que aparece en el escritorio del usuario tiene por ID de objeto **<NCID_***IdAplicación***>**, donde *IdAplicación* es el identificador con el que se creó la aplicación pública.

Remítase a Acerca de los IDs de los Objetos para obtener más información relativa a los IDs de los objetos.

Administración de usuarios y grupos

Herramienta de administración interactiva

La herramienta interactiva de administración de usuarios y grupos permite, de un modo sencillo, definir y modificar los usuarios, grupos y recursos SecureEntry, así como los perfiles de seguridad y personalización asociados.

Para lanzar la herramienta, utilice el objeto *Administración de usuarios y grupos* que se encuentra en la carpeta *SecureEntry: Herramientas de administración*. Si desea hacerlo manualmente, por línea de comandos, entre :

```
EDYSNADM
```

Las páginas siguientes describen brevemente la idea general de trabajo con esta aplicación. Para obtener información más detallada acerca de la misma, consulte la ayuda en línea disponible desde la misma.

Para empezar, hay una serie de observaciones previas a tener en cuenta :

Los diálogos y paneles que se refieren a características específicas Lan Server tan solo serán accesibles en máquinas con configuración SecureEntry de tipo Lan Server.

Siendo el aspecto común e independiente de la aplicación, existen ciertas diferencias operativas cuando se trabaja en entornos Lan Server frente a monoestación :

Vd. podrá solamente asignar componentes de seguridad a grupos SecureEntry, es decir, a aquellos grupos cuyos dos primeros carácteres sean 'SG'.

No se podrán definir usuarios que no pertenezcan a ningún grupo. Tenga en cuenta que como mínimo, un usuario debe pertenecer al grupo 'USERS', 'ADMINS' o 'GUESTS' en Lan Server.

No podrá definir grupos que pertenezcan a otros grupos (subgrupos). Sin embargo, en entornos Lan Server vd. podrá definir usuarios que pertenezcan a más de un grupo.

Diálogos de la aplicación

Diálogo inicial

Este diálogo muestra los grupos de usuarios principales definidos en la base de datos de usuarios y grupos, así como aquellos usuarios que no pertenecen a ningún grupo. Puede vd. consultar la información detallada de un grupo o usuario haciendo doble click sobre el icono que lo representa.

Vd. puede también ver, añadir o borrar usuarios o grupos seleccionando el grupo/usuario apropiado, y pulsando el botón correspondiente.

Para añadir un nuevo usuario dentro de un grupo, abra primero la vista del grupo (doble-click sobre su icono), y añada entonces el usuario desde el diálogo de información del grupo. Observe que, en caso de utilizar UCM, deberá vd. proveer un identificador de oficina asociado a los nuevos usuarios que defina, además de la información común solicitada.

Hay también un **menú de operaciones** que le permite, entre otras cosas, buscar usuarios directamente dado su identificador.

En el **menú de opciones** de este diálogo, podrá vd. habilitar el nivel de información de los mensajes de aviso mostrados por la aplicación.

El **botón de funciones Lan Server (*LS*)**, que se mostrará solamente en entornos IBM Lan Server, le mostrará el diálogo de definición de recursos :

En este panel vd. puede definir recursos Lan Server asociados a un nombre de alias, los cuales podrá vd. asignar a sus usuarios y/o grupos. Consulte la información IBM Lan Server apropiada para conocer el significado de los diferentes campos requeridos. En cualquier caso, SecureEntry provee las siguientes extensiones semánticas :

Si vd. no proporciona ningún nombre de servidor para un alias determinado, SecureEntry utilizará el nombre de servidor del controlador de dominio de su red para dar de alta el recurso en Lan Server. Esta característica es especialmente útil para trabajar con UCM.

Vd. puede arrastrar y soltar definiciones de alias desde/hasta el contenedor de definición de recursos. Una definición de alias es un archivo texto en formato compatible con la *herramienta de administración batch*. De este modo podrá vd. utilizar la aplicación como herramienta para crear sus archivos de administración desatendida (batch).

Además y si utiliza UCM, vd. dispondrá del **menú de UCM** donde podrá definir las características de refresco de oficinas de su corporación. Al seleccionar este menú vd. dispondrá de tres de opciones que se detallan a continuación:

Datos de Oficina

Mediante esta opción de menú vd. podrá consultar el nombre de oficina por el cual es conocida la estación administradora en la Base de Datos de UCM, el nivel de imagen de oficina en el que se encuentra el UCM, el nivel de oficina local en el que se encuentra la Base de Datos de SecureEntry en la estación administradora y si se produjo algún error en la última operación de refresco dinámico de datos. En el caso de que usted no tenga activa la política de refresco dinámico, esta pantalla no contendrá datos y se le reportará un error.

Política de Refresco

Mediante esta opción vd. podrá gestionar la política de refresco corporativa almacenada en la Base de Datos de UCM, el número de oficinas a partir del cual desea que se active la eliminación de cambios producidos sobre la Base de Datos de UCM y que ya han sido distribuidos a todas las oficinas, así como consultar la política de refresco activa que tiene usted configurada en la máquina administradora (que puede diferir de la almacenada en la Base de Datos de UCM).

Actividad de Anotación

Mediante esta opción vd. podrá activar la facilidad de anotación de operaciones de UCM. En el caso de ser activada, vd. tendrá de gestionar la eliminación de las filas que se generarán en la tabla de anotaciones de UCM a través de la herramienta EDYEXLOG tal y como se detalla en la Guía de Administración de UCM.

Diálogo de definición de grupos

En este diálogo, vd. puede modificar la definición de un grupo añadiendo nuevos usuarios o subgrupos (en entornos monoestación), o asignando perfiles de seguridad y personalización para el grupo. Hay también un campo de descripción disponible para poder definir el grupo.

Vd. puede ver, añadir o borrar usuarios o grupos seleccionando el grupo/usuario apropiado, y pulsando el botón correspondiente.

Para asociar un perfil de seguridad y personalización SecureEntry con el grupo, arrástrelo y suéltelo sobre el contenedor de componentes de seguridad inferior. El perfil será copiado en la base de datos de usuarios y grupos, y se activará cuando un usuario perteneciente al grupo se conecte.

Puede vd. también editar directamente un perfil de seguridad ya asociado a un grupo haciendo doble-click sobre el icono que lo representa en el contenedor.

El botón de funciones Lan Server (*LS*), que se mostrará solamente en entornos IBM Lan Server, le mostrará el diálogo de definición de recursos para el grupo :

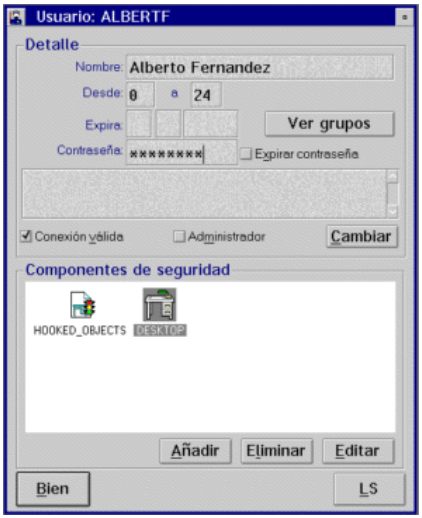
En este panel vd. puede definir los alias Lan Server asociados al grupo. Consulte la información IBM Lan Server apropiada para conocer el significado de los diferentes campos requeridos. En cualquier caso, SecureEntry provee las siguientes extensiones semánticas :

IBM Lan Server no soporta directamente las asignaciones de recursos en conexión para grupos. SecureEntry provee esta funcionalidad. Esto implica que cuando vd. use las herramientas de administración Lan Server directamente, no podrá ver estas asignaciones.

Asegúrese de que los recursos definidos estén disponibles en tiempo de administración, o no podrá ver sus definiciones y/o asociaciones.

Vd. puede arrastrar y soltar asociaciones de alias a grupos desde/hasta el contenedor de definición de recursos. Una asociación de alias es un archivo texto en formato compatible con la *herramienta de administración batch*. De este modo podrá vd. utilizar la aplicación como herramienta para crear sus archivos de administración desatendida (batch).

Diálogo de definición de usuarios



Este diálogo es muy similar al de definición de grupos, y permite definir y modificar los datos específicos de un usuario en particular, así como asignar y editar los perfiles de seguridad y personalización asociados específicamente al mismo.

Para asociar un perfil de seguridad y personalización SecureEntry con el usuario, arrástrelo y suéltelo sobre el contenedor de componentes de seguridad inferior. El perfil será copiado en la base de datos de usuarios y grupos, y se activará cuando el usuario se conecte.

Puede vd. también editar directamente un perfil de seguridad ya asociado a un usuario haciendo doble-click sobre el icono que lo representa en el contenedor.

El botón de funciones Lan Server (*LS*), que se mostrará solamente en entornos IBM Lan Server, le mostrará el diálogo de definición de recursos para el usuario :

En este panel vd. puede definir los alias Lan Server asociados al usuario. Consulte la información IBM Lan Server apropiada para conocer el significado de los diferentes campos requeridos. En cualquier caso, SecureEntry provee las siguientes extensiones semánticas :

SecureEntry amplía la sintaxis de especificación del directorio personal, de tal modo que :

Vd. puede dejar el nombre de servidor en blanco. Se utilizará el nombre de servidor del controlador de dominio.

SecureEntry ampliará automáticamente los derechos de acceso al directorio personal a los subdirectorios contenidos.

SecureEntry intentará crear el directorio al conectarse el usuario, si no existiese.

Estas características son especialmente importantes cuando se trabaja con administración centralizada (UCM). Por tanto, la sintaxis para especificar el directorio personal queda como sigue :

x:\[*NombreMáquina*]*y*$*vía*

o

\\[*NombreMáquina*]*y*$*vía*

donde :

x es el identificador de unidad asignado en tiempo de conexión al directorio personal para el usuario.

NombreMáquina es el nombre de servidor de la máquina donde reside físicamente el recurso, que vd. puede omitir para indicar el controlador de dominio en curso.

y es la unidad en el servidor donde reside el recurso.

vía es la vía de acceso en el servidor al recurso.

Asegúrese de que los recursos definidos estén disponibles en tiempo de administración, o no podrá ver sus definiciones y/o asociaciones.

Vd. puede arrastrar y soltar asociaciones de alias a usuarios desde/hasta el contenedor de definición de recursos. Una asociación de alias es un archivo texto en formato compatible con la *herramienta de*

administración batch. De este modo podrá vd. utilizar la aplicación como herramienta para crear sus archivos de administración desatendida (batch).

Privilegios de administración

Usted puede definir restricciones sobre las operaciones básicas de administración definiendo la variable de entorno **SGM_ADM_PRIV**. La aplicación de administración interactiva aplicará estas restricciones deshabilitando automáticamente los controles que den acceso a las operaciones sobre las que no se tengan permisos suficientes. De hecho, aunque en algún caso se permita invocar una operación inedependientemente de los permisos establecidos, el usuario nunca podrá completarla si no tiene permisos suficientes, y se le advertirá de ello mediante una mensaje de error.

Por ejemplo, si para una máquina determinada define SGM_ADM_PRIV = 0xFFFF555F, entonces desde esa máquina se podrán modificar todos los grupos,usuarios y recursos ya existentes, pero no se podrán añadir nuevos objetos ni borrar los que ya existan.
Nota: para poder usar la administración interactiva de grupos y usuarios, los siguientes derechos deben estar habilitados

EDYUCM_PRIVILEGE_SUB_VIEW

EDYUCM_PRIVILEGE_USER_GRP_VIEW

EDYUCM_PRIVILEGE_GRP_GRP_VIEW

Exits de Usuario

Usted puede instalar exits de usuario para la herramienta interactiva de administración (válidas sólo para esta herramienta) completando el fichero **EDYADMUS.CMD** y copiándolo al subdirectorio EXEC de su directorio de SecureEntry. Vd. encontrará un archivo ejemplo en el subdirectorio API\SOURCES\EDYADMUS. Como puede verse al editar el mismo, se soportan las siguientes exits de usuario:

UserExitBeforeADD_USER

Se llama justo antes de añadir un usuario

UserExitBeforeADD_USERGROUP

Se llama justo antes de relacionar un usuario con un grupo

UserExitBeforeADD_GROUP

Se llama justo antes de añadir un grupo

UserExitBeforeADD_GROUPGROUP

Se llama justo antes de relacionar un grupo con otro grupo

UserExitBeforeADD_RESOURCE

Se llama justo antes de añadir un recurso

UserExitBeforeADD_RESOURCEUSER

Se llama justo antes de relacionar un recurso con un usuario

UserExitBeforeADD_RESOURCEGROUP

Se llama justo antes de relacionar un recurso con un grupo

UserExitBeforeADD_SUBSYSTEM

Se llama justo antes de añadir un subsistema

UserExitBeforeUPDATE_USER

Se llama justo antes de actualizar los datos de un usuario

UserExitBeforeUPDATE_USERGROUP

Se llama justo antes de actualizar los datos de una relación usuario-grupo

UserExitBeforeUPDATE_GROUP

Se llama justo antes de actualizar los datos de un grupo.

UserExitBeforeUPDATE_GROUPGROUP

Se llama justo antes de actualizar los datos de una relación grupo-grupo

UserExitBeforeUPDATE_RESOURCE

Se llama justo antes de actualizar los datos de un recurso

UserExitBeforeUPDATE_RESOURCEGROUP

Se llama justo antes de actualizar los datos de una relación recurso-grupo

UserExitBeforeUPDATE_RESOURCEUSER

Se llama justo antes de actualizar los datos de una relación recurso-usuario

UserExitBeforeUPDATE_SUBSYSTEM

Se llama justo antes de actualizar los datos de un subsistema

UserExitBeforeDELETE_USER

Se llama justo antes de borrar un usuario

UserExitBeforeDELETE_USERGROUP

Se llama justo antes de borrar una relación usuario-grupo

UserExitBeforeDELETE_GROUP

Se llama justo antes de borrar un grupo

UserExitBeforeDELETE_GROUPGROUP

Se llama justo antes de borrar una relación grupo-grupo

UserExitBeforeDELETE_RESOURCE

Se llama justo antes de borrar un recurso

UserExitBeforeDELETE_RESOURCEUSER

Se llama justo antes de borrar una relación recurso-usuario

UserExitBeforeDELETE_RESOURCEGROUP

Se llama justo antes de borrar una relación recurso-grupo

UserExitBeforeDELETE_SUBSYSTEM

Se llama justo antes de borrar un subsistema

Estas exits de usuario le permiten insertar código para que sea ejecutado justo antes de llamar a cada operación soportada, pudiendo cancelar la operación y/o cambiar cualquiera de sus parámetros.

Edite el fichero edyadmus.cmd para saber más sobre los detalles de implementación relevantes para escribir sus exits de usuario de administración.

Herramientas de administración batch

SecureEntry provee de varias herramientas para la administración batch de la base de datos de usuarios y grupos que se explican en este capítulo.

EDYDEFS es un programa que permite añadir, modificar o borrar definiciones en la base de datos, a partir de un archivo de descripción de tarea. Esta herramienta dispone además de un objeto que la representa : *Administración de usuarios y grupos (no interactiva)* que se encuentra en la carpeta *SecureEntry: Herramientas de administración*.

EDYERASE es un programa que permite hacer un borrado selectivo de todas o algunas de las definiciones de la base de datos, según ciertos criterios.

EDYDUMP le permite volcar todas o parte de las definiciones actuales sobre un archivo de texto, en formato compatible con *EDYDEFS*.

EDYADMIN es una utilidad de administración genérica que le puede ser útil para escribir sus propios programas de administración, ya que mapea completamente la interfície de administración.

Todas estas herramientas se encuentran en la vía de acceso SecureEntry, subdirectorio EXEC, y requieren privilegios de administrador para poder ser ejecutadas satisfactoriamente.

EDYDEFS : La herramienta de proceso de archivos de definición

La herramienta batch de administración de usuarios y grupos permite realizar la administración de usuarios, grupos, recursos y perfiles de seguridad SecureEntry de un modo desatendido, tomando como entrada un archivo de definiciones a procesar.

La sintaxis del comando es como sigue :

```
  EDYDEFS Help | ([/]usuario [[/]clave:p] [[/]File:f] [[/]Action:a]
         [[/Trace] [[/]Warn] [[/]Ignore'

  Usuario y clave : Ignorados. Esta herramienta solamente puede ser usada
 por usuarios que se hayan conectado con privilegios de administrador.
  File   : Nombre del archivo de definiciones. Por defecto se busca EDYDEFS.TXT
  Action : Acción a ejecutar con los registros. Por defecto es ADD (Añadir). Los
                valores permitidos son ADD (Añadir), UPDATE (Modificar), DELETE
(Borrar)
  Trace  : Activa la presentación de rastro de las llamadas por pantalla
  Warn   : Solamente verificar sintácticamente el archivo. No procesar las
                llamadas a la API
  Ignore : Procesar todo el archivo ignorando posibles errores
```

La mejor forma de mostrar el formato de los archivos de definiciones es a través de dos ejemplos :

Archivo de definiciones para entornos monopuesto.

```
// ********************************************************************
// * Ejemplo de archivo de definiciones monopuesto para administración *
// ********************************************************************

[ACTION=ADD]                        //  Acciones permitidas son ADD, UPDATE
                                    // y DELETE.  Esta palabra clave establece
                                    // la  acción hasta que se especifique otra
// Definamos un grupo de cajeros

[GROUP=CAJEROS]
  FULL_NAME=Grupo de cajeros
  DESCRIPTION=Grupo para cajeros
  DESKTOP=EDYDESK.INI               //  Cualquier componente estándar SecureEntry
  LAUNCHPAD=SELP.INI                //  ,  p.e : DESKTOP,  PERS_DESKTOP,  LAUNCHPAD
  FLOPPY_DISK=FPY.INI               //  SYSTEM_MENUS,  FLOPPY_DISK,  TREE_LOCK,
                                    //  SES_BEHAVIOUR,  ....
// Definamos dos usuarios
[USER=PEPE]
  GROUP=CAJEROS                     //  Grupo debe existir al añadir el usuario
  PRIV_USER=USER                    // Solo  valores : USER o ADMIN
  FULL_NAME=Pepito de los palotes
  DESCRIPTION=Un usuario
  USER_EXPIRE=NEVER                 // NEVER  (nunca) o dd-mm-yyyy : fecha expiración
  CONNECTION=1                      // 1=>  Conexión permitida 0=> No permitida
  HOUR_START=8                      // Hora  inicio de conexión.
  HOUR_END=20                       // Hora  límite de conexión.
  PASSWORD=password                 // 'password'  es la clave de acceso por defecto
  LAUNCHPAD=SELP.INI                //  Cualquier componente estándar SecureEntry
  FLOPPY_DISK=FPY.INI               //  ,  p.e : DESKTOP,  PERS_DESKTOP,  LAUNCHPAD
                                    //  SYSTEM_MENUS,  FLOPPY_DISK,  TREE_LOCK,
[USER=MIGUEL]                       //  SES_BEHAVIOUR,  ....
  GROUP=CAJEROS
  PRIV_USER=USER
  FULL_NAME=Miguel Indurain
  DESCRIPTION=Ciclista
  USER_EXPIRE=NEVER
  CONNECTION=1
  HOUR_START=8
  HOUR_END=20

// Ahora definamos un grupo para dirección y dos usuarios

[GROUP=DIRECTOR]
  FULL_NAME=Grupo dirección         // El resto de palabras reservadas tomarán
                                    //  valores por defecto

[USER=ANDRES]
  GROUP=DIRECTOR
  PRIV_USER=USER                    //  Podríamos usar GROUP_LS en vez de
  FULL_NAME=Andrés Perez            //  PRIV_USER con el mismo significado
  DESCRIPTION=Un director
  USER_EXPIRE=1-1-1999
  CONNECTION=1
  HOUR_START=8
  HOUR_END=20

// Ahora modificamos Miguel añadiendole un launchpad, y le promocionamos a director..

[ACTION=UPDATE]                     // A  partir de ahora, modificar...

[USER=MIGUEL]
  GROUP=DIRECTOR                    //  Nuevo grupo
  LAUNCHPAD=SELP.INI                //  Nuevo componente

// Borremos ahora el launchpad recién añadido

[ACTION=DELETE]                     // A  partir de ahora, borrar
```

```
[USER=MIGUEL]                       // No  es un borrado de usuario, pues damos
  LAUNCHPAD                         //  palabras clave.Solo borrar de componente.

// Ahora borremos completamente  las definiciones hechas

[USER=MIGUEL]                       //  Borrado completo de usuario
[USER=ANDRES]
[USER=PEPE]
[GROUP=CAJEROS]                     //  Borrado de grupo (debe estar vacío)
[GROUP=DIRECTOR]
```

Archivo de definiciones para entornos Lan Server.

```
// ********************************************************************
// * Ejemplo de archivo de definiciones Lan Server para administración *
// ********************************************************************

[ACTION=ADD]                        //  Acciones permitidas son ADD, UPDATE
                                    // y DELETE.  Esta palabra clave establece
                                    // la  acción hasta que se especifique otra

// Definamos un recurso asociado a un alias

[ALIAS=TSTALIAS]
  TYPE=FILES                        //  Tipo de recurso.
                                    //  'FILES'  (directorio de red),
                                    //  'TREE' (dir. de red  c/subdirectorios),
                                    //  'SERIAL'  (puerto serie),
                                    //  'PRINTER'  (impresora)
                                    //  para el alias especificado
  NETNAME=C:\MAR\SGMSHELL           // Vía de acceso en la red
                                    // Se  puede usar RESNAME en su lugar
  SERVER=SERVER1                    // El  servidor donde reside sin '\\'
  WHEN_SHARED=STARTUP               //  Cuando se compartirá
                                    //  STARTUP (en  arranque),
                                    //   BYADMIN (por administrador),  o
                                    //  DYNAMIC  (dinámicamente)
  DESCRIPTION=Ejemplo  de alias     //  Descripción del alias
  MAX_CONN=45                       // Max.  número de conexiones

// Definamos un grupo de cajeros

[GROUP=SGCAJERO]                    //  Recuerde que los grupos SecureEntry deben
                                    //  empezar por 'SG'
  FULL_NAME=Grupo  cajeros          //  Ignorado en entornos Lan Server
  DESCRIPTION=Group para cajeros    //  Descripción del grupo
  ACCESS_FILE=ACCESS.DAT            //  'vieja forma' de definir accesos
                                    //  Ejemplo de ACCESS.DAT (archivo de accesos)
                                    //  ****************************************
                                    //  *[ALIAS=TSTALIAS]//  nombre alias          *
                                    // *   ACCESS=RWX    // privilegios            *
                                    // *   LOGON_ASN=J:  // asignación en conexión *
                                    //  ****************************************
                                    // Observe que  aunque defina acceso a modificar,
                                    //  este será creado de nuevo, por lo que se debe
                                    //  especificar completamente aquí :
                                    //  el nombre de alias,  los derechos de acceso y
                                    // la  asignación en conexión.
  ACCESS=TSTALIAS,RWX,J             //  'nueva forma' de definir accesos, completamente.
                                    // en  el archivo de definición.
                                    // Observe que  aunque defina un acceso a modificar,
                                    //  este será creado de nuevo, por lo que se debe
                                    //  especificar completamente aquí :
                                    //  ACCESS=nombrealias,derechos,asn_conexión.
  DESKTOP=EDYDESK.INI               //  Cualquier componente estándar SecureEntry
  LAUNCHPAD=SELP.INI                //  ,  p.e : DESKTOP,  PERS_DESKTOP,  LAUNCHPAD
```

```
  FLOPPY_DISK=FPY.INI                // SYSTEM_MENUS, FLOPPY_DISK, TREE_LOCK,
                                     //  SES_BEHAVIOUR, ....
// Ahora definamos dos usuarios

[USER=PEPE]
  BRANCH=BRANCH01                    // Observe que  esta palabra clave es válida y
                                     //  obligatoria solo en entornos UCM.
  GROUP=SGCAJERO                     // El grupo debe existir al añadir usuarios
  PRIV_USER=USER                     // Solo  valores : USER o ADMIN
  FULL_NAME=Pepito de los palotes    // Nombre completo
  DESCRIPTION=Un usuario             // Descripción
  USER_EXPIRE=NEVER                  // NEVER (nunca) o dd-mm-yyyy (usuario expira el..)
  CONNECTION=1                       // 1=> Conexión permitida 0=> No permitida
  HOUR_START=8                       // Hora inicio conexión válida
  HOUR_END=20                        // Hora final de  conexión permitida
  PASSWORD=password                  // 'password'  es la clave de conexión por defecto
  LAUNCHPAD=SELP.INI                 // Cualquier componente estándar SecureEntry
  FLOPPY_DISK=FPY.INI                // , p.e : DESKTOP, PERS_DESKTOP, LAUNCHPAD
                                     //  SYSTEM_MENUS, FLOPPY_DISK, TREE_LOCK,
                                     //  SES_BEHAVIOUR, ....

  // Estas son palabras reservadas específicas Lan Server

  HOME_DIR=X:\\c$\HOME\PEPE          // El directorio personal Lan Server para el
usuario
                                     //  Sintaxis :
                                     //      \\NombreMáquina\x$\vía,  o
                                     //     x:\NombreMáquina\x$\vía
                                     // Sin  NombreMáquina ==> usar controlador de
dominio
  MAX_STORAGE=2048000                //  Por defecto es -1 (sin límite)
  SCRIPT_PATH=C:\SCRIPTS             //  Archivo de arranque Lan server
  ACCESS_FILE=ACCESS.DAT             //  'vieja forma' de definir accesos
                                     //  Ejemplo de ACCESS.DAT (archivo de accesos)
                                     //  ********************************************
                                     // *  [ALIAS=TSTALIAS]  // nombre alias          *
                                     // *    ACCESS=RWX      // privilegios            *
                                     // *    LOGON_ASN=J:    // asignación en conexión *
                                     //  ********************************************
                                     // Observe que  aunque defina un acceso a modificar,
                                     //  este será creado de nuevo, por lo que se debe
                                     //  especificar completamente aquí :
                                     //  el nombre de alias,  los derechos de acceso y
                                     // la  asignación en conexión.
  ACCESS=TSTALIAS,RWX,J:             //  'nueva forma' de definir accesos, completamente.
                                     // en  el archivo de definición.
                                     // Observe que  aunque defina un acceso a modificar,
                                     //  este será creado de nuevo, por lo que se debe
                                     //  especificar completamente aquí :
                                     //  ACCESS=nombrealias,derechos,asn_conexión.
                                     //  Derechos permitidos :
                                     // D  (Borrar) A (Atributos) X (Ejecutar)
                                     // R (Leer) W  (Escribir) P (Permisos) N (Ninguno)
[USER=MIGUEL]
  GROUP=SGCAJERO
  PRIV_USER=USER
  FULL_NAME=Miguel Indurain
  DESCRIPTION=Ciclista
  USER_EXPIRE=NEVER
  CONNECTION=1
  HOUR_START=8
  HOUR_END=20

// Ahora grupo para directores y un usuario

[GROUP=SGDIRECT]
  DESCRIPTION=Grupo de directores    // El resto de palabras reservadas tomará
                                     //  valores por defecto
```

```
[USER=ANDRES]
  GROUP=SGDIRECT,OTROGRUP           // LAN Server  permite más de un grupo
                                    //  Especificar todos los grupos•3;!
  PRIV_USER=USER                    //  Podríamos haber usado GROUP_LS en vez de
  FULL_NAME=Andres Perez            //  PRIV_USER con el mismo propósito
  DESCRIPTION=Un director
  USER_EXPIRE=1-1-1999
  CONNECTION=1
  HOUR_START=8
  HOUR_END=20

// Ahora modificamos Miguel añadiendole un launchpad, y le promocionamos a director..

[ACTION=UPDATE]                     // A  partir de ahora, modificar...

[USER=MIGUEL]
  GROUP=SGDIRECT                    //  Nuevo grupo
  LAUNCHPAD=SELP.INI                //  Nuevo componente

// Borremos ahora el launchpad recién añadido

[ACTION=DELETE]                     // A  partir de ahora, borrar

[USER=MIGUEL]                       // No  es un borrado de usuario, pues especificamos
  LAUNCHPAD                         //  palabras clave. Solo es un borrado de
componente.

// Ahora borremos completamente las definiciones hechas

[USER=MIGUEL]                       //  Borrado completo de usuario
[USER=ANDRES]
[USER=PEPE]
[GROUP=SGCAJERO]                    //  Borrado de grupo (debe estar vacío)
[GROUP=SGDIRECT]
[ALIAS=TSTALIAS]                    //  Borrado del recurso

// Notas generales :
//
// - Recuerde especificar todos los grupos a los cuales pertenecen los usuarios
//   al modificarlos, excepto los reservados por Lan Server: ADMINS, USERS y GUESTS
//
// - Recuerde que los grupos SecureEntry deben empezar por 'SG'
//
// - Una modificación de accesos o componentes solamente modifica aquellos
//   especificados explícitamente. No aquellos que ya existiesen.
//
// - El borrado de objetos (grupos, usuarios, alias) solo se efectúa si
//   no se especifica palabra clave alguna.
```

La herramienta de borrado de definiciones

El programa *EDYERASE.CMD* permite hacer borrados masivos planificados sobre la base de datos de usuarios y grupos SecureEntry. La sintaxis del comando es como sigue :

```
  comando: EDYERASE [?|[/Help]|
                    [[/Branch]  [:nombreoficina]] [[/]Groups]
                     [[/]Ignoreerrors [[/]Local] [[/]NBbranch[:nombreoficina]]
                    [[/]Resources] [[/]Trace]  [[/]SGroups] [[/]Users]
                     [[/]Usersgroup[:grupo]] [/Warning]

   /Branch    : Borrar todos los usuarios de la oficina especificada
   /Groups    : Borrar todos los grupos
   /Help      : Ayuda
   /Ignore    : Ignorar errores
   /Local     : Proceso en modo local (ignorado si UCM no instalado)
```

```
/NBranch   : Borrar todos los usuarios no pertenecientes a la oficina
/Resources : Borrar todos los recursos excepto SGMSHELL (entornos LS)
/Trace     : Mostrar rastro de ejecución
/SGroups   : Borrar todos los grupos SecureEntry (todos si monoestación)
/Users     : Borrar todos los usuarios excepto administradores
/USERSGroup: Borrar recursivamente los usuarios de un grupo
/XGroups   : Preservar de borrado los grupos coincidentes mask
/XResources: Preservar de borrado los recursos coincidentes mask
/XUsers    : Preservar de borrado los usuarios coincidentes mask
/Warning   : No borrar. Tan solo listar los objetos afectados
```

Asi por ejemplo, para borrar todos los usuarios del grupo SG01 y aquellos que no pertenezcan a la oficina B001 de la base de datos, preservando en cualquier caso aquellos cuyo identificador empiece por '8' o '9' el comando será :

```
EDYERASE /USERSG:SG01 /B:B001 /XU:8* /XU:9*
```

La herramienta de volcado de definiciones

La herramienta *EDYDUMP.CMD* permite extraer las definiciones actuales de la base de datos SecureEntry de usuarios, grupos y recursos, sobre un archivo de texto en el formato aceptado por la herramienta EDYDEFS.CMD. Esta herramienta creará por tanto un archivo de tipo texto con las definiciones deseadas, así como los perfiles individuales de seguridad a los que se haga referencia, con nombres de archivo temporales. La sintaxis para su invocación es la siguiente :

```
EDYDUMP Help | [[/]File:f]  [[/]Password:p] [[/]Expire]
               [[/]Nofiles] [[/NOGroups] [[/]NOResources] [[/NOUsers]
              [[/]Trace]   [[/]Ignore]

          File    : Vía de acceso y nombre de archivo de definiciones a crear.
                    Los  perfiles se bajarán al mismo directorio
          Password:  Generar passwords para los usuarios. p puede contener
                     %(.x)U para el identficador de usuario
                     %(.x)N para el número secuencial del usuario
                     %(.x)D para el día actual
                     %(.x)M para el mes actual
                     %(.x)Y para el año actual
                    x  indica longitud forzada, rellenado por la izquierda con '0'.
          Expire  :  Añadir orden de expiración de password para todos los usuarios
          Nofiles :  No bajar perfiles. Solamente crear el archivo de definiciones
          NOGroups:  No extraer información de grupos
       NOResources:  No extraer información de recursos (entornos Lan Server)
          NOUsers :  No extraer información de usuarios
          Trace   :  Mostrar rastro de las llamadas
          Ignore  :  Ignorar errores y continuar

     Ejemplo : EDYDUMP /P:U%.7N
```

Observe que, dado que la API de administración nunca devuelve las claves de acceso por motivos de seguridad, esta información no estará disponible en el volcado resultante. Es por ello que vd. puede usar el parámetro '/P' para generar passwords nuevos para todos sus usuarios.

La utilidad genérica de administración por línea de comandos

El programa EDYADMIN.CMD permite realizar cualquier función de administración directamente. Dado que es una utilidad de propósito general, requiere un conocimiento profundo de la estructura del repositorio (base de datos) SecureEntry. Esta utilidad se describe en la siguiente sección bajo el capítulo Programando sus propias herramientas de administración.

Implementación de soluciones con SecureEntry

En algunos casos, los componentes básicos de SecureEntry pueden no bastar para ajustarse a todos los requisitos de un entorno determinado. SecureEntry tiene una arquitectura que permite extenderlo para adaptarlo a requisitos muy distintos con poco esfuerzo.

SecureEntry puede extenderse en las siguientes áreas:

- Programación de las funciones (API)s de información del usuario para poder obtener información sobre el usuario conectado desde una aplicación.
- Programación de exits de usuario para realizar las tareas requeridas en los distintos eventos de la sesión.
- Programación de filtros de nombres para ajustarse a requisitos de nomenclatura especiales del proceso de conexión.
- Adición de sus propios componentes para que se gestionen del mismo modo que los componentes básicos.
- Programación de sus procedimientos de conexión (LMPs) para gestionar la conexión a subsistemas específicos de su entorno cuando se conecte un usuario.
- Programación de sus propias herramientas de administración para realizar tareas de administración especiales.

SecureEntry tiene un conjunto de utilidades para ayudarle en la implementación de su solución y facilitarle la integración de software. Este incluye diversas utilidades para OS/2 y utilidades para la Máquina Virtual de DOS , además de un sofisticado subsistema de rastreo, que puede usar para depurar su solución con la ayuda de las utilidades de mantenimiento.

Funciones (APIs) de información del usuario

Las funciones de información de usuario le permiten saber qué usuario está conectado, sus privilegios, y otros datos relevantes sobre la sesión en curso. Los archivos necesarios para el uso de estas funciones están el el directorio VíaDeAccesoSecureEntry\API\SOURCES\EDYAPI.

Hay dos funciones disponibles:

```
unsigned long _System sgm_userinfo_getkey (char * key,
                                           char * data,
                                           unsigned long size,
                                           unsigned long reserved);
```

Permite obtener información parcial en base a claves.

```
unsigned long _System sgm_userinfo_get (char * buffer, long  buflen,
                                        short level, unsigned long reserved);
```

Permite obtener toda la información sobre el usuario.

Los códigos de retorno, las claves válidas y las estructuras de datos están definidos en el archivo EDYAPI.H.

Tenga en cuenta que el resto de funciones que aparecen en este archivo se mantienen únicamente por compatibilidad y no tienen efecto en SecureEntry 3.0; la gestión de perfiles debe hacerse ahora a través de las nuevas interfícies de administración.

Programación de exits de usuario

Utilice las exits de usuario si necesita realizar tareas especiales cuando ocurren distintos eventos. Puede programar exits de usuario tanto en REXX como en un lenguaje compilado; en cualquier caso, puede encontrar los archivos fuente en el directorio VíaDeAccesoSecureEntry\API\SOURCES\EDYCUST.

Para programarlas en REXX, modifique el archivo EDYCUST.CMD según sus necesidades y póngalo en el directorio VíaDeAccesoSecureEntry\EXEC. Tenga en cuenta que la invocación del programa EDYCUST.CMD tiene un impacto mínimo sobre el rendimiento: el programa se mantiene cargado en memoria como una función del módulo EDYSLA, gestor de eventos de sesión de SecureEntry. Este funcionamiento permite además dar un soporte limitado de persistencia de valores de variables REXX entre las distintas ejecuciones del programa que corresponden a cada exit; en el mismo EDYCUST.CMD se explica como definir variables de modo que sus valores sean persistentes.

Si las exits de usuario se programan en C, la librería de carga dinámica generada (EDYCUST.DLL) debe ponerse en el directorio VíaDeAccesoSecureEntry\DLL.

Las exits de usuario disponibles son las siguientes:

Exit posterior al arranque (UserExitAfterStartup)
Es una notificación de que el archivo EDYSTART.CMD ha sido procesado. Permite lanzar procesos de un modo simétrico a la exit anterior a concluir.
Se ejecuta en contexto de superusuario.

Exit anterior al diálogo de conexión (UserExitBeforeLogonDialog)
Permite forzar una conexión de invitado antes de que aparezca el diálogo de conexión; la conexión de invitado no requiere que se especifique el usuario y la contraseña.

Puede utilizarla para presentar su propio diálogo de conexión; en este caso, su diálogo deberá ser modal de sistema (system modal), e invocar al programa EDYUTIL (lanzador de eventos de sesión) con los parámetros apropiados para la función NEXTLOGON; si esto no se hace así, el diálogo de conexión de SecureEntry aparecerá posteriormente. Una vez cierre el diálogo, no olvide devolver la modalidad a la ventana que la tuviese anteriormente.

Se ejecuta en contexto de superusuario.

Puede forzar la conclusión del sistema al salir de esta exit.

Exit anterior a la conexión (UserExitBeforeLogon)
Puede usarse sobre forzar una conexión de invitado una vez que el usuario ha rellenado el diálogo de conexión. Por ejemplo, puede implementar conexiones de servicio con contraseñas calculadas por los servicios centrales .
Se ejecuta en contexto de superusuario.
Puede forzar la conclusión del sistema al salir de esta exit.

Exit anterior a la conexión con cambio de contraseña (UserExitBeforeLogonChangingPassword)

Es equivalente a la exit anterior, pero recibe la nueva password como parámetro.

Exit anterior a la activación de perfiles (UserExitBeforeProfilesActivation)
Esta exit se procesa en tiempo de conexión, una vez los perfiles de seguridad y personalización han sido bajados al directorio *WORK*. Se puede utilizar para modificar los perfiles de usuario/grupo antes de su activación.

Exit posterior a la conexión (UserExitAfterLogon)
Puede usarse para realizar cualquier proceso posterior a la conexión. Cuando se procesa esta exit, el WPS ya está inicializado. Tenga en cuenta que esta exit también se procesa en las conexiones de invitado, y en caso de que el shell de usuario (PMSHELL.EXE) se rearranque debido a una excepción. Se ejecuta en contexto de usuario.

Exit posterior a la conexión con cambio de contraseña (UserExitAfterLogonChangingPassword)
Es equivalente a la exit anterior, pero sirve también como notificación de que la contraseña ha sido cambiada.

Exit anterior a la desconexión cancelable (UserExitBeforeCancellableLogoff)
Sirve como notificación de que se ha realizado una petición de desconexión, y permite denegarla.
Se ejecuta en contexto de usuario.

Exit anterior a la desconexión inminente (UserExitBeforeImminentLogoff)
Permite el cierre ordenado de aplicaciones críticas. Esta exit le asegura que la desconexión no puede ser cancelada.
Se ejecuta en contexto de usuario.

Exit posterior a la desactivación de perfiles (UserExitAfterProfilesDeactivation)
Esta exit se procesa en tiempo de desconexión, una vez los perfiles de seguridad y personalización han sido desactivados. Se puede utilizar para modificar o limpiar los perfiles de usuario/grupo antes de que vuelvan a ser copiados al repositorio.

Exit posterior a la desconexión (UserExitAfterLogoff)
Permite realizar cualquier proceso de finalización necesario después de que la sesión de usuario ha terminado.
Se ejecuta en contexto de superusuario.

Exit anterior a concluir (UserExitBeforeShutdown)
Permite realizar cualquier proceso de finalización necesario antes de que el evento de concluir termine.
Se ejecuta en contexto de superusuario.

Exit posterior al arranque del WPS (UserExitAfterPmShell)
Sirve como notificación de que el WPS ya se ha inicializado. Tenga en cuenta que esta exit es especial en cuanto no permite asumir nada respecto a la conexión de usuarios.

Exit anterior al bloqueo cancelable (UserExitBeforeCancellableLockup)
Sirve como notificación de que se ha realizado una petición de bloqueo, y permite denegarla. Puede llamar al programa EDYUTIL para definir la contraseña que debe validarse para desbloquear el sistema.

Exit de bloqueo (UserExitLockup)
Sirve como notificación de que se ha realizado una petición de bloqueo que no puede ser cancelada.

Exit anterior al diálogo de desbloqueo (UserExitBeforeUnlockDialog)
Sirve como notificación de que va a procesarse un evento de desbloqueo. Puede utilizarse para presentar su propio diálogo de desbloqueo, o para llamar al programa EDYUTIL para modificar el comportamiento del diálogo estándar.

Si utiliza su propio diálogo de desbloqueo, éste deberá ser modal de sistema (system modal), e invocar al programa EDYUTIL con los parámetros apropiados para la función NEXTUNLOCK; si esto no se hace así, el diálogo de desbloqueo de SecureEntry aparecerá posteriormente. Una vez cierre el diálogo, no olvide devolver la modalidad a la ventana que la tuviese anteriormente.

Puede forzar la desconexión de la sesión o la conclusión del sistema al salir de esta exit.

Exit anterior al desbloqueo (UserExitBeforeUnlock)
Sirve como notificación de que se ha obtenido la contraseña de desbloqueo y va a validarse contra la contraseña de SecureEntry de la sesión en curso, o contra una contraseña de validación especificada con el programa EDYUTIL con parámetro NEXTUNLOCK. Puede hacer su propia validación de la contraseña si así lo requiere.
Puede forzar la desconexión de la sesión o la conclusión del sistema al salir de esta exit.

Exit posterior a un intento fallido de desbloqueo (UserExitAfterUnsuccessfulUnlock)
Utilice esta exit para modificar el comportamiento de desbloqueo estándar en caso de intento fallido. Aquí puede vd. efectuar la comprobación de una clave secundaria de desbloqueo, o forzar una desconexión o conclusión del sistema.

Exit posterior al desbloqueo (UserExitAfterUnlock)
Sirve como notificación de que el evento de desbloqueo está finalizando.

Exit anterior a la desconexión desde el diálogo de desbloqueo (UserExitBeforeLogoffFromUnlock)
Sirve como notificación de que se ha realizado una petición de desconexión desde el diálogo de desbloqueo, en el caso de que esta posibilidad esté habilitada por el perfil activo de características del SES. La petición puede ser denegada.

Exit anterior a concluir desde el diálogo de desbloqueo (UserExitBeforeShutdownFromUnlock)
Sirve como notificación de que se ha realizado una petición de concluir desde el diálogo de desbloqueo, en el caso de que esta posibilidad esté habilitada por el perfil activo de características del SES. La petición puede ser denegada.

Exit de señalización (UserExitSignal)
Sirve como mecanismo de comunicación desde una aplicación hacia el contexto de las exits de usuario, para poder realizar tareas desde el código de las exits de usuario. Utilice el programa EDYUTIL para activar una de estas exits.

Exit de señalización de superusuario (UserExitSignalSuperUser)
Sirve como mecanismo de comunicación desde una aplicación hacia el contexto de las exits de usuario, para poder realizar tareas desde el código de las exits de usuario actuando en contexto de superusuario. Utilice el programa EDYUTIL para activar una de estas exits.

Tenga en cuenta que si no está utilizando SES (Security Enabling Services), los procesos que se arranquen desde esta exit se ejecutarán en contexto de usuario en lugar de en contexto de superusuario.

Exits de LMP (UserExitBeforeLMP___ y UserExitAfterLMP___)
Estas exits sirven para cambiar el flujo normal de los procedimientos de conexión (LMPs) examinando el código de retorno que está a punto de ser devuelto y modificándolo convenientemente. Por ejemplo, puede usar estas exits para evitar la conexión de emergencia o forzar una contraseña calculada para algunos usuarios.

Exits de los objetos con activadores (UserExitBeforeOpenFolder y UserExitAfterCloseFolder)
Sirven como notificación de que un objeto configurado para lanzar exits de usuario al abrirse o cerrarse va a ser abierto o ha sido cerrado. La exit de notificación de apertura puede ser usada para denegarla.

Puede ver como se configura un objeto para que lance estas exits en el capítulo Definición de objetos con activadores.

Exit de teclas de sistema (UserExitHotkey)
Si el perfil de SES activo tiene definida la captura de alguna combinación de teclas de sistema, se lanzará esta exit cada vez que una de estas combinaciones sea detectada. Su código puede decidir si procesa las teclas o deja que éstas tengan su efecto normal.

Exit de antes de un rearranque (UserExitBeforeReboot)
Esta exit de usuario será lanzada cada vez que SecureEntry vaya a proceder al rearranque de la máquina como consecuencia de dicha solicitud por medio del diálogo de opciones de la combinación de teclas Ctl-Alt-Del, o bien cuando dicha combinación de teclas sea pulsada y esté configurada para efectuar el rearranque automático de la estación.

Puede obtener más información en la siguiente sección (Flujo de las exits de usuario) y en los comentarios de los archivos fuente que se dan como esqueleto. También puede ver un ejemplo de implementación de exits de usuario, asi como el modo de activar los diálogos de ejemplo de conexión y desbloqueo.

Flujo de las exits de usuario

La siguiente lista muestra el flujo normal de llamadas a las diferentes exits de usuario

```
* Arranque de la estación y conexión normal

UserExitAfterStartup
UserExitBeforeLogonDialog
UserExitBeforeLogon
UserExitBeforeLMPSignon              Nota : una  llamada por cada LMP
UserExitAfterLMPSignon
UserExitAfterPmShell                 Nota :  Asíncrona (orden indeterminado)
UserExitBeforeProfilesActivation
UserExitAfterLogon

* Bloqueo-desbloqueo

UserExitBeforeCancellableLockup
UserExitLockup
UserExitBeforeUnlockDialog
UserExitBeforeUnlock
UserExitAfterUnlock

* Concluir normal desde el escritorio

UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff
UserExitAfterProfilesDeactivation
UserExitBeforeLMPSignoff             Nota : una  llamada por cada LMP
UserExitAfterLMPSignoff
UserExitAfterLogoff
UserExitBeforeShutdown

* Arranque de la estación y conexión normal con cambio de contraseña

UserExitAfterStartup
UserExitBeforeLogonDialog
UserExitAfterPmShell                 Nota :  Asíncrona (orden indeterminado)
UserExitBeforeLogonChangingPassword
UserExitBeforeLMPSignon              Nota : una  llamada por cada LMP
UserExitAfterLMPSignon
UserExitBeforeProfilesActivation
UserExitAfterLogonChangingPassword

* Bloqueo-desconexión  desde el diálogo de desbloqueo
```

```
UserExitBeforeCancellableLockup
UserExitLockup
UserExitBeforeUnlockDialog
UserExitBeforeLogoffFromUnlock
UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff
UserExitAfterProfilesDeactivation
UserExitBeforeLMPSignoff              Nota : una  llamada por cada LMP
UserExitAfterLMPSignoff
UserExitAfterLogoff

* Concluir desde el diálogo de conexión

UserExitBeforeLogonDialog
UserExitBeforeShutdown

* Bloqueo-contraseña inválida-reintento con éxito y desbloqueo

UserExitBeforeCancellableLockup
UserExitLockup
UserExitBeforeUnlockDialog
UserExitBeforeUnlock
UserExitAfterUnsuccessfulUnlock
UserExitBeforeUnlock
UserExitAfterUnlock

* Desconexión normal desde el escritorio

UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff
UserExitAfterProfilesDeactivation
UserExitBeforeLMPSignoff              Nota : una  llamada por cada LMP
UserExitAfterLMPSignoff
UserExitAfterLogoff

* Conexión normal con cambio de contraseña

UserExitBeforeLogonDialog
UserExitBeforeLogonChangingPassword
UserExitBeforeLMPSignon               Nota : una  llamada por cada LMP
UserExitAfterLMPSignon
UserExitBeforeProfilesActivation
UserExitAfterLogonChangingPassword

* Desconexión normal desde el escritorio, cancelada por el usuario

UserExitBeforeCancellableLogoff

* Desconexión normal desde el escritorio

UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff
UserExitAfterProfilesDeactivation
UserExitBeforeLMPSignoff              Nota : una  llamada por cada LMP
UserExitAfterLMPSignoff
UserExitAfterLogoff

* Conexión de invitado forzada desde la exit anterior a la  conexión

UserExitBeforeLogonDialog
UserExitBeforeLogon                   Note : Retorna  RC_GUEST_LOGON
UserExitAfterLogon

* Desconexión desde el escritorio de un usuario invitado

UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff
```

```
* Conexión de invitado forzada desde la exit anterior al diálogo de conexión

UserExitBeforeLogonDialog            Note : Retorna  RC_GUEST_LOGON
UserExitAfterLogon

* Desconexión desde el escritorio de un usuario invitado

UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff

* Conexión normal

UserExitBeforeLogonDialog
UserExitBeforeLogon
UserExitBeforeLMPSignon              Nota : una llamada por cada LMP
UserExitAfterLMPSignon
UserExitBeforeProfilesActivation
UserExitAfterLogon

* Bloqueo y concluir desde el diálogo de desbloqueo

UserExitBeforeCancellableLockup
UserExitLockup
UserExitBeforeUnlockDialog
UserExitBeforeShutdownFromUnlock
UserExitBeforeCancellableLogoff
UserExitBeforeImminentLogoff
UserExitAfterProfilesDeactivation
UserExitBeforeLMPSignoff             Nota : una  llamada por cada LMP
UserExitAfterLMPSignoff
UserExitAfterLogoff
UserExitBeforeShutdown
```

Ejemplo de exits de usuario

Para clarificar el alcance de las exits de usuario, suponga el siguiente escenario de ejemplo.

Disponemos de una aplicación que gestiona la conexión y la desconexión, y queremos intergrar SecureEntry en este entorno para poder utilizar las funciones de bloqueo, manejo del crt-alt-supr y activación de perfiles. Supongamos que la aplicación tiene la siguiente lógica:

```
Do
  Obtener Usuario y Contraseña
  ValidarUsuario
  if not privilegiado then
     ejecutar aplicación de terminal
Until privilegiado
```

También queremos disponer de una 'puerta trasera' para permitir la conexión de un administrador de SecureEntry. Tenemos entonces tres tipos de usuarios:

Usuarios de terminal, con un conjunto de perfiles de seguridad restringidos.

Usuarios de servicios, con acceso limitado a los recursos de sistema.

Administradores de SecureEntry.

Considerando que es esta aplicación la que obtiene y valida los usuarios y contraseñas, una de las maneras más fáciles de implementar este escenario es mediante el uso de exits de usuario. Una posible solución es la siguiente:

Todos las conexiones serán de invitado, excepto cuando se conecte el administrador de SecureEntry. Esto quiere decir que el diálogo de conexión de SecureEntry nunca se mostrará excepto cuando se use la puerta trasera.

Los perfiles de seguridad restringidos de los usuarios de terminal serán los que se usarán por omisión, poniéndolos en el directorio NOUSER.

Los perfiles de seguridad privilegiados de los usuarios de servicios también estarán en el directorio NOUSER (p*.ini), pero serán activados y desactivados cuando se conecten y desconecten respectivamente.

La conexión del administrador de SecureEntry se implementará usando un parámetro pasado mediante una exit de señalización.

Para completar el ejemplo, abriremos el reloj del sistema para los administradores de SecureEntry.

Los cambios que se requieren en EDYCUST.CMD:

```
1) Declaramos una variable global

   Line 158:  MyGlobalVars='aString'

2) UserExitAfterStartup:

      /*
         Podemos utilizar esta exit para inicializar este entorno,
         puesto que esta será la primera exit, descontando la
         posterior al  arranque del shell.
      */

      /* Para poder abrir el reloj del sistema */
      call RxFuncAdd 'SysLoadFuncs',  'REXXUTIL', 'SysLoadFuncs'
      call SysLoadFuncs

      /* Asegurarse de que la primera conexión es normal */
      aString=''

   return RC_NONE

3) UserExitBeforeLogonDialog:

   /* Si no se usa la puerta trasera, siempre conexión de invitado */

   if strip(translate(aString))<>'SENTRY'  then
      return RC_GUEST_LOGON

   return RC_CONTINUE_NORMAL_LOGON_FLOW

4) UserExitAfterLogon:

      UserID=Reserved1

      if strip(translate(aString))<>'SENTRY'  then
      do

        /* Conexión normal...                    */
        /* Debe hacerse un 'detach' o un 'start', puesto que
           queremos que se ejecute en la sesión de usuario y
           no en la exit.                                    */

        'start /C  d:\sgmshell\exec\apprun.cmd'
      end
      else
      do
        /* Puerta trasera....                    */
```

```
        /* Cerramos la puerta: la siguiente conexión será normal */

        aString=''

        /* Abrimos el reloj del sistema */
        rc=SysOpenObject('<WP_CLOCK>','DEFAULT',1)
      end

   return RC_NONE

5) UserExitBeforeImminentLogoff:

      if strip(translate(aString))='PRIV'  then
      do
        /* Desactivamos los perfiles con privilegios
           activando los perfiles por omisión en NOUSER */

        'd:\sgmshell\exec\edyrefr.exe  d:\sgmshell\nouser\edydesk.ini'
        'd:\sgmshell\exec\edyflpy.exe  /I:d:\sgmshell\nouser\edyflopp.ini'
        aString=''
      end

      /* Nótese que no modificamos el valor de aString si indica que
         la siguiente conexión es de un administrador de SecureEntry ('SENTRY') */

   return RC_NONE

6) UserExitSignal:

      aString=AllParms

      if strip(translate(aString))='PRIV'  then
      do
        /* Activar los perfiles con privilegios */

        'd:\sgmshell\exec\edyrefr.exe  d:\sgmshell\nouser\pdesk.ini'
        'd:\sgmshell\exec\edyflpy.exe  /I:d:\sgmshell\nouser\pflopp.ini'
      end
      /* Forzar una desconexión si se pide una conexión de administrador */
      if strip(translate(aString))='SENTRY'  then
        'edyutil frlogoff'

   return RC_NONE
```

El código de la aplicación necesita el siguiente cambio en su lógica:

```
    Do
      Obtener Usuario y Contraseña
      ValidarUsuario

      RUN EDYUTIL NEXTUNLOCK /U:UserID /V:password

      if not privilegiado then
         ejecutar aplicación de terminal
    Until privilegiado

    RUN EDYUTIL SIGNAL PRIV
```

En cualquier momento, EDYUTIL SIGNAL SENTRY puede abrir la puerta trasera, forzando una desconexión y haciendo que la siguiente conexión sea realmente una conexión de SecureEntry.

¡Con qué facilidad 20 líneas de REXX han conseguido un cambio de comportamiento tan notable!

Diálogos de ejemplo de conexión y desbloqueo

Como ya se ha comentado, las exits de usuario permiten introducir fácilmente diálogos de conexión y desbloqueo creados por el propio usuario, como alternativa a los diálogos que SecureEntry proporciona por defecto.

Como ejemplo en el directorio EXEC del camino de SecureEntry podrá encontrar un diálogo de conexión y un diálogo de desbloqueo alternativos, totalmente configurables. Los ficheros fuente de ambos diálogos están disponibles en el directorio API\SOURCES\DIALOGS, en la vía de acceso de instalación SecureEntry. Se trata de dos proyectos VisproRexx, suministrados en formato de archivo empaquetado (ZIP).

El diálogo de conexión responde a la siguiente sintaxis de invocación:

```
LOGSAMP [/D:dominio | /d:[dominio]]
        [/U:usuario /L:file.bmp /S:string /NG /NC /Ns /NS
         /NH /P:px,py /T /F]
```

/D:

para especificar el dominio por defecto en la siguiente conexión.

/d:

para especificar el dominio por defecto, y que además el diálogo de conexión presente un campo de entrada que permita modificar este dominio.

/U:

para especificar el identificador de usuario por defecto que aparecerá en el campo de usuario.

/L:

para especificar el fichero con el logotipo que aparecerá en el diálogo, por defecto aparecerá el de IBM.

/S:

para especificar el string que figurará como encabezamiento en el diálogo de conexión, por defecto aparecerá "IBM Global Services".

/NG

para ocultar el botón de conexión como invitado.

/NC

para ocultar el botón de despejar.

/Ns

para ocultar el botón de concluir.

/NS

para ocultar el botón de concluir forzado.

/NH

para ocultar el botón de ayuda.

/P:

para especificar la situación del diálogo en la pantalla. Tanto las coordenadas horizontales (px) como las verticales (py) tienen su origen en la parte inferior izquierda de la pantalla y admiten valores entre 0 y 100, ambos inclusive. La posición por defecto es el centro de la pantalla.

/T

para mostrar el reloj.

/F

para mostrar la fecha.

Para el diálogo de desbloqueo la sintaxis es de la forma:

```
UNSAMP [/L:file.bmp /S:string /Nl /NL /Ns /NS
       /NH /P:px,py /T /F]
```

/L:

para especificar el fichero con el logotipo que aparecerá en el diálogo, por defecto aparecerá el de IBM.

/S:

para especificar el string que figurará como encabezado en el diálogo, por defecto aparecerá "IBM Global Services".

/Nl

para ocultar el botón de desconexión.

/NL

para ocultar el botón de desconexión forzada.

/Ns

para ocultar el botón de concluir.

/NS

para ocultar el botón de concluir forzado.

/NH

para ocultar el botón de ayuda.

/P:

para especificar la situación del diálogo en la pantalla. Tanto las coordenadas horizontales (px) como las verticales (py) tienen su origen en la parte inferior izquierda de la pantalla y admiten valores entre 0 y 100, ambos inclusive. La posición por defecto es el centro de la pantalla.

/T

para mostrar el reloj.

/F

para mostrar la fecha.

Si se está interesado en utilizar el diálogo de conexión alternativo con, por ejemplo, la siguiente configuración:

Con un dominio por defecto "dominio" modificable.

Sin botón de conexión como invitado.

Sin botón de concluir forzado.

Con fecha y hora.

se habría de modificar la exit de usuario anterior al diálogo de conexión, en el fichero EDYCUST.CMD, de la siguiente manera:

```
UserExitBeforeLogonDialog:
       /* Se realiza una invocación al diálogo de conexión alternativo */
        'LOGSAMP /d:dominio /NG/NS/F/T'
       /* Se retorna el RC proporcionado por LOGSAMP */
         return RC
```

La invocación al diálogo de desbloqueo se realizaría de manera similar pero modificando, en este caso, la exit de usuario anterior al diálogo de desbloqueo.

Para finalizar, debería vd. especificar el nombre de estos módulos con ayuda de la variable de entorno **SGM_USER_DLGS**, para así conseguir mayor robustez en el mecanismo de sobreseimiento de los diálogos por defecto.

Programación de filtros de nombres

El archivo EDYFILT.DLL, o DLL de filtro, puede usarse para permitir la traducción automática de identificadores de usuario, contraseñas y nombres de dominio. Esto permite integrar subsistemas con diferentes convenciones de nomenclatura.

El archivo fuente que debe ser modificado para programar una DLL de filtro se encuentra en el directorio VíaDeAccesoSecureEntry\API\SOURCES\EDYFILT. Una vez modificado y compilado, la DLL generada debe ponerse en el directorio SecureEntryPath\DLL. Si está disponible, la DLL de filtro será invocada por cada uno de los subsistemas de conexión antes de usar los parámetros que reciben. Por ejemplo, puede decidir que uno de sus subsistemas reciba las contraseñas encriptadas, o añadir un prefijo a los identificadores de usuario sin necesidad de que los usuarios tengan que introducirlo en el diálogo de conexión.

Si utiliza una DLL de filtro debe tener en cuenta que cualquier modificación que haga sobre los identificadores de usuario sólo se utilizará durante la conexión de los subsistemas, y no en las herramientas de administración, que usarán los identificadores sin modificar.

Adición de sus propios componentes

Las herramientas de administración le permiten asignar a usuarios y grupos perfiles de seguridad de cualquiera de los componentes de seguridad estándares de SecureEntry, como las restricciones del treelock o las del escritorio. Puede definir nuevos componentes de seguridad que son gestionados por SecureEntry de la misma manera que los componentes de seguridad estándares.

Un perfil de seguridad es una instancia concreta de un componente de seguridad. A pesar de esta terminología, un componente de seguridad no está necesariamente ligado a la seguridad, sino que puede usarse para almacenar cualquier tipo de información. Por ejemplo, puede decidir añadir como un nuevo componente el archivo de configuración de una aplicación o un archivo con información histórica sobre las actividades de un usuario.

Qué es un componente

Un componente de seguridad es un objeto (archivo) cuyas instancias, los perfiles de seguridad, tienen un comportamiento y características asociados:

1. Un componente tiene su nombre de componente.
2. Un componente tiene un nombre de archivo de perfil de seguridad por omisión. Éste es el nombre del archivo del perfil de seguridad que se activará durante la conexión.
3. Un componente tiene un editor. Éste se define mediante el nombre y los parámetros del programa capaz de reconocer y permitir la edición de un perfil del componente.
4. Un componente tiene un activador. Éste se define mediante el nombre y los parámetros del programa capaz de interpretar el perfil y hacerlo activo en el sistema, imponiendo las restricciones de seguridad necesarias si esta es la finalidad del componente.
5. Un componente tiene un icono que lo representa.
6. Un componente sigue una serie de reglas

   Es estático (sólo lectura) o dinámico (lectura y escritura): los perfiles de este componente sólo son actualizados en la base de datos a través de las herramientas de administración o, por el contrario, se guardan automáticamente en la base de datos durante la desconexión.

   Es obligatorio o prescindible para la conexión: la conexión de usuarios que no tienen un perfil de este componente asignado está o no permitida.

El archivo de descripción de componentes y el comando UPDATEDB

La tabla de descripción de las características de todos los componentes está almacenada en el repositorio de SecureEntry; ésta puede verse o actualizarse con el comando UPDATEDB. Para actualizar la tabla de componentes, debe actualizar el repositorio utilizando un archivo ASCII de descripción de componentes, de manera que la nueva tabla se active en el siguiente arranque de la máquina. La sintaxis es la siguiente:

```
UPDATEDB  archivoDeDescripcion
```

Si UPDATEDB no recibe el nombre del archivo de descripción como parámetro, mostrará la tabla de descripciones activa que está almacenada en el repositorio.

Tenga en cuenta que el archivo de descripción que se utiliza durante la instalación se llama 'SENTRY.DSC' y se encuentra en el primer disquete de instalación. Este archivo le puede servir como ejemplo en la definición de nuevos componentes.

A continuación se presenta un ejemplo de archivo de descripción de componentes.

```
[General]

MaxSignonAttempts   5       # ¡Es peligroso si sólo hay un administrador definido!
MinPasswordLen      4
PasswordExpireDays  0       # 0 significa que las contraseñas no expiran
```

```
[Components]

#CompName       DownloadName  Editor            Interface           Datatype Icon  Mand Chg
Description
#-------------------------------------------------------------------------------------------
--
DESKTOP         EDYDESK.INI   'EDYEDRES.EXE &'  $SENTRY             MISSING  @3003   N   A
Personal desktop profile
PERS_DESKTOP    EDY_PER.INI   MISSING           $SENTRY             MISSING   MISSING N   U
Personal desktop settings
SYSTEM_MENUS    EDYWIN.INI    'EDYWINE.EXE &'   'EDYWINR.EXE /F:&' MISSING  @3006   N   A
Window behavior
FLOPPY_DISK     EDYFLOPP.INI  'EDYFLINI.EXE /&' 'EDYFLPY.EXE /I:&' MISSING  @3005   N   A
Floppy disk behavior
TREE_LOCK       EDYDD32.INI   'E.EXE &'         'EDYDDUTL.EXE /F&' MISSING   MISSING N   A
SES_BEHAVIOUR   EDYSES.INI    'EDYSESE.EXE &'   'EDYBGINI.EXE /F&' MISSING  @3007   N   A
Lockup, timeouts and CAD
TLOCK_AUDIT     EDYDD32.AUD   'E.EXE &'         'EDYDDUTL.EXE /A&' MISSING   MISSING N   U
Tree Lock audit
LAUNCHPAD       EDYPAD.INI '/I EDYLNEDT.EXE /F&''EDYLNREF.EXE /F&' MISSING  @3004   N   A
Personal launchpad
SCENTER         EDYSC.INI  '/I EDYSCEDT.EXE &'  'EDYSCTST.EXE &'   MISSING  @3017   N   A
SmartCenter profile
WINDOW_LIST     EDYWDLST.INI   'EDYWDEDT.EXE &' 'EDYWDINI.EXE /F&' MISSING  @3011   N   A
WindowList behaviour
PERS_MODEL      EDYMPER.INI    'EDYEDPER.EXE &' $SENTRY             MISSING  @3013   N   A
Personal desktop model
SHORTCUTS       EDYHOTK.INI    'EDYHOTKE.EXE &' 'EDYHOTKR.EXE /F &'MISSING  @3014   N   A
Shortcuts profile
HOOKED_OBJECTS  EDYCUSWP.INI 'EDYEDPER.EXE /P &'$SENTRY             MISSING  @3016   N   A
Hooked objects
ROAMING_DESKTOP EDYROAM.INI    'EDYROAME.EXE &' 'EDYROAMT.EXE /F&' MISSING  @3018   N   A
Roaming desktops
EXECS_AUDITOR   EDYEXEC.INI    'EDYEXECE.EXE &' 'EDYEXECT.EXE /F&' MISSING  @3019   N   U
Processes auditor
```

La observación del archivo anterior deja claro como añadir nuevos componentes. Las siguientes notas le serán útiles para interpretar el archivo.

La sección [General] sólo es respetada en entornos monoestación, puesto que sus valores son reemplazados por los valores de Lan Server si éste es usado.

El carácter '#' sirve para iniciar comentarios. Estos pueden estar en cualquier línea.

La palabra clave reservada 'MISSING' indica que una característica no está disponible.

El nombre de componente (campo ComponentName) sirve como índice de la base de datos para asignar los perfiles de seguridad a usuarios y grupos. Debe usar este nombre como palabra clave cuando utilice las APIs de administración o las herramientas de administración no interactivas.

El nombre de archivo por omisión (campo 'DownloadName') es el nombre del archivo de perfil de seguridad que se obtendrá de la base de datos durante la conexión para dejarlo en el directorio WORK.

El editor debe ser un ejecutable que 'entienda' los perfiles de seguridad y sea capaz de guardarlos con el nombre de archivo que ha recibido como parámetro. Puede usar el editor del sistema para perfiles con formato ASCII. El comando que aparece en el archivo de descripción indica como invocar el editor, sustituyendo '&' por el nombre completo del perfil de seguridad que se va a editar.

El activador (campo 'Interface') debe ser un ejecutable que 'entienda' los perfiles y sea capaz de hacerlos activos al ser invocado a través del comando que se indica en el archivo de descripción, sustituyendo '&' por el nombre completo del perfil de seguridad que se va a activar. Tenga en cuenta que este comando se invocará sin nombre de archivo especificado durante la desconexión, y que el ejecutable es el responsable de dejar inactivo el perfil que se ha activado anteriormente. '$SENTRY' es un valor reservado por SecureEntry.

El campo 'Datatype' está reservado y debe tener 'MISSING' como valor.

El campo 'Iconfile' debe ser el nombre completo de archivo de un icono que representa el componente. El archivo de descripción de ejemplo utiliza números precedidos por '@' que indican que el icono se obtiene de la herramienta de administración; en lugar de esto, sus componentes deben especificar un nombre de archivo.

El campo 'Mand' indica si es imprescindible que el usuario que se conecta tenga asignado un perfil de seguridad del componente. Puede tomar los valores 'Y', para indicar que es imprescindible, o 'N', para indicar que no lo es.

El campo 'Chng' indica si el componente puede ser modificado por el usuario o sólo por el administrador. Puede tomar los valores 'U' para indicar que el usuario puede modificarlo, o 'A' para indicar que sólo se puede modificar con las herramientas de administración. Cuando un componente es modificable por el usuario, su perfil de seguridad se guarda en el repositorio en tiempo de desconexión para ser utilizado de nuevo en la siguiente conexión del usuario en cualquier estación que comparta el repositorio (en la LAN o en el host si utiliza UCM).

El campo 'Description' no tiene formato especial y sirve para describir el componente.

El nombre del componente y del archivo por omisión ha de ser único.

PRECAUCIONES IMPORTANTES

Cuando planee añadir o suprimir componentes debe tener en cuenta los siguientes puntos:

El comando UPDATEDB sobreescribe completamente la tabla de descripción de componentes que está activa. Por tanto, debe asegurarse de que no borra componentes que tienen algún perfil de seguridad almacenado en el repositorio.

La herramienta de administración interactiva puede añadir a los perfiles de seguridad una 'marca' para permitirle identificar el componente del que es una instancia. Esta marca permite que al soltar un perfil la herramienta no necesite preguntar de qué componente se trata. Cuando la herramienta de administración pregunta el componente correspondiente al perfil que se ha soltado, también da la oportunidad de añadir la marca.

Para los archivos INI de OS/2 (formato prf), la marca consiste en una entrada con Aplicación='SENTRY', Clave='COMPONENT' y valor igual al nombre del componente.

Para los archivos ASCII, la marca consiste en una primera línea con el nombre del componente.

Preste atención al aplicar mantenimiento de SecureEntry (SERVICE) a máquinas cuyo tabla de componentes ha sido modificada. Antes de aplicar el mantenimiento, copie su versión del archivo de descripción de componentes con el nombre SENTRY.DSC en el último disquete de instalación; de este modo, será su archivo el que se utilice por los procedimientos de instalación para actualizar el repositorio.

Programación de procedimientos de conexión (LMPs)

Los procedimientos de conexión a un subsistema, o LMPs (Logon Modular Procedures), le permiten que la conexión a este subsistema esté completamente integrada con la conexión de SecureEntry. Un LMP se implementa con una DLL que exporta funciones capaces de gestionar la identificación de usuarios del subsistema, su conexión y desconexión, y, posiblemente, los cambios de contraseñas para permitir la sincronización de ésta con otros subsistemas. A continuación se describe el código necesario para integrar su subsistema con SecureEntry; como verá, el código es bastante simple.

Escribir e instalar un LMP

El archivo fuente que debe ser modificado para escribir el LMP de un subsistema se encuentra en el directorio VíaDeAccesoSecureEntry\API\SOURCES\LMP.

Una vez modificado, compílelo para generar una DLL llamada EDYxxLMP.DLL, donde xx son dos letras que identifican su subsistema. Para que la DLL se pueda cargar, no olvide modificar también el nombre de la librería en el archivo DEF para que coincida con el nombre de la DLL.

Para instalar el LMP, ponga la nueva DLL en el directorio DLL y modifique el archivo de configuración de LMPs VíaDeAccesoSecureEntry\NOUSER\EDYSSLMP.DAT de modo que su DLL se invoque durante la conexión. Puede ver una descripción de este archivo en la sección Configuration files

Funciones exportadas por un LMP

A continuación se describen las funciones que un LMP exporta para que sean invocadas por SecureEntry.

EdySignOn

En esta función

establezca la conexión del usuario al subsistema.

asigne los recursos específicos del subsistema que estén configurados, tal como el Lan Server asigna unidades e impresoras durante la conexión.

tome nota del usuario, la contraseña y, si se requiere, el dominio para su uso posterior.

Cuando la función devuelve OK, implica que ha permitido la conexión del usuario con la contraseña especificada. Si es así, el subsistema estará en estado de conexión y esta función no será invocada de nuevo sin que antes se invoque la función de desconexión EdySignOff.

El orden en que se invoca esta función para los distintos LMPs es el mismo en que los LMPs aparecen en el archivo de configuración EDYSSLMP.DAT.

EdySignOff

En esta función debe desconectarse del subsistema, reinicializar sus variables y tomar nota de que está en estado de desconexión.

EdyForcePassword

Esta función sólo será invocada si otro subsistema, como RACF o similar, actua como sincronizador de contraseñas. Debe forzar que le sea asignada al usuario la contraseña especificada como parámetro.

Si utiliza el esqueleto de LMP del directorio SecureEntryPath\API\SOURCES\LMP, tendrá garantizado un mecanismo de seguridad por el que esta función sólo puede ser invocada por SecureEntry cuando el usuario esté verificado.

EdyQueryUserid

En esta función debe devolver los parámetros de conexión que le han sido especificados en la función de conexión EdySignOn, de manera que se pueda saber quién está conectado a su subsistema.

EdyPwSyntaxValidation

En esta función debe verificar que la sintaxis de una contraseña es válida y que puede ser aceptada en una operación de cambio de contraseña como nueva contraseña.

EdyIdSyntaxValidation

En esta función debe verificar que la sintaxis de un identificador de usuario es válida y que puede ser aceptado en una operación de cambio de contraseña.

EdyUserPwValidation

Esta función es invocada por SecureEntry para verificar que una combinación de usuario u contraseña es válida en su subsistema, pero sin que se haga la conexión al mismo. Esta función puede ser invocada por SecureEntry a petición de alguna aplicación.

Algunas reglas para escribir un LMP

Todas las funciones de la sección anterior deben ser completadas y exportadas, excepto la función para forzar una nueva contraseña (EdyForcePassword). Ésta sólo se necesita si su LMP está sincronizado por otro; si su LMP se encarga de sincronizar a los demás, la función nunca será invocada.

Utilice el esqueleto de LMP VíaDeAccesoSecureEntry\API\SOURCES\LMP\EDYxxLMP.c. Éste le asegura que las funciones que pueden tener riesgos de seguridad sólo pueden ser invocadas por SecureEntry.

No modifique los parámetros de entrada que reciba por referencia.

Tenga en cuenta que los direcciones de los parámetros de una función sólo son válidas mientras está procesando esta función: no almacene apuntadores a los parámetros para su uso posterior.

Devuelva siempre códigos de retorno definidos en el archivo EDYERROR.TXT, o utilice el parámetro previsto para mensajes de error.

Programación de herramientas de administración

Hay tres niveles de funciones (APIs) sobre las que puede desarrollar sus propias herramientas de administración:

La API en línea de comando (EDYADMIN)

La API de REXX

La API de 'C'

Cada una de estas APIs gestiona los mismos objetos; puede usarlas indistintamente en función de sus requisitos y experiencia programando.

Cualquiera de estas API le permite realizar cuatro funciones principales,

Añadir (Add)

Borrar (Delete)

Actualizar (Update)

Ver (View)

sobre objetos de tipos distintos. Los siete tipos de objetos que puede manipular son

Usuario (User): contiene las características (palabras clave) de un usuario determinado. Las palabras clave definen la información de conexión y los perfiles de seguridad asignados.

Grupo (Group): contiene las características (palabras clave) de un grupo determinado. Las palabras clave definen la información de conexión y los perfiles de seguridad asignados.

Recurso (Resource): contiene las características (palabras clave) de un recurso determinado. Este tipo de objeto sólo se usa en entornos de Lan Server, y define la información de los recursos que son compartidos con un alias.

Usuario-Grupo (UserGroup): define la pertenencia de un usuario a un grupo.

Grupo-Grupo (GroupGroup): define la pertenencia de un grupo a otro grupo. Este tipo de objetos sólo se usa en entornos monoestación en los que puede definirse un grupo como perteneciente a otro.

Recurso-Usuario (ResourceUser): define la relación 'usado por' entre un recurso y un usuario. Las palabras clave definen las asignaciones de conexión y los privilegios de acceso.

Recurso-Grupo (ResourceGroup): define la relación 'usado por' entre un recurso y un grupo. Las palabras clave definen las asignaciones de conexión y los privilegios de acceso.

Como ejemplo, los siguientes pasos muestran como añadir un usuario a la base de datos:

1. Haga una llamada ADD de un objeto User, con las palabras clave de sus distintos perfiles de seguridad asignados y sus datos de usuario (LAN_DATA). La clave LAN_DATA define características como el horario de conexión permitido, la contraseña, la descripción...
2. Haga llamadas ADD de los objetos UserGroup necesarios para incluir al usuario en todos los grupos que le corresponden
3. Haga llamadas ADD de los objetos ResourceUser necesarios para asignar al usuario los recursos a los que debe tener acceso.

Utilidad EDYADMIN

Esta utilidad permite invocar las funciones de administración desde archivos CMD o desde la línea de comandos. Todas las funciones de administración están disponibles a través de este comando.

```
EDYADMIN [S=Subsistema] Acción TipoDeObjeto=IdDeObjeto[,IdDeObjeto2]  [PalabrasClave]
```

Subsistema

Nombre del agente que procesa la petición. Trabajando con los subsistemas estándares de SecureEntry, no necesitará especificar este parámetro; este parámetro está disponible para permitir trabajar con agentes de subsistemas no estándares.

Acción

Un nombre de acción válido. Estos son:

Add, para añadir objetos.

Delete, para borrar objetos.

Update, para actualizar objetos.

View, para ver listas de objetos o sus valores.

TipoDeObjeto

Un nombre de objeto válido. Estos son:

Group

GROUPGroup

Resource

RESOURCEGroup

RESOURCEUser

Subsystem

User

USERGroup

IdDeObjeto[,IdDeObjeto2]

Un nombre de objeto válido, o, cuando se trate de un objeto de uno de los tipos que relaciona dos objetos distintos, los nombres de los dos objetos separados por una coma.

PalabrasClave

Lista de palabras clave/valor separadas por comas. Por ejemplo,

```
LAUNCHPAD=@archivo1,LAN_DATA=DESCRIPTION=Un  usuario
```

El identificador de clave es siempre el nombre que aparece a la izquierda del primer signo igual. El operador de indirección '@' le permite referirse a un archivo.

Ejemplos:

```
EDYADMIN A U=JUAN
                  Añade el usuario Juan con valores por omisión
EDYADMIN A USERG=JUAN,CAJEROS
                  Añade Juan al grupo de CAJEROS
EDYADMIN U U=JUAN DESKTOP=@EDYDESK.INI
                  Actualiza las restricciones del escritorio para Juan
EDYADMIN U U=JUAN LAN_DATA=FULL_NAME=Juan  Jo DESCRIPTION=Un cajero
                  Actualiza el nombre de Juan y  su descripción
EDYADMIN V USERG=*,*
                  Obtiene la lista de todos los usuarios que peretenecen
                  a  todos los grupos
EDYADMIN V USERG=*,CAJEROS
                  Obtiene la lista de todos los usuarios que pertenecen
                  al  grupo CAJEROS
EDYADMIN V USERG=*,
                  Obtiene la lista de todos los usuarios que no pertenecen
                  a  ningún grupo
```

La API de REXX

La API de administración en REXX está exportada por la DLL RXUCM. Las herramientas de administración batch (EDYERASE.CMD, EDYADMIN.CMD y EDYDEFS.CMD) son buenos ejemplos de cómo puede usarse esta API.

A continuación se describen las funciones disponibles:

RxEdyUcmLoadFuncs

Esta función sirve para cargar el resto de funciones disponibles, tal como muestra el siguiente ejemplo.

```
If RxFuncQuery('RxEdyUcmLoadFuncs')  Then
Do
  call RxFuncAdd 'RxEdyUcmLoadFuncs',  'RXUCM', 'RxEdyUcmLoadFuncs'
  call RxEdyUcmLoadFuncs
End
```

RxEdyUcmDropFuncs

Simétrica a la anterior, esta función sirve para descargar las funciones de la API de REXX.

```
call RxEdyUcmDropFuncs
```

RxEdyUcmGetError

Esta función obtiene el mensaje de error correspondiente a la última función que ha devuelto un error.

```
say RxEdyUcmGetError()
```

El mensaje de error tiene el siguiente formato:

`ERROR:`*`errorcode`* `SEVERITY:`*`severidad`* `TYPE:`*`tipo`* `MESSAGE:`*`mensaje`*

Donde:

errorcode

Número del error

severidad

Nivel de severidad del error.

Los componentes de SecureEntry siguen el siguiente convenio:

'E' para mensajes de error.

'W' para mensajes de aviso.

'I' para mensajes informativos.

tipo

Tipo del error

Este campo pretende facilitarle la identificación del componente que ha generado el error. Consiste en una cadena de cuatro carácteres; los dos primeros representan el componente que ha detectado el error, mientras que los dos siguientes, el subcomponente. Por ejemplo:

UCSQ indica que el agente de UCM ha encontrado un error de SQL de DB2.

LSER indica que el agente Lan Server ha encontrado un error de la API de Lan Server.

SESR indica que el agente de SecureEntry ha encontrado un error en el Registry de SecureEntry.

RXUC indica que el error se ha producido en la misma RXUCM.DLL.

mensaje

Mensaje de error.

Tenga en cuenta que seguir este convenio no es obligatorio para los componentes. Tenga también en cuenta que no todas las funciones devolverán siempre errores cuyo mensaje asociado pueda ser obtenido con esta función.

RxEdyUcm_AddObj

Esta función añade un nuevo objeto en el repositorio. A continuación se describe la sintaxis.

```
rc=RxEdyUcm_AddObj(subsistema,  tipoDeObjeto, objeto1, objeto2, 'variableDeClaves')
```

Donde:

subsistema

es la identificación del subsistema para seleccionar el agente que procesa la función. Normalmente deberá usar siempre el valor 'SENT' para la administración de SecureEntry.

tipoDeObjeto

Es el tipo de objeto sobre el que se invoca la función.

Los tipos de objetos válidos son:

'GROUP'

'GROUPGROUP'

'RESOURCE'

'RESOURCEGROUP'

'RESOURCEUSER'

'SUBSYSTEM'

'USER'

'USERGROUP'

objeto1

objeto2

Son los identificadores que definen el objeto sobre el que la función se invoca. El parámetro 'objeto2' sólo debe usarse para identificar objetos que se definen por la relación entre dos objetos; en otros casos, debe usarse una cadena de carácteres vacía (").

variableDeClaves

Este es el nombre de un radical (stem) de REXX que se usa para almacenar las palabras claves y los valores asociados del objeto. El elemento 0 se usa para guardar el número de elementos que siguen; el resto tienen la forma 'nombreDeClave=valorDeClave'.

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'WARNING' para operaciones con un código de retorno de aviso.

'ERROR' para errores: la operación no ha podido realizarse.

En caso de obtener un error o un aviso, la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_UpdateObj

Esta función actualiza un objeto del repositorio. A continuación se describe la sintaxis.

```
rc=RxEdyUcm_UpdateObj(subsistema,  tipoDeObjeto,  objeto1,  objeto2,
'variableDeClaves')
```

Donde:

subsistema

es la identificación del subsistema para seleccionar el agente que procesa la función. Normalmente deberá usar siempre el valor 'SENT' para la administración de SecureEntry.

tipoDeObjeto

Es el tipo de objeto sobre el que se invoca la función.

Los tipos de objetos válidos son:

'GROUP'

'GROUPGROUP'

'RESOURCE'

'RESOURCEGROUP'

'RESOURCEUSER'

'SUBSYSTEM'

'USER'

'USERGROUP'

objeto1

objeto2

Son los identificadores que definen el objeto sobre el que la función se invoca. El parámetro 'objeto2' sólo debe usarse para identificar objetos que se definen por la relación entre dos objetos; en otros casos, debe usarse una cadena de carácteres vacía (").

variableDeClaves

Este es el nombre de un radical (stem) de REXX que se usa para almacenar las palabras claves y los valores asociados del objeto. El elemento 0 se usa para guardar el número de elementos que siguen; el resto tienen la forma 'nombreDeClave=valorDeClave'.

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'WARNING' para operaciones con un código de retorno de aviso.

'ERROR' para errores: la operación no ha podido realizarse.

En caso de obtener un error o un aviso, la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_ViewObj

Esta función obtiene un objeto del repositorio. A continuación se describe la sintaxis.

```
variableDeClaves.0 = 0

rc=RxEdyUcm_ViewObj(subsistema, tipoDeObjeto, objeto1, objeto2,
'variableDeClaves')
```

Donde:

subsistema

es la identificación del subsistema para seleccionar el agente que procesa la función. Normalmente deberá usar siempre el valor 'SENT' para la administración de SecureEntry.

tipoDeObjeto

Es el tipo de objeto sobre el que se invoca la función.

Los tipos de objetos válidos son:

'GROUP'

'GROUPGROUP'

'RESOURCE'

'RESOURCEGROUP'

'RESOURCEUSER'

'SUBSYSTEM'

'USER'

'USERGROUP'

objeto1

objeto2

Son los identificadores que definen el objeto sobre el que la función se invoca. El parámetro 'objeto2' sólo debe usarse para identificar objetos que se definen por la relación entre dos objetos; en otros casos, debe usarse una cadena de carácteres vacía (").

variableDeClaves

Este es el nombre de un radical (stem) de REXX que se usa para almacenar las palabras claves y los valores asociados del objeto. El elemento 0 se usa para guardar el número de elementos que siguen; el resto tienen la forma 'nombreDeClave=valorDeClave'.

El valor 0 en el elemento 0 del radical indica que se pide toda la información del objeto. Algunos agentes permiten obtener valores de clave específicos, por lo que es importante que no olvide inicializar el elemento 0 para evitar resultados inconsistentes.

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'WARNING' para operaciones con un código de retorno de aviso.

'ERROR' para errores: la operación no ha podido realizarse.

En caso de obtener un error o un aviso, la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_DeleteObj

Esta función borra un objeto del repositorio. También borra selectivamente claves de un objeto. A continuación se describe la sintaxis.

```
rc=RxEdyUcm_DeleteObj(subsistema,  tipoDeObjeto,  objeto1,  objeto2,
'variableDeClaves')
```

Donde:

subsistema

es la identificación del subsistema para seleccionar el agente que procesa la función. Normalmente deberá usar siempre el valor 'SENT' para la administración de SecureEntry.

tipoDeObjeto

Es el tipo de objeto sobre el que se invoca la función.

Los tipos de objetos válidos son:

'GROUP'

'GROUPGROUP'

'RESOURCE'

'RESOURCEGROUP'

'RESOURCEUSER'

'SUBSYSTEM'

'USER'

'USERGROUP'

objeto1

objeto2

Son los identificadores que definen el objeto sobre el que la función se invoca. El parámetro 'objeto2' sólo debe usarse para identificar objetos que se definen por la relación entre dos objetos; en otros casos, debe usarse una cadena de carácteres vacía (").

variableDeClaves

Este es el nombre de un radical (stem) de REXX que se usa para almacenar las palabras claves y los valores asociados del objeto. El elemento 0 se usa para guardar el número de elementos que siguen; el resto tienen la forma 'nombreDeClave=valorDeClave'.

Puede usar una lista de claves que quiere borrar. Para borrar el objeto en lugar de alguna de sus claves, utilice una cadena de carácteres vacía (").

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'WARNING' para operaciones con un código de retorno de aviso.

'ERROR' para errores: la operación no ha podido realizarse.

En caso de obtener un error o un aviso, la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_SetAgent

Esta función puede usarse durante el desarrollo de agentes específicos de la API para indicarle a la RXUCM.DLL que debe dirigir las peticiones directamente al agente especificado en lugar de utilizar el agente selector. Esto le permite trabajar en un entorno sin SecureEntry previo a la fase de integración. A continuación se describe la sintaxis.

```
rc=RxEdyUcm_SetAgent(idDeAgente)
```

Donde *idDeAgente* es una cadena de dos carácteres que identifica la DLL del agente, que debe llamarse EDYxxAGT.DLL.

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'ERROR' en caso de error; la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_QueryUsersDB

Esta función permite obtener el tipo de base de datos que define los usuarios locales. No requiere parámetros y retorna el identificador del componente que gestiona la base de datos.

```
Locdb=RxEdyUcm_QueryUsersDB()
```

Esta función puede retornar los siguientes valores:

'SR' para el Registry de SecureEntry.

'LS' para el UPM de Lan Server.

'ERROR' en caso de error; la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_Enable_Remote

Esta función habilita o deshabilita el acceso remoto del resto de funciones cuando UCM está presente, independientemente del valor la variable de entorno SGM_UCM_ENABLE. La función sólo tiene efecto para el proceso que la llama. Admite un parámetro que debe valer 0 ó 1. Por ejemplo,

```
Rc=RxEdyUcm_Enable_Remote(0)
```

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'ERROR' en caso de error; la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_Connect

Utilice esta función para notificar al subsistema de administración de que va a empezar a trabajar con la API de administración, de modo que se haga la conexión de DB2 si se requiere acceso al host.

```
Rc=RxEdyUcm_Connect()
```

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'ERROR' en caso de error; la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_Disconn

Utilice esta función para notificar al subsistema de administración de que ha terminado de trabajar con la API de administración, de modo que se haga la desconexión de DB2 si se estableció acceso al host.

```
Rc=RxEdyUcm_Disconn()
```

Esta función puede retornar los siguientes valores:

'OK' para operaciones correctas.

'ERROR' en caso de error; la función RxEdyUcmGetError puede usarse para obtener más información.

RxEdyUcm_GetUser

Esta función permite obtener información sobre el usuario que está conectado. Normalmente no devolverá ningún error.

```
Userinfo=RxEdyUcm_GetUser()
```

El valor retornado puede ser fácilmente analizado, pues tiene el siguiente formato:

```
USER:usuario GROUP:grupo DOMAIN:dominio COMPUTER:máquina ADMIN:x
```

Donde x puede ser 0 ó 1.

La API de 'C'

Equivalente a la API de REXX, está disponible una API para código 'C'. Puede encontrar los archivos de definiciones y librerías en el directorio VíaDeAccesoSecureEntry\API\SOURCES\EDYUCM. También encontrará en este directorio un programa de ejemplo con comentarios; el programa sirve para ver los grupos de primer nivel. A continuación se describe la API y las diferencias con la API de REXX.

Las siguientes funciones están disponibles, y definidas en el archivo EDYSLAGT.H:

EdyUcm_Enable_Remote

Esta función se usa para acceder a la base de datos local incluso si UCM está instalado. El ejemplo muestra su uso habitual:

```
...
Funciones de administración central
...
EdyUcm_Enable_Remote(0)
  ...
  Funciones de administración local
  ...
EdyUcm_Enable_Remote(1)
...
Funciones de administración central
...
```

El efecto de esta función es que el subsistema de administración es informado cuando las funciones de administración han de ser dirigidas a la base de datos local en lugar de la base de datos DB2 del host de UCM.

Tenga en cuenta que el parámetro no modifica un contador recursivo, sino que tiene efecto inmediato.

EdyUcm_Connect

Esta función sólo es necesaria cuando se usa la gestión centralizada (UCM). Su cometido es hacer la conexión DBM a la base de datos. No tiene parámetros. Cuando esta función es necesaria, debe ser llamada antes que cualquier otra función de administración.

EdyUcm_Disconn

Es simétrica a la llamada anterior: sólo es necesaria cuando se usa la gestión centralizada (UCM) y, en caso de ser necesaria, debe ser la última función de administración que se llama antes de que el programa finalice. Tiene un parámetro que determina si el UCM debe guardar (commit) o descartar (rollback) los últimos cambios antes de la desconexión. El valor 0 guarda los cambios mientras que 1 los descarta. Observe que dado que las funciones de UCM funcionan con atomicidad garantizada (autocommit), el parámetro será ignorado por el sistema normalmente. No obstante, le recomendamos que lo utilice con su sentido original (commit/rollback), ya que en el futuro UCM podría proporcionar funciones avanzadas de integridad transaccional.

EdyUcm_AddObj

Esta función, como su equivalente de REXX, se usa para añadir objetos al repositorio. Sus parámetros están explicados en la sección **Definición de parámetros comunes**.

EdyUcm_DeleteObj

Esta función, como su equivalente de REXX, se usa para borrar objetos del repositorio. Sus parámetros están explicados en la sección **Definición de parámetros comunes**.

EdyUcm_UpdateObj

Esta función, como su equivalente de REXX, se usa para modificar, añadir o borrar pares de claves/valor de un objeto definido en el repositorio. Sus parámetros están explicados en la sección **Definición de parámetros comunes**.

EdyUcm_ViewObj

Esta función, como su equivalente de REXX, se usa para obtener la lista de pares de claves/valor de un objeto definido en el repositorio. Sus parámetros están explicados en la sección **Definición de parámetros comunes**.

EdyUcm_FreeMemUcm

Utilice esta función después de llamar a EdyUcmViewObj para liberar los recursos utilizados por ésta.

Definición de parámetros comunes: Parámetros para las funciones EdyUcm_AddObj, EdyUcm_DeleteObj, EdyUcm_UpdateObj y EdyUcm_ViewObj.

Ucm_ObjectType

Tipo de objeto sobre el que se realiza la operación:

USR Usuario

GRP Grupo

RES Recurso

USR_GRP Relación usuario-grupo

RES_USR Relación recurso-usuario

GRP_GRP Relación grupo-grupo

RES_GRP Relación recurso-grupo

*void **

apuntador a la estructura que identifica el objeto. El tipo de la estructura depende del tipo de objeto sobre el que se hace la operación: la estructura es Ucm_*XxxXxx*Data donde *XxxXxx*es el tipo de objeto usado. Esta estructura es siempre un parámetro de entrada, y tiene los siguientes campos:

Subsistema

Es el identificador del subsistema destino. Utilice la cadena 'SENT' para la administración SecureEntry.

identificadores de objetos

Se trata de uno o dos campos que identifican el objeto sobre el que se hace la operación.

Condición

Deje este campo inicializada a ceros si no utiliza UCM. Si utiliza UCM, puede poner el valor de la condición de select SQL que debe aplicarse a la tabla especificada.

unsigned short

Número de definiciones de claves que deben procesarse. Para la función EdyUcm_ViewObj debe ponerlo a cero si quiere obtener todas las claves.

*Ucm_KeyData **

Apuntador a una matriz de estructuras Ucm_KeyData, cada una de las cuales contiene las definiciones de claves. Para la función EdyUcm_ViewObj, puede poner este valor a NULL para obtener todas las claves.

*Ucm_Error **

Apuntador a una estructura, donde se pondrá la información relativa a un posible error.

Nerror Código de error.

Severity Severidad del error, según lo que se indica en el archivo de definiciones ('I','W', 'E','C','S').

Type Tipo de error.

UCSQ UCM: error de SQL. Busque el código de error en el manual de referencia de SQL.

UCAP UCM: error de la API Busque el código de error en el archivo EDYSLAGT.H.

UCME UCM: error de memoria (falta de recursos).

LSER Error de Lan Server. Busque el código de error en la documentación de Lan Sever.

SESR Error del Registry de SecureEntry. Busque el código de error en el archivo EDYERROR.H.

msg

Mensaje

asoc_struc

No se usa actualmente.

Claves válidas

Claves para objetos de tipo USER

LAN_DATA. Los valores de esta clave son pares de (subclave=valor), separados por un carácter '\0', seguido de un '\0' final (este es un formato equivalente al que se usa en las variables de entorno de un programa). El tipo de esta clave debe ser 'A' (ASCII). Las subclave permitidas son:

HOUR_START

inicio del horario en el que se permite la conexión.

HOUR_END

final del horario en el que se permite la conexión.

PRIV_USER

ADMIN,USER, or GUEST. Sólo para entornos Lan Server.

FULL_NAME

Nombre completo.

CONNECTION

1 (permitida), 0 (no permitida).

USER_EXPIRE

NEVER, o dia-mes-año.

DESCRIPTION

Descripción en formato libre.

PASSWORD

Contraseña, sólo válida como subclave de entrada.

PASSWD_EXPIRED

1 (expirar la contraseña), 0 (no expirarla)

HOME_DIR

\\NombreDeMaquina\x$\ViaDeAcceso, o x:\NombreDeMáquina\x$\ViaDeAcceso. Sólo para entornos Lan Server.

MAX_STORAGE

Tal como lo requiere Lan Server. -1=sin límite. Sólo para entornos Lan Server.

SCRIPT_PATH

Tal como lo requiere Lan Server. Sólo para entornos Lan Server.

Cualquier otro valor. Se considera que la clave es el identificador de un componente de seguridad de SecureEntry, tal como se especifica en el archivo SENTRY.DSC del directorio ViaDeAccesoSecureEntry\INSTALL. El tipo esperado es 'B' (binario), y los valores son áreas de memoria con una copia del perfil de seguridad correspondiente precedida por un LONG de valor 4.

Claves para objetos de tipo GROUP

LAN_DATA. Los valores de esta clave son pares de (subclave=valor), separados por un carácter '\0', seguido de un '\0' final (este es un formato equivalente al que se usa en las variables de entorno de un programa). El tipo de esta clave debe ser 'A' (ASCII). Las subclave permitidas son:

FULL_NAME

Nombre completo.

CONNECTION

1 (permitida), 0 (no permitida).

USER_EXPIRE

NEVER, o dia-mes-año.

DESCRIPTION

Descripción en formato libre.

Cualquier otro valor. Se considera que la clave es el identificador de un componente de seguridad de SecureEntry, tal como se especifica en el archivo SENTRY.DSC del directorio ViaDeAccesoSecureEntry\INSTALL. El tipo esperado es 'B' (binario), y los valores son áreas de memoria con una copia del perfil de seguridad correspondiente precedida por un LONG de valor 4.

Claves para objetos de tipo RESOURCE

Este tipo de objetos sólo está soportado en entornos Lan Server. Todas las claves definidas son de tipo 'A' (ASCII). El identificador de los objetos de este tipo el el nombre del alias.

SERVER

Nombre del servidor.

TYPE

FILES, TREE, PRINTER o SERIAL.

WHEN_SHARED

STARTUP, BYADMIN, o DYNAMIC.

RESNAME

Nombre del recurso.

DESCRIPTION

Descripción en formato libre.

MAX_CONN

Número de conexiones simultáneas permitidas.

Claves para objetos de tipo RESOURCEGROUP y RESOURCEUSER

Este tipo de objetos sólo está soportado en entornos Lan Server. Todas las claves definidas son de tipo 'A' (ASCII).

ACCESS

Tipo de acceso. Por ejemplo, RWX.

LOGON_ASN

Nombre de dispositivo al que se asigna el recurso.

Claves para objetos de tipo USERGROUP y GROUPGROUP

Sin claves definidas.

Listado de objetos

Si quiere un listado de los objetos existentes de un tipo determinado puede utilizar la función EdyUcm_ViewObj utilizando '*' como un identificador de objeto. Se generará una lista de todos los objetos que cumplen el criterio especificado; esta lista se devuelve en el arreglo de claves.

Una excepción a esta regla se da para listar usuarios o grupos. Para acceder a listas de usuarios o grupos en cualquier entorno, debe ver las listas correspondientes de objetos de tipo USERGROUP o GROUPGROUP, tal como se muestra en el archivo de ejemplo LISTGRP.C.

Información adicional:

Notificación de errores: los errores se devuelven en cada función a través de la estructura de error que se pasa como parámetro (Ucm_Error). El código de retorno para las funciones EdyUcm_xxxObj cumple las siguiente reglas:

Rc=0 Función procesada correctamente.

Rc<0 Error. La función no se ha realizado. La estructura de error contiene más información.

Rc>0 Aviso. La función se ha realizado, pero se ha detectado una condición inesperada. La estructura de error contiene más información.

Inicialice siempre las estructuras antes de invocar una función. Si no se indica lo contrario, todos los campos deben valer cero. Esto incluye las estructuras de error Ucm_Error y las estructuras de claves Ucm_KeyData.

Libere la memoria utilizada por el arreglo de estructuras Ucm_KeyData que la función EdyUcm_FreeMemUcm retorna. Utilice la función EdyUcm_FreeMemUcm para este cometido.

La indirección a través del carácter '@' no está soportada por la API de 'C'. Tal como se explica en la sección **Claves válidas**, los perfiles de seguridad deben pasarse en memoria.

El paso de minúsculas a mayúsculas y la supresión de blancos es su responsabilidad cuando utilice la API de 'C'.

Debe linkeditarse con la DLL EDYSLAGT para trabajar con la API de 'C'.

Utilidades para OS/2

SecureEntry le da distintas utilidades para facilitarle la implementación de su solución de seguridad. En este capítulo se describen aquellas que se ejecutan en OS/2 nativo.

Lanzador de eventos de sesión: EDYUTIL

Visualización de información sobre el usuario: EDYUSINF

Gestión de las clases de WPS de Lan server: WPSLAN

Utilidad de Lista de Tareas: EDYSWL2

Gestor de semáforos: EDYSEM2

Cierre selectivo de aplicaciones: EDYCLOSE

Gestión de emuladores de CM/2: EDYE3270

Salvaguarda del sector de arranque: EDYRWMBR

Lanzador de eventos de sesión: EDYUTIL

Este programa le permite arrancar distintos eventos de sesión. También sirve para preparar los valores de los parámetros de los siguientes eventos de conexión y desbloqueo.

La sintaxis de invocación del programa es la siguiente:

```
EDYUTIL TOLOCKUP | TOLOGOFF | FRLOGOFF | REBOOT
        TOSHTDWN [REBOOT] |
        FRSHTDWN [REBOOT] |
        NEXTLOGON [/CLEAR | /ASK /U:usuario /P:contraseña
                   /N:nuevaContraseña /D:dominio] |
        NEXTUNLOCK [/CLEAR | /ASK /U:usuario|NO
                   /V:contraseñaDeValidación|NO /P:contraseña] |
        SIGNAL "aString" |
        SUPERSIGNAL "aString"
```

TOLOCKUP

Lanza un evento de bloqueo.

TOLOGOFF

Lanza un evento de desconexión.

FRLOGOFF

Lanza un evento de desconexión forzada (no cancelable).

REBOOT

Lanza un evento para rearrancar la máquina.

TOSHTDWN

Lanza un evento de concluir. Añada el parámetro REBOOT para rearrancar la máquina una vez concluir ha terminado.

FRSHTDWN

Lanza un evento de concluir forzado (no cancelable). Añada el parámetro REBOOT para rearrancar la máquina una vez concluir ha terminado.

NEXTLOGON

Especifica los parámetros de la siguiente conexión. Este parámetro debe ir seguido uno de los siguientes parámetros:

/CLEAR para borrar los parámetros que hayan sido especificados anteriormente.

Uno o más de los siguientes parámetros:

/U: para especificar el usuario de la siguiente conexión.

/P: para especificar la contraseña de la siguiente conexión.

/D: para especificar el dominio de la siguiente conexión.

/N: para especificar una nueva contraseña en la siguiente conexión.

/ASK para hacer que se presente el diálogo de conexión antes de intentar hacer la conexión. Si no se especifica, la conexión se intentará realizar con los parámetros especificados a través de esta llamada. Si se especifica, el usuario tendrá ocasión de modificar los parámetros especificados.

NEXTUNLOCK

Especifica el usuario y la contraseña de desbloqueo en la sesión de usuario actual, y, opcionalmente, especificar el valor del campo de contraseña del diálogo de desbloqueo. Este parámetro debe ir seguido uno de los siguientes parámetros:

/CLEAR para borrar los parámetros que se hayan especificado anteriormente.

Uno o más de los siguientes parámetros:

/U: para especificar el usuario en el campo informativo del diálogo de desbloqueo, o NO para que no aparezca.

/V: para especificar la contraseña válida que debe usarse en el siguiente diálogo de desbloqueo.

/P: para especificar la contraseña que aparecerá en el campo correspondiente del diálogo de desbloqueo.

/ASK para hacer que se presente el diálogo de desbloqueo durante el bloqueo. Si no se especifica y el campo de la contraseña (parámetro /P) ha sido especificado, se intentará el desbloqueo con esta contraseña.

SIGNAL

Para invocar la exit de usuario de señalización (UserExitSignal) con el parámetro aString.

SUPERSIGNAL

Para invocar la exit de usuario de señalización en contexto de superusuario (UserExitSignalSuperUser) con el parámetro aString.

Los parámetros de conexión o desbloqueo (especificados mediante los parámetros principales NEXTLOGON o NEXTUNLOCK) pueden notificarse incluso en las exits de usuario previas a los diálogos de conexión y desbloqueo. Esto facilita el uso de sus propios diálogos en lugar de los de SecureEntry. Si utiliza sus propios diálogos en una exit de usuario debe tener en cuenta que estos deben ser modales de sistema (system modal).

Por otra parte, estas funciones permiten la identificación de usuarios con mecanismos de entrada de datos distintos al teclado.

Este programa se proporciona no solamente como una herramienta, sino también como un programa ejemplo de cómo pueden ser invocadas estas funciones desde su aplicación. En el directorio VíaDeAccesoSecureEntry\API\SOURCES\EDYFLOW encontrará tanto los archivos fuente del programa EDYUTIL.EXE como las definiciones y librerías de la API para lanzar eventos de sesión.

Observe que este programa ejecuta los eventos de manera asíncrona, con lo que devolverá el control **antes** de que la función se haya procesado.

Esta utilidad se encuentra en el directorio *VíaDeAccesoSecureEntry*\EXEC.

ADVERTENCIAS IMPORTANTES

Esta utilidad no puede usarse durante el arranque de la máquina mientras que SecureEntry no esté inicializado para procesar eventos de sesión. El sistema puede considerarse apto para lanzar eventos a partir de que se lanza la exit de usuario posterior al arranque (UserExitAfterStartup).

Los eventos de sesión están serializados por la arquitectura del SES. Esto significa que no podrá utilizar este programa para lanzar un evento mientras se está procesando un evento de SES. Por ejemplo, no puede lanzar un evento de desconexión o concluir desde una exit de usuario causada por un evento de SES; en estas circunstancias, puede forzar estos eventos con el código de retorno apropiado. Una excepción a la regla que impide lanzar eventos mientras otro evento tiene lugar se dá cuando se están mostrando los diálogos de conexión y desbloqueo: entonces, SecureEntry le permite que EDYUTIL sea invocado para forzar la desconexión o concluir.

Visualización de información sobre el usuario: EDYUSINF

Esta utilidad muestra el usuario conectado, su grupo, dominio, servidor, máquina y si se trata de un administrador.

La sintaxis de invocación del programa es la siguiente:

```
EDYUSINF
```

Los datos se muestran como en el siguiente ejemplo:

```
USER:USERID
GROUP:
DOMAIN:SEDOMAIN
SERVER:\\SESRV01
ADMIN:YES
COMPUTER:SESRV01
```

Esta utilidad se encuentra en el directorio *VíaDeAccesoSecureEntry*\TOOLS.

Clases de WPS de Lan Server : WPSLAN

Lan Server instala sus propias clases de WPS que añaden entradas de menú en la mayoría de objetos del sistema. Si quiere que estas entradas de menú no aparezcan puede desinstalar las clases de Lan Server. Esta utilidad le permite desinstalar (desregistrar) o instalar (registrar y reemplazar) estas clases.

La sintaxis de invocación del programa es la siguiente:

```
WPSLAN /U   (para desregistrar las clases de Lan Server)
WPSLAN /I   (para registrar y remplazar las clases de Lan Server)
```

Esta utilidad se encuentra en el directorio *VíaDeAccesoSecureEntry*\TOOLS.

Utilidad de Lista de Tareas: EDYSWL2

Si quiere obtener *ayuda en línea* sobre esta utilidad, teclee:

```
EDYSWL2
```

Esta utilidad da acceso a la Lista de Tareas (List de Ventanas) del OS/2 y las entradas que contiene, incluso si son invisibles. Su uso permite la gestión de las sesiones.

Los archivos de esta utilidad se encuentra en el directorio *VíaDeAccesoSecureEntry*\TOOLS. La sintaxis de este comando es:

```
EDYSWL2  [acción:sesión]
```

acción

La acción a realizar sobre la sesión especificada. Puede tomar los siguientes valores:

HIDE Elimina la sesión de la Lista de Tareas.

KILL Mata el proceso que se está ejecutando en la sesión.

SHOW Añade la sesión a la Lista de Tareas.

SWITCHTO Da el control a la sesión.

LIST Visualiza la lista de sesiones. Para esta última acción no debe especificarse ninguna sesión.

MINIWIN Minimiza todas las ventanas de la sesión.

HIDEWIN Esconde todas las ventanas de la sesión.

RESTWIN Restaura todas las ventanas de la sesión.

MAXIWIN Maximiza todas las ventanas de la sesión.

ACTIWIN Activa todas las ventanas de la sesión.

DEACWIN Desactiva todas las ventanas de la sesión.

CLOSWIN Cierra todas las ventanas de la sesión.

Tenga en cuenta que las acciones *WIN se hacen sobre las ventanas y no sobre las entradas de la lista de tareas, y que se hacen de modo asíncrono (rc=0 indica únicamente que se ha enviado el mensaje para que la acción tenga lugar).

sesión

Sesión sobre la que se ejecutará la acción especificada. El valor de este parámetro puede ser especificado de formas distintas:

HSWL:*manejador*

Donde *manejador* (handle) es el manejador para la Lista de Tareas de la sesión en base hexadecimal.

PID:*pid*

Donde *pid* es el ID de proceso en base hexadecimal.

SESSID:*IDsesión*

Donde *IDsessión* es el ID de sesión en base hexadecimal.

SLINDEX:*index*

Donde *index* es el índice de la sesión dentro de la Lista de Tareas en base decimal.

TITLE:*título*

Donde *título* es el título de sesión.

Los carácteres blancos y de control deben ser sustituídos por el carácter de subrayado '_' Observe que la secuencia de carácteres (CR)(LF) requiere dos carácteres de subrayado.

Gestor de semáforos: EDYSEM2

Si quiere obtener *ayuda en línea* sobre esta utilidad, teclee:

```
EDYSEM2
```

Esta utilidad proporciona acceso a los semáforos de OS/2 desde una línea de comandos. Permite sincronizar procesos entre distintas sesiones.

La sintaxis para este comando es:

```
EDYSEM2 [Post|Wait] NombreSem
```

Post

Abre, si ya existe, el semáforo de eventos de OS/2 llamado \SEM32\NombreSem, y le lanza (post) un evento. Si el semáforo no existe se espera hasta que éste sea creado.

Wait

Abre, o crea si no existe, el semáforo de eventos de OS/2 llamado \SEM32\NombreSem, y se espera hasta que se lance un evento sobre el semáforo.

NombreSem

Nombre del semáforo. No se distinguen mayúsculas y minúsculas en el valor de este parámetro.

SecureEntry también proporciona la utilidad EDYSEMV, que da la misma funcionalidad a partir de los mismos parámetros, pero que se ejecuta desde una VDM.

La utilidad EDYSEM2 puede ser parada si se teclea Ctrl-C. La utilidad EDYSEMV no soporta esta característica.

Cierre selectivo de aplicaciones: EDYCLOSE

Esta utilidad le permite el cierre de las aplicaciones después de algún evento.

Los ejecutables que componen esta utilidad se encuentran en el directorio VíaDeAccesoSecureEntry\TOOLS Se intentarán cerrar todas las aplicaciones excepto aquellas que estén especificadas en un archivo de configuración.

Cuando se ejecuta EDYCLOSE, se lee el archivo INI de configuración y las aplicaciones que **no** están especificadas y aparecen en la lista de tareas se cierran. No se cierra la sesión en la que se ejecuta EDYCLOSE. Si no se encuentra el archivo de configuración, no se cierra ninguna sesión. Para cerrar las sesiones, se utiliza la función DosKillProcess.

La sintaxis para este comando es:

```
EDYCLOSE [VíaDeAcceso]NombreDeArchivo[.INI]
```

VíaDeAcceso

Vía de acceso del archivo de configuración. Si se omite, se utiliza el directorio activo.

NombreDeArchivo

Nombre del archivo INI de configuración donde se especifican las aplicaciones que no deben cerrarse. El nombre por omisión es **EDYCLOSE**.

Puede utilizar esta herramienta para cerrar aplicaciones desde una exit de usuario o desde una de sus aplicaciones. Tenga en cuenta que el uso de esta herramienta para cerrar las aplicaciones de usuario no es necesario durante la desconexión, puesto que SecureEntry las cierra automáticamente.

Editor del archivo de configuración de cierre selectivo

Para crear los archivos de configuración de EDYCLOSE, puede utilizar el programa EDYEDTCL.

La sintaxis para este comando es:

```
EDYEDTCL [VíaDeAcceso]NombreDeArchivo[.INI]
```

VíaDeAcceso

Vía de acceso del archivo de configuración. Si se omite, se utiliza el directorio activo.

NombreDeArchivo

Nombre del archivo INI de configuración donde se especifican las aplicaciones que no deben cerrarse. El nombre por omisión es **EDYCLOSE**.

Los campos de este editor son

Nombre

Identifica la aplicación que no debe cerrarse. El nombre debe coincidir con una entrada de la lista de tareas.

Para especificar una ventana correspondiente a un objeto WPS cuyo título tiene más de una línea, separe las líneas con los carácteres \n. Por ejemplo, Visor de ventanas\nMinimizadas

Una vez haya especificado el nombre, añádalo en la Lista con el botón Añadir. Especifique todas las aplicaciones que no deben ser cerradas.

Lista

Contiene los nombres de todas las aplicaciones que no deben cerrarse. Puede suprimir elementos de la lista con el botón Eliminar.

Gestión de emuladores de CM/2: EDYE3270

Esta utilidad le permite controlar el arranque y la parada de sesiones de emulación de CM/2 a través de la línea de comandos. Está pensado para ser invocado desde las exits de usuario, de manera que las sesiones de emulación se abran durante la conexión y se cierren en desconexión.

La sintaxis para este comando es:

```
EDYE3270 START  para arrancar las sesiones configuradas
EDYE3270 STOP   para parar las sesiones configuradas
EDYE3270 SWITCH para cambiar el estado de las sesiones configuradas
```

Esta utilidad se encuentra en el directorio *VíaDeAccesoSecureEntry*\TOOLS.

Si sus emuladores no utilizan el soporte de CM/2, sino el del Access Feature (AF) vía Personal Communications (PCOM), entonces deberá usted prescindir de la utilidad EDYE3270 y usar las propias del PCOM como sigue:

```
PCSWS    nombre.WS      para arrancar la sesión configurada en el archivo nombre.WS
PCSBAT   nombre.BCH /R  para arrancar el conjunto de sesiones configuradas en el
                        archivo nombre.BCH
PCSSTOP                 para detener las sesiones arrancadas
```

La detención de las sesiones arrancadas de los emuladores la efectuará SecureEntry automaticamente si así la tiene identificada en el archivo EDYKILL.NOT, que actualmente ya da este soporte.

Remítase a Archivos de configuración y lea la sección de comentarios de dicho archivo para obtener más información sobre él. Remítase a la publicación *Personal Communications v4.2 Quick Beginnings* para obtener más información sobre la gestión de emuladores usando PCOM.

Salvaguarda del sector de arranque: EDYRWMBR

Todos los sistemas están expuestos a virus o a otras incidencias que puede hacer que pueda perder la capacidad de arranque. SecureEntry le da la posibilidad de restaurar el sector de arranque (MBR, o Master Boot Record) original si algún evento externo lo daña. Esto puede hacerse aunque no se utilice la protección de arranque vía software de SecureEntry.

Para el uso de esta utilidad, le recomendamos generar una copia de sus sectores de arranque en el último de los disquetes de arranque de OS/2, de manera que pueda restaurar los sectores arrancando desde disquetes cuando no es posible arrancar desde el disco duro.

Haga una copia de seguridad de los sectores de arranque originales:

```
EDYRWMBR.EXE /R [/FvíaDeAcceso]
donde: /R     lee los sectores originales de los discos físicos
```

```
/FvíaDeAcceso graba los archivos que contienen los sectores en
              la víaDeAcceso especificada. Por omisión, se usa
              el directorio activo.
```

Se crea un archivo para cada disco físico del sistema. El nombre de los archivos es EDYBOOT, y la extensión 001 para el primer disco físico, 002 para el segundo, y así sucesivamente. Por ejemplo, en un sistema con dos discos físicos, el comando

```
EDYRWMBR /R /Fa:
```

grabará los archivos EDYBOOT.001 y EDYBOOT.002 en el disco A:.

Si la protección de arranque vía software está instalada, los archivos contendrán los sectores de arranque originales. En caso contrario, los archivos contendrán los sectores de arranque tal como estén en ese momento.

Si los archivos destino ya existen serán sobreescritos.

Los archivos no se crearán si los sectores no son válidos.

Restaurar una copia de seguridad de los sectores de arranque:

```
EDYRWMBR.EXE /W [/Pcontraseña] [/FvíaDeAcceso]

donde: /W   copia los archivos de sectores sobre los discos físicos.
/Ppassword  necesario si la protección de arranque vía software
            está instalada.
/Fpath_name obtiene los archivos que contienen los sectores en la
            víaDeAcceso especificada. Por omisión, se usa el directorio
            Activo.
```

Si la protección de arranque vía software está instalada y los archivos con las copias de seguridad están en el directorio activo, puede restaurar los sectores originales con el comando

```
EDYRWMBR /W /Pxxxx
```

Si la protección de arranque vía software no está instalada y los archivos con las copias de seguridad están en la unidad A:, puede restaurar los sectores de la copia de seguridad con el comando

```
EDYRWMBR /W /Fa:
```

Puesto que este comando se usará cuando el sistema no pueda arrancar, utilizará una estrategia de 'hacer lo que se pueda', con lo que se harán las mínimas comprobaciones de los sectores de arranque actuales.

Utilidades para la Máquina Virtual de DOS

Para poder ejecutar programas de DOS en el entorno de máquina virtual de DOS que proporciona el OS/2 (VDMs) es necesario hacer algunos cambios en el entorno de proceso de estos programas.

OS/2 es una plataforma multitarea que los programas DOS pueden aprovechar. Es decir, distintos programas DOS pueden estar ejecutándose a la vez en entornos privados sobre diferentes VDMs.

SecureEntry proporciona una serie de programas orientados a facilitar los esquemas de sincronización que requiere un entorno multitarea:

Lanzador VDM de programas : EDYSTRTV

Para lanzar programas de OS/2 desde una VDM.

Lanzador VDM de comandos NET : EDYNETV

Para ejecutar comandos de red desde una VDM.

Utilidad VDM de Lista de Tareas : EDYSWLV

Para acceder a la lista de tareas del OS/2 desde una VDM.

Controlador VDM de cambio de sesión : EDYBRNGV

Para traer a primer plano un programa de OS/2 desde una VDM.

controlador VDM de semáforos : EDYSEMV

Para poder trabajar con semáforos de OS/2 desde una VDM.

Los ejecutables correspondientes a estos programas residen en el subdirectorio TOOLS de su directorio de SecureEntry.

Lanzador VDM de programas : EDYSTRTV

Si quiere obtener *ayuda en línea* para este comando, teclee:

```
EDYSTRTV
```

Esta utilidad arranca programas de OS/2 desde una VDM. La ruta hasta el programa CMD.EXE debe estar especificada en la sentencia PATH del archivo CONFIG.SYS del OS/2.

La sintaxis de este comando es:

```
EDYSTRTV [/S:TipoSesión] [/F:ModoSesión] [/T:TítuloSesión]
         [/D:ValoresDOS] [/X:PosXVen] [/Y:PosYVen] [/W:Anchura]
         [/H:Altura] NombrePrograma ParamsPrograma
```

TipoSesión

Se soportan los siguientes tipos de sesión:

1 Pantalla completa de OS/2

2 Ventana de OS/2

3 Presentation Manager de OS/2

4 Virtual DOS machine (DOS VDM o WINOS2 VDM)

7 Ventana VDM

El valor por defecto es **1**.

ModoSesión

Se soportan los siguientes modos de sesión:

0 Primer plano

1 Segundo plano

El valor por defecto es **1**.

TítuloSesión

El título de sesión puede ser cualquier cadena de carácteres.

Los carácteres blancos y de control deben ser sustituídos por el carácter de subrayado '_' Observe que la secuencia de carácteres (CR)(LF) requiere dos carácteres de subrayado.

DOSsettings

Los valores de DOS deben estar separados por el carácter ;. Se puede especificar también un archivo que contenga los valores mediante @nombre_archivo.

PosXVen

Coordenada horizontal de la posición de la ventana.

PosYVen

Coordenada vertical de la posición de la ventana.

Anchura

Anchura de la ventana.

Altura

Altura de la ventana.

NombrePrograma

Nombre del programa a arrancar.

Los carácteres blancos y de control deben ser sustituídos por el carácter de subrayado '_' Observe que la secuencia de carácteres (CR)(LF) requiere dos carácteres de subrayado.

ParamsPrograma

Parámetros de entrada del programa a arrancar.

Lanzador VDM de comandos NET : EDYNETV

Si quiere obtener *ayuda en línea* sobre esta utilidad, teclee:

```
EDYNETV
```

Esta utilidad ejecuta comandos de NET de OS/2 desde una VDM.

Para obtener información sobre el comando NET de OS/2, teclee:

```
EDYNETV HELP
```

No se soportan comandos NET interactivos. Tampoco se soporta la redirección de la entrada (como por ejemplo cuando se usa el comando SEND) ni los nombres completos de archivo (como por ejemplo, cuando se usa el comando COPY).

Se requieren las siguientes condiciones:

Debe estar instalada la API de soporte para LAN sobre VDMs del IBM LAN Server.

El programa IBM LAN Requester tiene que estar activo.

El usuario de SecureEntry tiene que estar conectado.

Las rutas de acceso a NET.EXE y a EDYSEM2.EXE deben estar especificada en la sentencia PATH del archivo CONFIG.SYS del OS/2.

La sintaxis de este comando es:

```
EDYNETV [ MACH | USE SpecsRedirección ]
```

MACH

Devuelve el ID de máquina.

USE

Si no se especifica ningún parámetro de redirección, devuelve la lista de todos los dispositivos y unidades redireccionadas.

Se puede especificar lo siguiente:

dev \\servidor\nombredered [contraseña]

Redirecciona el dispositivo.

d: \\servidor\nombredered [contraseña]

Redirecciona la unidad.

dev /D

Finaliza la redirección de un dispositivo.

Cualquier otra especificación se pasa tal cual a la sesión de OS/2 en la que se esté ejecutando el programa NET.EXE.

Utilidad VDM de Lista de Tareas : EDYSWLV

Si quiere obtener *ayuda en línea* sobre esta utilidad, teclee:

```
EDYSWLV
```

Esta utilidad proporciona acceso a la Lista de Tareas del OS/2, saltándose las restricciones de visibilidad que se hayan establecido para éstas entradas. Permite gestionar sesiones desde una VDM.

Las rutas de acceso a CMD.EXE y a EDYSWL2.EXE deben estar especificadas en la sentencia PATH del archivo CONFIG.SYS del OS/2.

La sintaxis de este comando es:

```
EDYSWLV  [acción:sesión]
```

acción

La acción a realizar sobre la sesión especificada. Puede tomar los siguientes valores:

HIDE

Elimina la sesión de la Lista de Tareas.

KILL

Mata el proceso que se está ejecutando en la sesión.

SHOW

Añade la sesión a la Lista de Tareas.

SWITCHTO

Da el control a la sesión.

LIST

Visualiza la lista de sesiones. Para esta última acción no debe especificarse ninguna sesión.

MINIWIN

Minimiza todas las ventanas de la sesión.

HIDEWIN

Esconde todas las ventanas de la sesión.

RESTWIN

Restaura todas las ventanas de la sesión.

MAXIWIN

Maximiza todas las ventanas de la sesión.

ACTIWIN

Activa todas las ventanas de la sesión.

DEACWIN

Desactiva todas las ventanas de la sesión.

CLOSWIN

Cierra todas las ventanas de la sesión.

sesión

Sesión sobre la que se ejecutará la acción especificada. El valor de este parámetro puede ser especificado de formas distintas:

HSWL:*manejador (handle)*

Donde *manejador* es el manejador para la Lista de Tareas de la sesión en base hexadecimal.

PID:*pid*

Donde *pid* es el ID de proceso en base hexadecimal.

SESSID:*IDsesión*

Donde *IDsesión* es el ID de sesión en base hexadecimal.

SLINDEX:*index*

Donde *index* es el índice de la sesión dentro de la Lista de Tareas en base decimal.

TITLE:*título*

Donde *título* es el título de sesión.

Los carácteres blancos y de control deben ser sustituídos por el carácter de subrayado '_' Observe que la secuencia de carácteres (CR)(LF) requiere dos carácteres de subrayado.

Nota : para que esta utilidad funcione correctamente, su utilidad gemela EDYSWL2 debe residir en uno de los directorios especificados en la sentencia PATH.

Controlador VDM de cambio de sesión : EDYBRNGV

Si quiere obtener *ayuda en línea* sobre esta utilidad, teclee:

```
EDYBRNGV
```

Esta utilidad permite traer programas que se están ejecutando a primer plano. Si el programa especificado no se está ejecutando, se arranca y se trae a primer plano. Las rutas de acceso a CMD.EXE y a EDYSWL2.EXE deben estar especificadas en la sentencia PATH del archivo CONFIG.SYS del OS/2.

Tanto los programas de DOS como los de OS/2 pueden residir en cualquier lugar del sistema de archivos, sin embargo, si sus rutas de acceso no están especificados en la sentencia PATH, o en el caso de los programas DOS, si estos no residen en el directorio actual, entonces debe proporcionarse la ruta de acceso completa al programa.

La sintaxis para este comando es:

```
EDYBRNGV [/S:TipoSesión] [/F:ModoSesión] [/T:TítuloSesión]
         [/D:ValoresDOS] [/X:PosXVen] [/Y:PosYVen] [/W:Anchura]
         [/H:Altura] NombrePrograma ParamsPrograma
```

TipoSesión

Se soportan los siguientes tipos de sesión:

1 Pantalla completa de OS/2

2 Ventana de OS/2

3 Presentation Manager de OS/2

4 Virtual DOS machine (DOS VDM o WINOS2 VDM)

7 Ventana VDM

El valor por defecto es **1**.

ModoSesión

Se soportan los siguientes modos de sesión:

0 Primer plano

1 Segundo plano

El valor por defecto es **1**.

TítuloSesión

El título de sesión puede ser cualquier cadena de carácteres.

Los carácteres blancos y de control deben ser sustituídos por el carácter de subrayado '_' Observe que la secuencia de carácteres (CR)(LF) requiere dos carácteres de subrayado.

DOSsettings

Los valores de DOS deben estar separados por el carácter ;. Se puede especificar también un archivo que contenga los valores mediante @nombre_archivo.

PosXVen

Coordenada horizontal de la posición de la ventana.

PosYVen

Coordenada vertical de la posición de la ventana.

Anchura

Anchura de la ventana.

Altura

Altura de la ventana.

NombrePrograma

Nombre del programa a arrancar.

Los carácteres blancos y de control deben ser sustituídos por el carácter de subrayado '_' Observe que la secuencia de carácteres (CR)(LF) requiere dos carácteres de subrayado. Para especificar un programa CMD, el valor del parámetro debe ser:

```
CMD.EXE /C nombrearchivo.CMD
```

ParamsPrograma

Parámetros de entrada del programa a arrancar.

Gestor VDM de semáforos : EDYSEMV

Si quiere obtener *ayuda en línea* sobre esta utilidad, teclee:

```
EDYSEMV
```

Esta utilidad proporciona acceso a los semáforos de OS/2 desde una VDM. Está pensado para facilitar la sincronización de procesos entre VDMs o entre VDMs y sesiones OS/2.

La sintaxis para este comando es:

```
EDYSEMV [Post|Wait] NombreSem
```

Donde :

Post

Abre, si ya existe, el semáforo de eventos de OS/2 llamado \SEM32\NombreSem, y le lanza (post) un evento. Si el semáforo no existe se espera hasta que éste sea creado.

Wait

Abre, o crea si no existe, el semáforo de eventos de OS/2 llamado \SEM32\NombreSem, y se espera hasta que se lance un evento sobre el semáforo.

NombreSem

Nombre del semáforo. No se distinguen mayúsculas y minúsculas en el valor de este parámetro.

SecureEntry también proporciona la utilidad EDYSEM2, que da la misma funcionalidad a partir de los mismos parámetros, pero que se ejecuta sobre OS/2.

La utilidad EDYSEM2 puede ser parada si se teclea Ctrl-C. La utilidad EDYSEMV no soporta esta característica.

Utilidades SecureEntry de Mantenimiento

SecureEntry proporciona también un conjunto de utilidades para su propio mantenimiento, además de otras de uso general en el sistema. El propio SecureEntry utiliza algunas de ellas en distintas situaciones, pero puede ser interesante conocerlas de cara a solucionar problemas o defectos es situaciones concretas.

Borrando directorios con EDYDD

Desempaquetando archivos de instalación usando UNPACK32

Actualizando las definiciones de la base de datos de SecureEntry con UPDATEDB

Regenerando una base de datos de SecureEntry con CREADB

Registrando clases de WPS con EDYCLASS

Arreglando archivos INI de OS/2 vía EDYCLINI

Instalando DLLs de PM con EDYWINI

Regenerando la carpeta de trabajo de SecureEntry usando EDYCRWRK

Estableciendo enlaces a la red SecureEntry con EDYSRV y EDYFREE

Migrando definiciones de SecureEntry 2.0 usando MIGRADB

Controlando el tamaño de los archivos de anotaciones usando EDYLOGFS

Examinando los archivos de anotación con EDYLOGBR

Obteniendo y visualizando archivos de fotografías con EDYPHOTO

ATENCION! El uso incorrecto de algunas de estas utilidades puede dejar su sistema en un estado inestable/inútil.

EDYDD

El programa EDYDD es una utilidad de 'borrar directorio' genérica. Borra el contenido del directorio especificado y todos sus descendientes, sin tener en cuenta la existencia de archivos marcados de sólo lectura. Este programa reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

El formato de esta utilidad es:

```
EDYDD NombreDeDirectorio [/N]
```

NombreDeDirectorio

El camino completo al directorio a borrar

/N

Use este parámetro para evitar preguntas de confirmación

UNPACK32

El programa UNPACK32.EXE se usa para obtener un componente dado a partir de un disquete de instalación comprimido. SecureEntry lo usa internamente durante el proceso de instalación o servicio. Su sintaxis es idéntica que la del programa UNPACK2.EXE proporcionado con el OS/2 de base. Remítase a la documentación del OS/2 para obtener más información. Este programa reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

UPDATEDB

Éste programa sirve para actualizar características estáticas de la base de datos de SecureEntry, tales como el tiempo de caducidad de las contraseñas o la adición de nuevos componentes a la tabla de componentes ya existentes. Remítase al capítulo 'Añadiendo sus propios componentes' para obtener instrucciones sobre su uso. El programa reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

CREADB

Éste programa se usa durante la instalación para crear una base de datos SecureEntry de componentes y usuarios vacía. Este programa toma como entrada el nombre de un subsistema y un archivo de descripción de componentes. Reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

La sintaxis de este comando es:

```
CREADB NombreDeSubsistema  ArchivoDeConfiguración
```

NombreDeSubsistema

Nombre del subsistema a crear. El único valor soportado es SENTRY

ArchivoDeConfiguración

Camino y nombre del archivo de configuración. El usado por el programa de instalación de SecureEntry es la vía de acceso SecureEntry, INSTALL\SENTRY.DSC

EDYCLASS

SecureEntry utiliza ésta utilidad para registrar/desregistrar las clases de SOM SecureEntry requeridas. Generalmente, no es necesario usar este comando manualmente, puesto que el producto tiene en cuenta el registro de las clases necesarias en el momento de reiniciar el sistema. Este programa reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

La sintaxis de este comando es:

```
EDYCLASS /I | /U [PerfilBinario]
```

/I

Para registrar las clases SecureEntry.

/U

Para desregistrar las clases SecureEntry. Especifique opcionalmente un perfil de restricciones del Escritorio que defina los valores de los objetos establecidos por defecto.

EDYCLINI

Este programa se puede usar para mantener y limpiar los archivos de inicialización del sistema OS2.INI y OS2SYS.INI. Este programa debe ser usado con sumo cuidado, puesto que puede destruir los valores establecidos de su sistema o provocar un funcionamiento defectuoso.

ATENCION: DEBE ESTAR ABSOLUTAMENTE SEGURO DE LO QUE HACE!!!!!

```
EDYCLINI [Modo de Operación] [Acciones]

Modo de Operación:

  /B[+|-]   Modo batch:  habilitar (-) o deshabilitar (+) interacción con el
            usuario.
  /D[+|-]   Modo diferido. /D+ arrancará el programa después del siguiente
            reinicio del sistema.
```

```
            /D- cancelará el efecto de una llamada previa con /D+.
   /T[+|-]  Modo test. /T+ no escribirá las correcciones a disco.
            /T- actualizará los archivos *.INI.
   /V[0|1|2] Modo informativo: silencioso (0) o prolijo (2).

 Acciones:

   /N[+|-]   Sombras en Nowhere: borrar (+) o ignorar (-) sombras de la
             carpeta <WP_NOWHERE>.
   /H[+|-]   Handles: borrar (+) o ignorar (-) los handles de
             objetos que no tengan archivo o directorio asociado.
   /I[+|-]   Identificadores: borrar(+) o ignorar (-) los identificadores de
             objetos sin handle asociado.
   /Runidad  Borrar todos los handles de los objetos definidos en las unidades
             especificadas. Se puede indicar más de uno usando ';' como
             separador.
   /U[i|d|c] unidades UNC: Ignorar (i), borrar (d) o verifiCar (c)
             las unidades especificadas vía nombres UNC (\\...).

 Valores por defecto:

   EdyClini /B- /T- /V2 /N- /H- /I-  /Ui
```

Tenga presente que si usa este programa para limpiar la carpeta <WP_NOWHERE>, y el sistema funciona de manera defectuosa a partir de ese momento, la única manera posible (no garantizada) de arreglar el problema podría ser:

Reiniciar el sistema hasta una línea de comandos arrancada en el archivo config.sys

Borrar el directorio físico <WP_NOWHERE>

Continuar el proceso de inicio del sistema

Ejecutar el siguiente código:

```
/* */
call RxFuncAdd 'SysLoadFuncs', 'REXXUTIL', 'SysLoadFuncs'
call SysLoadFuncs
call SysSetObjectData '<WP_NOWHERE>','OBJECTID=<WP_NOWHERE>'
```

Ahora utilice cualquier herramienta de mantenimiento de archivos INI para borrar del archivo OS2.INI la información correspondiente a la aplicación PM_ABSTRACT:FolderContents dentro de la llave correspondiente al handle de objeto <WP_NOWHERE>, que puede localizarse buscando la aplicación PM_WorkPlace:Location para la llave <WP_NOWHERE>.

Finalmente, reinicie el sistema de nuevo

EDYWINI

Este programa sirve para instalar o desinstalar las DLLs de PM que necesitan algunos componentes. Está ubicado en el subdirectorio EXEC en su directorio de SecureEntry, y su sintaxis es:

```
EDYWINI /I[fichini] nombredll [..nombredll] |
        /U[fichini] nombredll [..nombredll] |
        /L[fichini]
```

/I

Para instalar una serie de DLLs (nombredll(s)) en el sistema.

/U

Para desinstalar una serie de DLLs (nombredll(s)) del sistema.

/L

Para listar los nombres de las DLLs instaladas.

Además, vd. puede especificar opcionalmente el perfil de usuario con el que debe trabajar la utilidad, para cada uno de los comandos (fichini). Por defecto se utilizará el archivo *OS2.INI* indicado por la variable USER_INI en el archivo *CONFIG.SYS* de arranque.

Las DLLs requeridas para el arranque correcto de una estación SecureEntry son, *EDYWIN*,*EDYSESNO*, y *EDYLKSTR*. Por tanto, si vd. reconstruye o importa su archivo de usuario del OS/2 *OS2.INI*, deberá, antes de intentar el arranque de la estación, ejecutar el comando :

```
EDYWINI /I EDYWIN EDYSESNO EDYLKSTR
```

Observe que esta utilidad puede funcionar en un entorno sin PM, como por ejemplo desde una linea de comandos OS/2 obtenida vía el menú de opciones Alt-F1.

EDYCRWRK

Éste comando REXX puede ser usado para crear de nuevo la carpeta de herramientas de trabajo de SecureEntry en caso de que sea necesario. Debe ser usado por un administrador, y su sintaxis de invocación es:

```
EDYCRWRK
```

Este comando está ubicado en el subdirectorio INSTALL de su directorio SecureEntry.

EDYSRV y EDYFREE

El programa EDYSRV es un proceso que se ejecuta en segundo plano en los servidores de SecureEntry instalados en entorno de red, y que se comunica con los clientes a través de netbios. Si se necesita este programa, la sentencia correcta para lanzarlo habrá sido añadida a su comando de arranque de la estación EDYSTART.CMD. Ambos programas residen en el subdirectorio EXEC de su directorio de SecureEntry.

La sintaxis de invocación para EDYSRV es :

```
(detach) EDYSRV [/N:nombrenetbios] [/S:sesionesnetbios]
                [/R:política_refresco]
```

nombrenetbios

El nombre de netbios a añadir a la red. Tenga en cuenta que los clientes usan el nombre EDYnombredominio para comunicarse con este módulo, donde nombredominio es el nombre de su dominio IBM Lan Server.

sesionesnetbios

Es el número de sesiones paralelas de netbios que deben usarse. El valor por defecto es 4. Se recomienda aumentar este número si se espera una utilización masiva de la máquina servidora (i.e, muchos usuarios conectándose a la vez con el RACF o UCM).

política_refresco

La política de refresco a utilizar en la máquina servidora. Este parámetro puede tomar los siguientes valores:

```
/R:H -> EDYSRV utilizará la política corporativa
        almacenada en la base de datos central (UCM) para refrescar la oficina.
/R:I -> EDYSRV ignorará la política corporativa y refrescará la oficina
        en tiempo de IPL.
/R:L -> EDYSRV ignorará la política corporativa y refrescará la oficina
        en tiempo de conexión de los usuarios.
/R:N -> EDYSRV ignorará la política corporativa y no refrescará
        nunca la oficina.
/R:T<hhmm> -> EDYSRV ignorará la política corporativa
       y refrescará la oficina a la hora y minutos especificada.
/R:E<mmmmm>-> EDYSRV ignorará la política corporativa
        y refrescará la oficina en tiempo de IPL, y después periódicamente
        cada mmmmm minutos.
```

EDYFREE es el comando que descarga un EDYSRV que se esté ejecutando. La sintaxis de invocación es :

```
EDYFREE nombrenetbios
```

MIGRADB

Este comando REXX puede ser usado para migrar una base de datos de usuarios y componentes de SecureEntry 2.0 a una de SecureEntry 3.0. Debe ser ejecutado desde el controlador de dominio (desde donde estén los componentes de SecureEntry 2.0). Para poder utilizarlo debe haber instalado SecureEntry 3.0 encima de SecureEntry 2.0, y haberse asegurado de que la variable de entorno SGM_LS esté aún definida y apunte a la de la base de datos antigua de SecureEntry 2.0.

La sintaxis de este comando es :

```
MIGRADB  SECP|BOTH
```

SECP

Use esta opción si sólo quiere migrar las componentes de seguridad y seguir usando las definiciones de grupos y usuarios de IBM Lan Server que ya tenía (entorno IBM Lan Server)

BOTH

Use esta opción si ha instalado SecureEntry 3.0 en modo monoestación y quiere redefinir los usuarios y grupos que tenía definidos para poder usarlos en el nuevo entorno.

EDYLOGFS

El programa EDYLOGFS permite controlar automáticamente el tamaño de los archivos de registro de SecureEntry. Este programa reside en el directorio EXEC de su directorio de SecureEntry.

Toma por entrada un archivo ASCII llamado EDYLOGS.STR que debe residir en el directorio NOUSER de su directorio de SecureEntry. Cada línea de este archivo especifica la ubicación de un archivo de registro de

SecureEntry y una política de control de tamaño que será aplicada a este archivo de registro. Como primera aproximación, una línea de este archivo se interpreta así:

```
donde_localizar_el_archivo    qué_política_de_control_de_tamaño_aplicar
```

Localización del archivo de registro

Todas las líneas del archivo EDYLOGS.STR que no estén en blanco y no sean comentarios deben empezar especificando una ruta de archivo que termina con el nombre del archivo de registro. Esta ruta puede ser interpretada de tres maneras distintas según su cabecera:

`x$...`

Nombre completo del archivo empezando desde la raíz de la unidad x

`boot...`

Nombre completo del archivo empezando desde la raíz de la partición de arranque

`\...`

Nombre relativo del archivo empezando desde el directorio de SecureEntry

A continuación de la ruta de archivo puede especificarse (opcionalmente) el nombre de una variable de entorno. Así, para localizar el archivo, primero se usará (si existe) ésta variable de entorno interpretando su valor como un nombre completo de directorio en el que debe residir el archivo (cuyo nombre se obtiene de la ruta). Si esta primera búsqueda falla, se usa la ruta de archivo.

Políticas de control del tamaño

Todas las líneas del archivo EDYLOGS.STR que no estén en blanco y no sean comentarios deben terminar especificando una política de control de tamaño para que sea aplicada al archivo especificado al principio de esa misma línea.

La utilidad EDYLOGFS ofrece dos modos de restringir el tamaño de los archivos de registro:

Por Tamaño (en Kb)

Para establecer una política de control de tamaño basada en el tamaño del archivo, deben especificarse dos números, opcionalmente precedidos de una 'S', al final de una línea de EDYLOGS.STR que referencie un archivo particular. Como por ejemplo:

```
c$\myfile.log          MY_ENV_VAR          S64,32
```

Estos números se interpretan (de izquierda a derecha) como:

El tamaño base en Kb del archivo (**BFS**)

El incremento máximo permitido (en Kb) sobre **BFS**. (**IBFS**)

NOTA: el segundo número, **IBFS**, no es obligatorio. El valor por defecto es **BFS**/2

De ellos se deriva el tamaño máximo permitido para el archivo de registro especificado, que es **BFS**+**IBFS** Kb. Si EDYLOGFS descubre que el archivo tiene un tamaño mayor que este valor, purgará el archivo hasta conseguir un tamaño tan cercano como sea posible a **BFS** Kb garantizando que ninguna línea del archivo quede incompleta, y lo hará siguiendo una política FIFO, es decir, borrando primero los datos más antiguos del archivo.

A continuación se dan ejemplos de control de tamaño basado en el tamaño del archivo en Kb:

```
c$\myfile.log          MY_ENV_VAR          64
c$\myfile.log          MY_ENV_VAR          s64,32
boot\myfile.log                            S23
\nouser\myfile.log                         56,10
```

Por número de líneas

Para establecer una política de control de tamaño basada en el número de líneas del archivo, deben especificarse dos números, precedidos por una 'L', al final de la línea de EDYLOGS.STR que referencie el archivo que se quiere controlar. Por ejemplo:

```
boot\myfile.log                              L100,10
```

Estos dos números se interpretan (de izquierda a derecha) como:

El número Base de líneas del archivo (**BNL**)

El incremento máximo de líneas permitido sobre **BNL** (**IBNL**)

Note: el segundo número, **IBNL**, no es obligatorio. El valor por defecto es **BNL**/2

De estos dos números se deriva el máximo número de líneas que el archivo puede tener, que es **BNL**+**IBNL** . Si EDYLOGFS descubre que el archivo tiene un número de líneas superior a este valor, purgará el archivo para que tenga exactamente **BNL** líneas, y lo hara con política FIFO, es decir, borrando primero las líneas más antiguas.

El archivo de entrada para la utilidad EDYLOGFS.

EDYLOGFS lee su entrada del archivo ASCII EDYLOGS.STR ubicado en el subdirectorio NOUSER de su directorio SecureEntry. Toda línea de este archivo que no esté en blanco y no sea un comentario, debe especificar cómo localizar un archivo y qué política de control de tamaño aplicarle.

Sintaxis del archivo EDYLOGS.STR

A continuación se da la gramática que especifica la sintaxis del archivo EDYLOGS:STR:

(**<LINE>** | **<COMMENT>**) ('\n')*

<COMMENT>

= ';' (cualquier cadena)

<LINE>

= (<blanks>|<null>) **<PATHNAME>** ((<blanks> **<ENV_VAR>**) | <null>) <blanks> **<SIZE_CTRL_POLICY>** (<blanks>|<null>|**<COMMENT>**)

<null>

= la cadena vacía

<blanks>

= ('_'|'\t')+

<PATHNAME>

= (**<BOOT>** | **<DRIVE>** | <null>) <os/2 pathname> .br /*Especifica una ruta a un archivo*/

<ENV_VAR>

= cualquier cadena que sea válida como nombre de variable de entorno .br /*Especifica una variable de entorno que tiene por valor una ruta a un directorio*/

<SIZE_CTRL_POLICY>

= (**<POL_CHAR>** | <null>) **<TRUNC_SIZE>** (<null> | (',' **<OFFSET>**))

<BOOT>

= cualquier combinación en mayúsculas o minúsculas de la palabra 'BOOT'.

<DRIVE>

= <char> '$'

<os/2 pathname>

= cualquier ruta de archivo válida de OS/2 sin unidad y terminada con un nombre de archivo

<POL_CHAR>

= 'S'|'s'|'L'|'l'

<TRUNC_SIZE>

= <num>

<OFFSET>

= <num>

<char>

= ('a'-'z') U ('A'-'Z')

<num>

= cualquier número entero

NOTA: las unidades sintácticas <num>, **<ENV_VAR>** y <os/2 pathname> tienen restricciones de longitud. Si alguna de estos elementos tiene más carácteres de los permitidos, se retorna un error de sintaxis.

Un ejemplo de archivo EDYLOGS.STR

Este es un ejemplo de EDYLOGS.STR:

```
;EJEMPLO DE archivo DE CONTROL DEL TAMAÑO DE ARCHIVOS

;Estas líneas en blanco se ignoran

\install\myfile.log       64
;   Tamaño máximo 128 Kb. Se purgaría a 64 Kb.
```

```
;   El archivo "myfile.log" se buscaría en el subdirectorio INSTALL del
;   directorio de SecureEntry

c$\install\myfile.log    L10
;  Número máximo de líneas: 15. Se purgaría a 10 líneas.
;  El archivo "myfile.log" se buscaría en el directorio c:\install.

c$colon.myfile.log       MY_ENV_VAR    l100,50
;  Número máximo de líneas: 150. Se purgaría a 100 líneas.
;  El archivo "myfile.log" se buscaría primero en el directorio
;  apuntado por la variable de entorno MY_ENV_VAR, y, si no se
;  encontrara, se buscaría en la raíz de la unidad c.
```

El archivo EDYLOGS.STR por defecto proporcionado por SecureEntry.

El archivo EDYLOGFS.STR por defecto que proporciona SecureEntry es como sigue:

```
;SENTRY LOG FILES SIZE CONTROLLER CONFIGURATION FILE

\install\sentry.log                                  64,64 ;SENTRY INSTALLATION LOG FILE
boot\edylkini.log                  SGM_INI_LOGPATH   64,64 ;STARTUP MESSAGES LOG FILE
\nouser\edyadmin.log               SGM_SL_LOGPATH     64,64 ;SENTRY ADMINISTRATION LOG
FILE
boot\os2\security\sesdb\edysla.log    SGM_SES_LOGPATH   64,64 ;SENTRY SESSION ACTIVITY LOG
```

Después de aplicar una actualización a su versión de SecureEntry, el nuevo archivo EDYLOGS.STR proporcionado por defecto será copiado al directorio VíaDeAccesoSecureEntry\EXEC. Si el archivo VíaDeAccesoSecureEntry\NOUSER\EDYLOGS.STR no ha sido actualizado para su instalación, este último será automáticamente actualizado; en otro caso, usted tendrá que actualizarlo manualmente para que los cambios surtan efecto.

Sintaxis de invocación

La sintaxis para invocar la utilidad EDYLOGFS es:

```
EDYLOGFS [(/V|/?)]
```

/V	Mostrar todos los mensajes por la salida estándar.
/?	Mostrar la ayuda

Instalando EDYLOGFS

EDYLOGFS se puede invocar desde dos lugares distintos:

Desde el archivo config.sys. Esta es la opción por defecto que la instalación de SecureEntry implementa.

Para controlar de forma automática el tamaño de los archivos de registro de SecureEntry en tiempo de IPL, se recomienda invocar EDYLOGFS.EXE desde el config.sys. Para ello puede añadir la siguiente línea a su archivo CONFIG.SYS:

```
CALL=SecureEntryPath\exec\edylogfs.exe
```

También se podría invocar ésta utilidad desde cualquier exit de usuario. SecureEntry garantiza que las exits de usuario toman control con los archivos de registro cerrados, y, por lo tanto, pueden ser purgados.

Códigos de Error

La utilidad EDYLOGFS retorna el valor 0 si todo ha ido bien, si no, retorna un valor entero negativo...

Esta es una lista de los códigos de error que EDYLOGFS puede retornar:

-1

No se encontró el directorio de SecureEntry. O bien la variable de entorno SGM_SHELL no estaba definida o bien apuntaba a un directorio no válido

-2

El archivo de entrada (EDYLOGS.STR) no pudo ser abierto o no se encontró en el subdirectorio NOUSER del directorio de SecureEntry

-3

Error de E/S sobre el archivo de entrada (EDYLOGS.STR)

-4

El archivo de entrada (EDYLOGS.STR) no pudo ser cerrado

-5

El proceso EDYLOGFS.EXE no pudo reservar suficiente memoria

-6

El flujo de programa alcanzó un punto de ejecución que se suponía no alcanzable

EDYLOGBR

El programa **EDYLOGBR** puede utilizarse para examinar de forma cómoda los archivos de anotación SecureEntry, convenientemente unificados en una vista lógica ordenada por fecha y hora :

El archivo de anotaciones de eventos de sesión

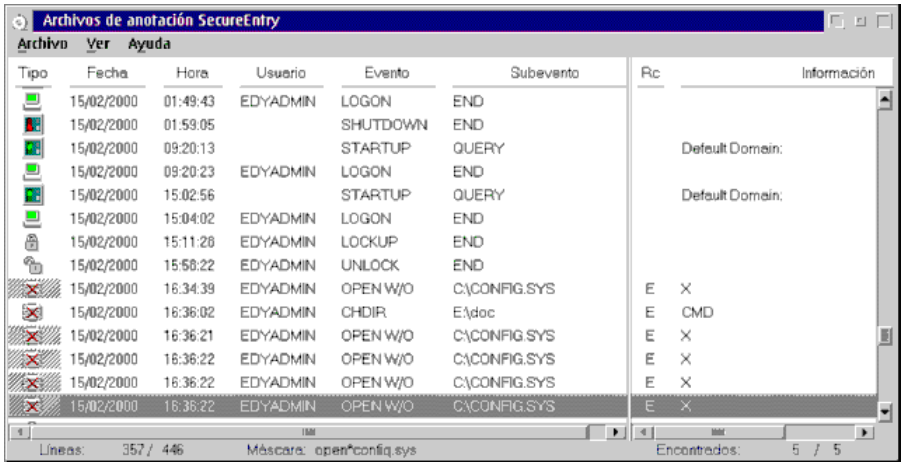
El archivo de anotaciones de eventos de administración

El archivo de anotaciones de eventos de accesos denegados del *Treelock*, siempre que se halle activo.

Puede ejecutarse desde una línea de comandos, tecleando :

```
EDYLOGBR
```

O directamente a través del objeto indicado de la capeta de *Herramientas de instalación SecureEntry* :



Una vez arrancado, el programa presentará los registros de anotación seleccionados según los criterios del menú *Ver* :

Errores/denegados Presentará solamente aquellas líneas de anotación que se refieran a eventos que terminaron con alguna condición de error o indican algún acceso denegado a recurso.

Vista simplificada Se visualizarán todas las líneas de anotación, no obstante, no se enseñará mas de una línea por evento. Así por ejemplo, se excluirán los eventos de inicio de una acción, o los eventos de administración relativos al subsistema Lan Server, por ser redundantes con la anotación equivalente para el subsistema SecureEntry, quien en primer término anota la acción.

Vista completa Presentará todos los registros actuales de los archivos de anotación deseados.

Eventos de sesión Utilice esta entrada de menú para incluir/excluir las anotaciones procedentes del archivo de anotaciones de eventos de sesión (p.e. consexión, desconexión, bloqueo,...).

Eventos de administración Utilice esta entrada de menú para incluir/excluir las anotaciones procedentes del archivo de anotaciones de eventos de administración (p.e. añadir/borrar usuarios, grupos,...).

Audit de accesos denegados Utilice esta entrada de menú para incluir o excluir las anotaciones procedentes del archivo de anotaciones de accesos denegados *Treelock*, siempre que se halle configurado dicho archivo a tal efecto como defecto de máquina en la carpeta SecureEntry *NOUSER*.

Ver iconos Con esta opción puede vd. habilitar/deshabilitar la vista de iconos gráficos indicadores del tipo de entrada de anotación

Refrescar ahora Seleccione esta opción para forzar una relectura de los archivos de anotación.

El menú *Archivo* dispone de las siguiente opciones :

Exportar Permite guardar en un archivo texto las anotaciones presentadas.

Buscar Permite la intoducción de una máscara de búsqueda, con caracteres de sustitución, para localizar todos los eventos presentados con los que haya coincidencia. Se debe asumir que los registros son examinados como si se tratase de registros de una sola línea, resultado de concatenar el valor de todas las columnas que los componen. Así por ejemplo, con la máscara *perez*logon* se encontrarán registros referentes a eventos de conexión asociados al usuario *perez*.

Siguiente Buscará y seleccionará el siguiente registro, con respecto a la posición actual, con el que coincida la máscara de búsqueda.

Previa Buscará y seleccionará el registro anterior, con respecto a la posición actual, con el que coincida la máscara de búsqueda.

Salir Para terminar la aplicación.

Algunas notas importantes con respecto a la aplicación :

En primer lugar, tenga en cuenta que en tiempo de arranque, el controlador de tamaño de los archivos de anotaciones irá eliminado de dichos archivos las líneas mas antiguas, por tanto, cuando utilice esta herramienta, no verá los eventos por que hayan sido limpiados automáticamente.

Esta utilidad utiliza los formatos de fecha y hora especificados vía el objeto de configuración de *país* de OS/2. Si vd. cambia dichos valores de configuración, el programa puede confundirse o no ordenar correctamente los eventos ocurridos antes del cambio de la configuración.

Por último, recuerde que el alcance de los archivos de anotación de eventos de sesión y de accesos denegados es local: vd. solamente verá eventos ocurridos en la máquina en la que se ejecute la utilidad. No obstante, y para máquinas Lan Server, los eventos de administración tienen alcance a nivel de dominio, por haber un solo archivo de anotaciones por dominio.

EDYPHOTO

Los programas **EDYPHOTO** permiten crear una vista en formato de archivo binario de los archivos de configuración de la máquina, lo que es muy útil para poder detectar y/o resolver problemas. Tanto el programa fotografiador como el visualizador pueden ser arrancados manualmente o desde la carpeta de **Herramientas de instalación de SecureEntry**.

Haga doble click sobre el icono del **generador de fotos** para obtener un archivo llamado **MMDDhhmm.BIN** que contiene una copia de los archivos de la configuración de la máquina. También puede obtener la foto de configuración tecleando:

```
EDYPHOTO
```

Con el parámetro '?' vd. obtendrá una breve descripción de la sintaxis completa del mandato, y otros parámetros disponibles.

Arrastre y suelte el archivo generado anteriormente sobre **el icono del visualizador de fotos** para poder ver su contenido. O bien, invóquelo mediante :

```
EDYPHDSP  [nombrearchivo]
```

Observe que los archivos de foto se crean normalmente con atributo de sólo lectura para que no puedan ser borrados por accidente.

El Servidor de Rastreo

Se proporciona un servidor de rastreo para que las aplicaciones puedan registrar datos de rastreo (traces).

Mientras se ejecutan las aplicaciones, éstas pueden recoger información útil para la depuración de las mismas (tanto a nivel de desarrollo como a nivel de diagnóstico) y para la detección y corrección de errores en tiempo de producción.

Modos de operación

Cambiando el modo de operación

Cargando el servidor de rastreo

Modos de operación

El servidor de rastreo soporta los siguientes modos de operación:

Rastreo a memoria (memory status)

Rastreo a archivo (file status)

Además el servidor de rastreo puede estar cargado sin ser operativo (stop status).

Para minimizar la sobrecarga debido al rastreo se recomienda cargar el sevidor de rastreo en modo no operativo y cambiar el modo de operación dinámicamente según las necesidades.

Rastreo a memoria

El programa EDYTRDSP.EXE permite visualizar en pantalla la información de rastreo recogida por el servidor de rastreo.

El contenido del panel de rastreo se actualiza sólo bajo demanda del usuario. Para refrescar el contenido, seleccione la opción apropiada de menú o presione la tecla de función F5.

La fuente del contenido puede ser modificada arrastrando una nueva fuente desde la paleta de fuentes y soltándola sobre el panel. Debe seleccionar un tipo de fuente no proporcional, por ejemplo 'monoespaciada de sistema', 'system VIO' o 'courier'.

Rastreo a archivo

El programa EDYTRCS.EXE puede salvar la información de rastreo en un archivo.

Puede visualizar el contenido del archivo de rastreo usando el programa EDYTRDSP.EXE.

Cambiando el modo de operación

El programa EDYTRSET.EXE permite cambiar el modo de operación del servidor de rastreo.

Para arrancar este programa, escriba:

```
EDYTRSET  [/S:status]
```

Donde *status* es el modo de operación que quiere para el servidor de rastreo:

M : Rastreo a memoria

F : Rastreo a archivo

S : No operativo (no se rastrea)

El parámetro F sólo es válido si se ha cargado el programa EDYTRCS.EXE.

Cargando el servidor de rastreo

Esta sección explica cómo cargar el servidor de traceo y los posibles códigos de retorno al ejecutar ésta operación.

Si especifica que el servidor de rastreo salve los datos a un archivo y este archivo ya existe, los parámetros especificados para la carga del servidor serán ignorados y los datos de rastreo se añadirán al final del archivo ya existente.

La sentencia de carga

A continuación se da la sintaxis del comando EDYTRCS para cargar el servidor de rastreo. Para conocer los errores que se puedan producir durante la carga **o** la ejecución del servidor de rastreo puede redireccionar la salida a un archivo.

```
DETACH EDYTRCS [/S:status] [/M:tamañobuffer]
               [/T:tamañoarchivo] [/PT:drive:ruta\nobrearchivo]
               [/PC:unidad:ruta] [/N:numerorastreo]
```

donde :

Status es el modo de operación (MEMORY, FILE o STOP). FILE es el valor por defecto.

TamañoBuffer es el Tamaño de memoria, en KB, destinada a salvar los datos de rastreo.

El parámetro es válido sólo si el programa EDYTRCS.EXE ha sido cargado antes de que ninguna apliacación haya enviado datos de rastreo. El rango de valores para el parámetro es de 4 a 512. El valor por defecto es **64**.

Tamañoarchivo es el tamaño máximo del archivo, en KB, donde serán salvados los datos de traceo. Sin incluir la cabecera del archivo.

El valor máximo para el parámetro es el espacio disponible de disco. El valor por defecto es **150**.

/PT y /PC especifican el nombre completo del archivo de rastreo (opcional). El nombre por defecto es EDYTRC.DAT y se ubica donde resida el archivo EDYTRACE.INI.

Númerorastreo es el número de líneas de rastreo que han de ser salvadas antes de cumplimentar una condición de paro de rastreo (stop status)

El rango de valores es de 0 a 512. El valor por defecto es **10**.

Códigos de retorno de carga

La siguiente lista muestra los códigos que pueden ser retornados en tiempo de carga:

```
Valor     significado
------------------
x'5A'     Error al crear o abrir el archivo de rastreo.
x'5C'     Parámetro especificado no válido.
x'5D'     No hay suficiente espacio en el disco para el archivo de rastreo.
x'5F'     archivo de rastreo dañado.
x'61'     Error al  inicializar el servidor de rastreo.
x'62'     Servidor de traceo ya cargado
```

Información técnica relativa a SecureEntry

Este capítulo contiene una descripción de los recursos utilizados por SecureEntry 3.0, variables de entorno y archivos de anotaciones y de configuración.

Estructura de Directorios de SecureEntry

El directorio de SecureEntry incluye los siguientes subdirectorios:

El directorio API, donde reside el código fuente para la implementación de llamadas a funciones (APIs), así como la traducción NLS.

El directorio DLL, donde residen todas las DLLs de SecureEntry.

El directorio EXEC, donde residen las interfícies de la línea de comandos y los programas ejecutables.

El directorio TOOLS, donde residen las herramientas de SecureEntry (integración de programas).

El directorio NOUSER, donde reside la información relativa a la configuración de la máquina, así como el repositorio de los perfiles de seguridad.

El directorio WORK, donde residen los perfiles de seguridad que son actualizados desde el repositorio del servidor en tiempo de conexión de la sesión.

El directorio HELP, donde residen los archivos de ayuda.

El directorio TEMPLATE, donde residen los modelos básicos de los perfiles así como algunos ejemplos de componentes.

También puede haber el directorio TEMP, usado por las herramientas de administración para almacenar copias temporales de los archivos del repositorio.

Y por último, y bajo un nombre dependiente de la versión NLS, existe el directorio de las herramientas de trabajo, donde residen los objetos de las distintas herramientas.

Variables de Entorno

SecureEntry utiliza las siguientes variables de entorno:

Propósito General

Específicas de Lan Server

Relacionadas con el Control de la Sesión

Específicas de UCM

Específicas de la Administración

Relacionadas con el Escritorio

Relacionadas con otros Componentes

Propósito General

SGM_SHELL Esta variable es obligatoria y debe estar definida en el archivo config.sys. Debe contener el nombre del camino en el que están instalados los archivos de SecureEntry. Por defecto, y a menos que se especifique lo contrario, apunta al directorio C:SGMSHELL.

SGM_DB Esta variable también es obligatoria y debe estar definida en el archivo config.sys. Apunta al directorio donde se encuentra la base de datos de los perfiles de seguridad de SecureEntry (archivo EDYREGDB.VLB). En entornos de red, puede tratarse de un camino UNC.

Específicas de Lan Server

SGM_LS Esta variable está obsoleta y generalmente no se usa, aunque debe estar establecida a su valor original en el caso de que haya que ejecutar la utilidad MIGRADB, a fin de obtener los perfiles de seguridad originales (SecureEntry 2.0).

SGM_LS_IFLOGGED Esta variable de entorno indica la acción a realizar, en entornos de LAN Server, cuando en la conexión de la sesión se encuentre una conexión a dominio. Las opciones son:

```
SET SGM_LS_IFLOGGED=INFORM    :  No realizar la conexión. Mostrar un mensaje
                                 de error  (es el valor por defecto).
SET SGM_LS_IFLOGGED=FORCE     :  Forzar una desconexión y reintentar la
                                  conexión automáticamente.
SET SGM_LS_IFLOGGED=USE       :  Usar la sesión conectada si el Id de Usuario
                                 y  el dominio solicitados coinciden con el Id
                                 de  Usuario y el dominio ya conectados,
                                  respectivamente.  Informar en caso contrario.
SET SGM_LS_IFLOGGED=FORCEUSE  :  Usar la sesión conectada si el Id de Usuario
                                 y  el dominio solicitados coinciden con el Id
                                 de  Usuario y el dominio ya conectados,
                                  respectivamente.  Forzar una desconexión y
                                  reintentar en caso contrario.
```

Esta variable puede resultar muy útil a la hora de integrar SecureEntry con otros productos de seguridad, ya que la responsabilidad de la conexión puede ser compartida.

SGM_SGMSHELL_GROUP SecureEntry/2 permite la conexión de los usuarios Lan Server definidos en el dominio a través del repositorio de perfiles, accesible por todos ellos a través del recurso Lan Server *SGMSHELL*. A este recurso le dá acceso SecureEntry automáticamente cuando, a través de sus herramientas de administración, se define o modifica un grupo SecureEntry (que empieza

por las letras 'SG'). Si vd. tiene previsto definir mas de 64 grupos SecureEntry, entonces no podrá hacerlo ya que el límite Lan Server de las listas de control de acceso por recurso es de 64 entradas.

Con objeto de eliminar este límite, vd. puede definir esta variable de entorno en sus máquinas, y así especificar que, en lugar de garantizar el acceso a dicho recurso para todos los grupos SecureEntry, se haga para uno solo, cuyo nombre especifica esta variable.

Así, si vd. dá a esta variable el valor *USERS*, entonces cualquier usuario definido en el dominio (no GUEST) podrá hacer una conexión SecureEntry. Del mismo modo, si vd. le dá otro valor a esta variable, solamente aquellos usuarios que, además de pertenecer a un grupo SecureEntry (SG) pertenezcan también al grupo indicado, podrán conectarse. Será entonces su responsabilidad el asegurarse de que todos los usuarios SecureEntry estén definidos en este grupo.

Observe que el acceso al recurso *SGMSHELL* solamente estará garantizado una vez vd. haya definido o modificado por lo menos uno de sus grupos SecureEntry con esta variable de entorno configurada apropiadamente, ya que es en ese momento en el que SecureEntry creará dicho acceso si no existiese.

Relacionadas con el Control de la Sesión

SGM_EDYLK_SHOW Esta variable se puede usar para ocultar el dialogo de arranque de la estación, incluso en el caso de que en el directorio raíz de la partición de arranque exista un archivo EDYSTART.CMD, asignándole el valor **NO** o **0**.

SGM_HIDE_WAIT_DLGS Use esta variable de entorno con valor **YES** para evitar que se muestren los diálogos informativos del tipo 'xxx en proceso, por favor espere'. En caso de que esta variable no esté definida, o tenga otro valor, dichos diálogos se mostrarán.

SGM_INI_LOGPATH Esta variable de entorno establece el camino al archivo EDYLKINI.LOG, que mantiene información sobre la actividad en el proceso de arranque. Esta variable no la establece el proceso de instalación. Por defecto, si esta variable no está establecida, dicho archivo de anotación residirá en el directorio raíz de la partición de arranque, es decir, el mismo directorio en el que reside el archivo EDYSTART.CMD.

SGM_SES_LOGPATH Esta variable de entorno establece el camino al archivo EDYSLA.LOG, que mantiene información sobre la actividad de la sesión del sistema. Esta variable no la establece el proceso de instalación. Por defecto, si esta variable no está establecida, dicho archivo de anotación residirá en el camino apuntado por la variable SESDBPATH (siendo esta normalmente el camino OS2\SECURITY\SESDB de la partición de arranque). En caso de que los servicios de SES no estén instalados, se utilizará entonces por defecto el directorio SGMSHELL\NOUSER para guardar este archivo.

SGM_WPS_FASTLOAD Esta variable no es obligatoria. Determina la secuencia de activación de las restricciones del Escritorio en tiempo de carga del WPS. El WPS se carga cuando se arranca la estación de trabajo, después de que un error cause su terminación, y después de realizar una conexión de sesión en el caso de que la variable de entorno de SES 'RESTARTUSERSHELL' esté puesta a **YES**.

Si la carga rápida está inhabilitada, las restricciones del Escritorio definidas en NOUSER se aplican cuando se carga el WPS. Una vez el WPS está totalmente inicializado, se aplican las restricciones de todos los otros componentes de SecureEntry; y a continuación se aplican las restricciones del Escritorio del usuario.

Si la carga rápida está habilitada, las restricciones del Escritorio del usuario se aplican tan pronto como estén disponibles (identificadas por el usuario); y a continuación se aplican las restricciones de todos los otros componentes de SecureEntry. Esto significa que el usuario puede acceder al Escritorio antes de que se apliquen restricciones adicionales. La carga rápida puede afectar a la seguridad si las

restricciones del Escritorio del usuario permiten manipular objetos que deberían estar disponibles sólo cuando todas las otras restricciones estuvieran aplicadas (por ejemplo, arrancar un editor antes de que se apliquen las restricciones del Sistema de Archivos).

Un segundo efecto de ésta variable consiste en especificar 'cuando levantar el telón' en tiempo de conexión, es decir, en qué momento el usuario podrá usar el Escritorio. Si la carga rápida está habilitada, el archivo de mapa de imágen de fondo se cerrará en cuanto el usuario haya sido identificado. En caso contrario, el archivo de mapa de imágen de fondo no se cerrará hasta que todos los perfiles de seguridad estén activos, evitando así cualquier interacción del usuario con el sistema hasta ese momento.

Por defecto, la carga rápida está inhabilitada. Para habilitarla, establezca su valor a **YES** o a cualquier otro valor que empiece por **Y**.

SGM_ALLOW_CAD Establezca ésta variable de entorno a **YES** para permitir que una única combinación de Ctrl-Alt-Del haga que el sistema se reinicie, tal y como se comporta cualquier sistema OS/2 convencional. Por defecto, el valor de **NO** habilitará el sistema para que SecureEntry responda de manera adecuada a dicha combinación. El tercer valor permitido es **TWICE**, que fuerza el que sea una doble combinación de Ctrl-Alt-Del lo que haga que el sistema se reinicie. Esto es útil de cara a la generación de volcados del sistema, puesto que una combinación de Ctrl-Alt-Del seguida de otra de Ctrl-Alt-NumLock-NumLock forzará el volcado del sistema.

SGM_PM_WAIT_B4_KILL Use ésta variable de entorno para especificar el intervalo de espera (en segundos) antes de que SecureEntry decida terminar las aplicaciones PM ejecutándose en contexto de usuario después de haberles enviado el mensaje de cierre, en tiempo de desconexión. Esta variable resulta muy útil si quiere garantizar que el evento de desconexión termine incluso si las aplicaciones solicitan una interacción con el usuario cuando reciben el mensaje WM_CLOSE de PM. Por ejemplo, si Vd. está editando un archivo y decide desconectarse de la sesión, el comportamiento típico del editor será preguntarle si desea salvar o descartar los cambios realizados. Una vez que el período de tiempo especificado haya expirado sin intervención del usuario, el editor se terminará y el evento de desconexión se reanudará.

El valor por defecto es de 20 segundos. Especifique un valor de -1 para indicar un tiempo de espera indefinido. Se desaconseja explícitamente especificar un valor de 0, ya que es aconsejable dar a las aplicaciones PM una oportunidad para que salven sus datos.

SET SGM_WAIT_B4_FLUSH Establezca ésta variable a xxx, donde xxx es el número de segundos a esperar antes de que los contenidos de las antememorias del sistema queden grabados en el disco en tiempo de conclusión y en caso de que dicha conclusión no finalice satisfactoriamente.

Esto significa que un apagado de la máquina no implicará un chkdsk en el siguiente reinicio del sistema si han pasado xxx segundos desde el principio de WinShutdownSystem.

Si se especificó "edyutil { toshtdwn | frshtdwn } reboot", entonces el reinicio tendrá lugar casi inmediatamente si la conclusión del sistema finaliza satisfactoriamente, o después de que hayan pasado xxx segundos desde que se haya iniciado WinShutdownSystem.

Si no se especifica, xxx toma su valor por defecto a 300 segundos (5 minutos).

Si xxx==0, entonces se usará un valor de 300 segundos (5 minutos).

```
Formato:
o Si xxx empieza por 0, entonces el valor se tomará en octal
o Si xxx empieza por 0x o 0X, entonces el valor se tomará en hexadecimal.
o En otro caso, el valor se tomará en decimal.
```

SGM_SS_ALLOW_IU Esta variable de entorno tan solo tiene sentido si vd. está usando validación de contraseñas en RACF (o vía el emulador de RACF), ya que permite configurar la acción que tomará el programa al recibir el error *'Usuario desconocido'* desde el subsistema de gestión centralizada durante una conexión. Los valores posibles son :

0 (valor por defecto) Se interrumpirá el proceso de conexión informando al usuario de que no está dado de alta como usuario válido del sistema.

1 El programa se comportará como en una conexión en estado de emergencia. Es decir, se permitirá que la conexión continúe de tal modo que ésta se efectúe siempre que el par usuario/contraseña utilizado sea válido localmente. No se permitirá el cambio de contraseña en esta conexión.

2 El programa se comportará como en una conexión normal pero sin sincronizar la contraseña entrada en la oficina. Es decir, se permitirá que la conexión continúe de tal modo que ésta se efectúe siempre que el par usuario/contraseña utilizado sea válido localmente. Se permitirá el cambio de contraseña en esta conexión.

3 El programa se comportará como en una conexión normal pero sin sincronizar la contraseña entrada en la oficina. Es decir, se permitirá que la conexión continúe de tal modo que ésta se efectúe siempre que el par usuario/contraseña utilizado sea válido localmente. Se permitirá el cambio de contraseña en esta conexión. Adicionalmente, se le presentará al usuario un mensaje innformativo de esta situación (número de mensaje 106).

Observe que si usa valores distintos de 0 para esta variable de entorno, UCM no podrá garantizar la consistencia de la base de datos de usuarios con respecto al conjunto de usuarios definidos en las oficinas. No obstante, esto puede ser requerido por su corporación para facilitar cierta libertad de administración paralela en las oficinas.

SGM_SS_ALLOW_IP Esta variable de entorno tan solo tiene sentido si vd. está usando validación de contraseñas en RACF (o vía el emulador de RACF), ya que permite configurar la acción que tomará el programa al recibir el error *'Contraseña inválida'* desde el subsistema de gestión centralizada durante una conexión. Los valores posibles son :

0 (valor por defecto) Se interrumpirá el proceso de conexión informando al usuario de que la contraseña es inválida.

1 El programa se comportará como en una conexión en estado de emergencia. Es decir, se permitirá que la conexión continúe de tal modo que ésta se efectuará siempre que el par usuario/contraseña utilizado sea válido localmente en la oficina. No se permitirá el cambio de contraseña en esta conexión.

2 El programa se comportará como en una conexión normal pero sin sincronizar la contraseña entrada en la oficina. Es decir, se permitirá que la conexión continúe de tal modo que ésta se efectúe siempre que el par usuario/contraseña utilizado sea válido localmente. Se permitirá el cambio de contraseña en esta conexión.

3 El programa se comportará como en una conexión normal pero sin sincronizar la contraseña entrada en la oficina. Es decir, se permitirá que la conexión continúe de tal modo que ésta se efectúe siempre que el par usuario/contraseña utilizado sea válido localmente. Se permitirá el cambio de contraseña en esta conexión. Adicionalmente, se le presentará al usuario un mensaje informativo de esta situación (número de mensaje 106).

Observe que si usa valores distintos de 0 para esta variable de entorno, UCM no podrá garantizar la consistencia de la base de datos de usuarios con respecto al conjunto de usuarios definidos en las oficinas. No obstante, esto puede ser requerido por su corporación para facilitar cierta libertad de administración paralela en las oficinas.

SGM_SS_IF_NO_AUTOLOCKUP Establezca ésta variable de entorno a **NO** si quiere inhabilitar la funcionalidad de salvapantallas cuando no se define bloqueo automático a través del perfil de restricciones de SES, es decir, cuando Vd. sólo quiere la funcionalidad de salvapantallas en una pantalla de bloqueo, y no en un Escritorio desprotegido.

SGM_SS_USEREXIT Establezca ésta variable de entorno a **NO** si desea que la función del salvapantallas NO esté activa mientras se procesan las exits de usuario. En este caso, y si vd. proporciona sus propios diálogos de conexión y desbloqueo, estos serán responsables de evitar la pérdida de foco y deberán proporcionar su propia función salvapantallas.

SGM_SS_WHEN_LOCKUP Establezca ésta variable de entorno a **YES** si quiere que la funcionalidad del salvapantallas se active en el mismo momento en que se procesa un evento de bloqueo, sea este a petición explícita del usuario o debido a la inactividad. El temporizador de inactividad de salvapantallas definido en el perfil de seguridad se utilizará para:

Mostrar el salvapantallas cuando no se esté en estado de bloqueo (si no se usa la funcionalidad de bloqueo automático), o

Mostrar el salvapantallas cuando se esté en estado de bloqueo después de que el usuario haga aparecer el dialogo de desbloqueo a través de la pulsación de una tecla.

SGM_BACK_BITMAP Establezca ésta variable a **NO** si quiere inhabilitar la aparición del archivo de mapa de imágen de fondo durante el proceso de los eventos de conexión, desconexión y bloqueo de la sesión. Esta característica, generalmente poco utilizada, puede ser de utilidad en aquellas instalaciones en las que SecureEntry debe ser integrado de manera transparente con aplicaciones ya existentes.

Si Vd. requiere mayor granularidad, la misma variable de entorno acepta una sintaxis alternativa:

```
SET SGM_BACK_BITMAP=xyz
```

Donde:

x especifica donde mostrar el archivo de mapa de imágenes de fondo en tiempo de arranque.

y especifica donde mostrar el archivo de mapa de imágenes de fondo durante conexión/desconexión.

z especifica donde mostrar el archivo de mapa de imágenes de fondo durante el bloqueo.

Especifique cada uno de los valores x, y, z como el carácter '0' (inhabilitado) o '1' (habilitado).

SGM_DISABLE_SYSTEM_KEYS Establezca ésta variable con un número para especificar una combinación de teclas dadas a inhabilitar. Este número puede ser la suma de:

```
Ctrl-Alt-Del ..............  1
Ctrl-Alt-NumlockNumlock  ...  2
Ctrl-Esc ..................  4
Alt-Esc ...................  8
Alt-Tab ................... 16
Pausa ..................... 32
Impr-Pant ................. 64
Tecla Windows izquierda . 128
Tecla Windows derecha ... 256
Tecla selección Windows . 512
```

Se puede especificar notación octal -empezando el número con '0'-, hexadecimal -empezándolo con '0x' o '0X'-, o decimal -en otro caso-. Para que esta característica funcione correctamente, su teclado debe ser plenamente compatible con IBM-PS2.

Si Vd. inhabilita una cierta combinación de teclas a través de esta variable de entorno, pero también la habilita para un perfil de SES activo, entonces la combinación quedará inhabilitada puesto que la decisión para habilitar o inhabilitar una combinación se hace en base a una operación lógica de bits OR.

El valor por defecto es 0 (habilitar todas las combinaciones de teclas).

SGM_HOOK_SYSTEM_KEYS

Esta variable de entorno le permite configurar qué combinaciones de teclas deben ser pasadas a una Exit de Usuario. Los valores permitidos son los mismos que los de la variable SGM_DISABLE_SYSTEM_KEYS. Si una combinación dada está inhabilitada y al mismo tiempo configurada para ser pasada a la Exit de Usuario, entonces la Exit de Usuario no la verá. Si configura una combinación de teclas para ser pasada a la Exit de Usuario a través de ésta variable de entorno, pero también configura que el perfil de SES activo no pase dicha combinación a la Exit de Usuario, entonces la combinación de teclas se pasará finalmente a la Exit de Usuario ya que la decisión para pasar una combinación a la Exit de Usuario se hace en base a una operación lógica de bits OR.

El valor por defecto es 0 (no pasar ninguna combinación de teclas a la Exit de Usuario).

SGM_SES_CAD

Establezca ésta variable a **YES** para forzar al sistema a que use la función (API) de SES para recibir las notificaciones de Ctrl-Alt-Del, en lugar de utilizar el propio controlador de dispositivo de SecureEntry (que es el comportamiento por defecto). El uso del propio controlador de dispositivo de SecureEntry para recibir las notificaciones de Ctrl-Alt-Del tiene la ventaja de que dicha combinación de teclas puede distinguirse de la combinación Ctrl-Alt-Numlock-NumLock, pero tiene la desventaja de que puede no funcionar si Vd. utiliza dispositivos de teclado no estándares.

SGM_SES_INACTIVITY

Establezca ésta variable a **YES** para forzar al sistema a que use la función (API) de SES para recibir las notificaciones de inactividad, en lugar de utilizar el propio controlador de dispositivo de SecureEntry (que es el comportamiento por defecto). El uso del propio controlador de dispositivo de SecureEntry para recibir las notificaciones de inactividad tiene la ventaja de obtener mayor precisión, pero tiene la desventaja de que puede no funcionar si Vd. aplica un FixPak de OS/2 para el cual esta característica no ha sido probada.

SGM_HOOK_CANN_KEY

Si esta variable tiene valor *NO*, entonces SecureEntry *no* tomará el control en respuesta a Ctrl-Alt-NumLock-NumLock. Esto significa que si la protección de boot está instalada, entonces *no* se podrá realizar el dump a la partición formateada FAT de nombre SADUMP, en el caso de que en el config.sys haya puesta la entrada TRAPDUMP=[ON|OFF],x: donde x es la unidad lógica asociada a la partición SADUMP.

Es de destacar que si la variable de entorno tiene valor *NO*, entonces no se llamará a la exit de usuario asociada a la combinación Ctrl-Alt-NumlockNumlock aunque así lo especifique la variable de entorno SGM_HOOK_SYSTEM_KEYS o el perfil de SES activo en ese momento. No obstante, si la variable de entorno SGM_DISABLE_SYSTEM_KEYS o el perfil de SES activo indican que hay que inhabilitar la combinación de teclas, el sistema no hará nada en respuesta a Ctrl-Alt-NumlockNumlock.

El valor por defecto para esta variable es *YES*.

SGM_USER_DLGS

Si vd. está cambiando los diálogos de conexión/desbloqueo por defecto, entonces puede también especificar con esta variable de entorno el nombre de sus procesos o los títulos de las ventanas que implementan dichos diálogos. Al hacerlo así, SecureEntry utilizará esta información para filtrar qué

ventanas modales pueden aparecer por encima de la imagen de fondo de bloqueo durante el proceso de las exits de usuario. Si no especifica ningun valor, entonces SecureEntry asumirá que la primera ventana modal que aparezca durante dicho proceso es la ventana del diálogo de conexión/desbloqueo deseada, creando así un agujero potencial de unos segundos durante los cuales un aviso asíncrono del sistema podría 'hacerse pasar' por su diálogo.

Especifique sus procesos o títulos separados por comas, y entre comillas dobles cuando indique títulos de ventanas. Los carácteres de sustitución '*' y '?' están permitidos. Así por ejemplo, el valor de la variable de entorno para cuando se quiera utilizar los diálogos de ejemplo de conexión/desbloqueo podría ser :

```
SET SGM_USER_DLGS=*LOGSAMP.EXE,*UNSAMP.EXE
```

SGM_HIDE_EXIT_AFTER_LOGON

Utilice esta variable de entorno para indicar si desea que SecureEntry mantenga la imagen de fondo modal de la conexión durante el proceso de la exit de usuario de después de la conexión (valor **YES**), o por el contrario desea que se procese dicha exit de usuario con el escritorio accesible (valor **NO**). Observe que SecureEntry pondrá por defecto, en tiempo de instalación, dicha variable a valor **YES** para garantizar la seguridad del sistema, ya que durante la ejecución de dicha exit de usuario las restricciones de treelock no están habilitadas.

SGM_NC

Esta variable de entorno sirve para especificar que sistemas de los definidos en el archivo de configuración del **NSC** actuarán como sincronizador de contraseñas cuando se este utilizando el LMP asociado a NSC/2. Los valores que puede tomar son los siguientes:

ALL. Todos los sistemas definidos en el **NSC** actúan como sincronizadores. Este es su valor por defecto.

Los índices, separados por comas, de las definiciones de sistema (LOCAL, SERVER, LANSERVER, HOST) del archivo de configuración del **NSC** que desee actuen como sincronizadores. Por ejemplo:

SGM_NC=2,3,6

En este caso los sistemas definidos en segundo, tercero y sexto lugar en el archivo de configuración del **NSC** actúan como sincronizadores.

SGM_SHUTDOWN_AT_LOGON_PANEL

Use esta variable de entorno con valor **NO** si desea inhibir el botón *Concluir* en el diálogo estándar SecureEntry de conexión cuando, por ejemplo, desee evitar que dicha operación la efectúen usuarios no identificados. El valor por defecto es **YES** (se permite concluir el sistema desde dicho diálogo).

Específicas de UCM

SGM_UCM_ENABLE Esta variable debe ser definida solamente si se utiliza el UCM, en la estación de trabajo de administración centralizada. Cuando su valor se establece a **YES**, todas las peticiones de administración vía función (API) se re-encaminan al host a través del agente de UCM DB2/DDCS. Vd. puede establecer ésta variable según la sesión de administración, es decir, no tiene por qué establecerla forzosamente en el archivo config.sys.

SGM_UCM_BRANCH Esta variable debe ser definida solamente si se utiliza el UCM, en la estación de trabajo de administración centralizada. Define el nombre de la oficina por defecto a usar por las utilidades de administración cuando se añada un nuevo usuario al repositorio de la corporación.

SGM_UCM_THIS_BRANCH Esta variable de entorno define el nombre de la oficina a través de la cual dicha oficina será conocida en el host. Sólo se utiliza a efectos informativos, para que Vd. pueda relacionar un identificador de oficina, proporcionado automáticamente por el host, con una cadena de carácteres con sentido. En realidad, ésta variable de entorno sólo se usará una vez, siempre que la nueva oficina sea conocida al host la primera vez, por lo que si Vd. intenta utilizarla tendrá que establecerla durante el proceso de instalación de sus nuevos servidores de oficina. Una vez instalado, la utilidad **EDYBRNVW.EXE** puede ser usada en cualquier estación de trabajo para visualizar la información de sincronización e identificación de la oficina.

EDY_UCM_MAXROWS Esta variable puede ser definida para establecer el número máximo de filas que la función (API) de UCM será capaz de manejar como resultado de una petición antes de devolver el error MANY_ROWS_FETCHED. Si no se especifica, por no se impone ningun límite.

SGM_REFRESH_PARMS Esta variable de entorno no es obligatoria. Debe ser definida en el archivo config.sys. Establece el número de reintentos para la tarea de refresco de oficina en el caso de que haya habido un error, el intervalo de tiempo entre las operaciones de reintento y el intervalo de tiempo en minutos a ser usado a la hora de calcular la hora inicial de refresco de la oficina. Esta variable puede tomar los siguientes valores: SGM_REFRESH_PARMS=a,b,c con rangos: 0 a 9, 0 a 99 y 0 a 180 para a, b, c respectivamente. Los valores por defecto si SGM_REFRESH_PARMS no se especifica son 1,15,30.

SGM_UCM_LOGPATH Esta variable de entorno establece el camino al archivo de anotaciones EDYDIS.LOG, que mantiene información relativa a la actividad de refresco de una oficina. Esta variable no la establece el proceso de instalación. Por defecto, si no está establecida, el archivo de anotaciones residirá en el camino apuntado por la variable de entorno SGM_DB (normalmente el subdirectorio NOUSER de la vía de acceso SecureEntry de la máquina servidora).

SGM_NETBIOS_ADAPTER_NUM Para que la comunicación NETBIOS entre el servidor y el cliente en tiempo de conexión (especialmente cuando se utiliza UCM) se efectúe usando un adaptador lógico de red diferente de 0, deberá indicarlo con ésta variable de entorno tanto en el cliente como en el servidor de perfiles. Los valores válidos son 0,1,2 o 3.

SGM_FORCE_LUALIAS Si no se especifica esta variable (situación por defecto), el EDYSRV utilizará la LU 6.2 independiente configurada como defecto para la configuración de Communications Manager/2. Si se le dá un valor, se utilizará la LU alias especificada en la variable de entorno para la comunicación entre el EDYSRV y el EDYTP

SGM_UCM_DBDFT Unicamente para la estacion administradora de UCM. Si usted cataloga la Base de Datos de UCM en la estación administradora de UCM con un alias diferente a 'UCM' debe definir esta variable de entorno con el nombre de alias que ha dado a la Base de Datos de UCM.

SGM_UCM_CORPORATE_NAME Unicamente para la estación administradora de UCM cuando vd. tenga instalada y configurada la Emulación de RACF. Si vd. desea administrar UCM desde **una única estación** en una corporación compuesta por varias empresas donde en cada una de ellas se ha instalado UCM, entonces ha de configurar lo siguiente:

Decidir antes de instalar SecureEntry y UCM el nombre de corporación para cada empresa. Si vd. desea que el nombre de corporación sea el mismo para todas las empresas no necesita utilizar esta variable de entorno.

Crear una copia del objeto *Administración de usuarios y grupos UCM* por cada empresa que desea administrar desde la estación administradora de UCMs.

Crear una copia del archivo UCMADM.CMD ubicado en **\SGMSHELL\EXEC** por cada empresa que usted desea administrar desde la estación administradora de UCMs. (Ejemplo: UCMADM**1**.CMD..UCMADM**n**.CMD).

En el archivo *UCMADM**x**.CMD* ha de incluir esta variable de entorno con el nombre de la empresa que desea administrar desde cada copia del objeto *Administración de usuarios y grupos UCM*. Este nombre de empresa ha de coincidir con el nombre de corporación especificado en la Instalación de SecureEntry para cada empresa. Asegúrese así mismo de que cada uno de los archivos haga conexión DB2 al alias de base de datos apropiado para cada institución.

Por último, recuerde asociar cada objeto copiado con cada uno de los archivos de comandos modificados en el punto anterior, editando sus propiedades directamente.

SGM_FORCE_MODE Solo para las estaciones controlador de dominio de las oficinas. Si usted desea definir un APPCMODE alternativo para el canal de comunicaciones de UCM, debe definir en esta variable de entorno el nombre del APPCMODE que desee utilizar. Esto puede ser de gran utilidad en instalaciones con RACF y UCM. Si usted utiliza la emulación de RACF provista por SecureEntry, entonces esta variable de entorno no es necesaria.

SGM_SNA_TIMEOUT Use esta variable de entorno para especificar el tiempo máximo (segundos) de espera para las respuestas SNA (APPC) a las transacciones UCM. Solamente son válidos valores superiores al valor mínimo (y por defecto), que es de 180 segundos.

Específicas de la Administración

SGM_SL_LOGMODE Esta variable no es obligatoria, y puede ser usada para establecer el modo de anotación para las utilidades de administración. Sus valores posibles son:

```
SET SGM_SL_LOGMODE=TEST     : Anotar toda actividad, incluyendo los valores de
                              las contraseñas devueltas en operaciones de
                              consulta. Util para la prueba de sus propios
                              agentes.
SET SGM_SL_LOGMODE=ALL      : Anotar toda actividad.
SET SGM_SL_LOGMODE=UPDATES  : Anotar sólo las actividades que modifican la
                             base de  datos. Es el valor por defecto.
SET SGM_SL_LOGMODE=NONE     : No anotar ninguna actividad.
```

SGM_SL_LOGPATH Esta variable de entorno establece el camino al archivo de anotaciones EDYADMIN.LOG, que mantiene información acerca de todas las actividades de administración. Esta variable no la establece el proceso de instalación. Por defecto, si no está establecida, el archivo de anotaciones residirá en el camino apuntado por la variable de entorno SGM_DB (normalmente el directorio NOUSER de la vía de acceso SecureEntry de la máquina servidora).

SGM_ADM_PRIV Esta variable de entorno puede utilizarse para filtrar qué operaciones de administración no deben permitirse desde una máquina determinada. Su valor debe ser un número entero especificado en decimal, hexadecimal (prefijo 0x), o binario (prefijo 0b), en el que cada bit indica una operación determinada, según la siguiente lista :

```
  EDYUCM_PRIVILEGE_SUB_VIEW          0x00000001
  EDYUCM_PRIVILEGE_SUB_ADD           0x00000002
  EDYUCM_PRIVILEGE_SUB_UPDATE        0x00000004
  EDYUCM_PRIVILEGE_SUB_DELETE        0x00000008
  EDYUCM_PRIVILEGE_RESOURCE_VIEW     0x00000010
  EDYUCM_PRIVILEGE_RESOURCE_ADD      0x00000020
  EDYUCM_PRIVILEGE_RESOURCE_UPDATE   0x00000040
  EDYUCM_PRIVILEGE_RESOURCE_DELETE   0x00000080
  EDYUCM_PRIVILEGE_GROUP_VIEW        0x00000100
  EDYUCM_PRIVILEGE_GROUP_ADD         0x00000200
  EDYUCM_PRIVILEGE_GROUP_UPDATE      0x00000400
```

```
EDYUCM_PRIVILEGE_GROUP_DELETE      0x00000800
EDYUCM_PRIVILEGE_USER_VIEW         0x00001000
EDYUCM_PRIVILEGE_USER_ADD          0x00002000
EDYUCM_PRIVILEGE_USER_UPDATE       0x00004000
EDYUCM_PRIVILEGE_USER_DELETE       0x00008000
EDYUCM_PRIVILEGE_USER_GRP_VIEW     0x00010000
EDYUCM_PRIVILEGE_USER_GRP_ADD      0x00020000
EDYUCM_PRIVILEGE_USER_GRP_UPDATE   0x00040000
EDYUCM_PRIVILEGE_USER_GRP_DELETE   0x00080000
EDYUCM_PRIVILEGE_RES_USER_VIEW     0x00100000
EDYUCM_PRIVILEGE_RES_USER_ADD      0x00200000
EDYUCM_PRIVILEGE_RES_USER_UPDATE   0x00400000
EDYUCM_PRIVILEGE_RES_USER_DELETE   0x00800000
EDYUCM_PRIVILEGE_GRP_GRP_VIEW      0x01000000
EDYUCM_PRIVILEGE_GRP_GRP_ADD       0x02000000
EDYUCM_PRIVILEGE_GRP_GRP_UPDATE    0x04000000
EDYUCM_PRIVILEGE_GRP_GRP_DELETE    0x08000000
EDYUCM_PRIVILEGE_RES_GRP_VIEW      0x10000000
EDYUCM_PRIVILEGE_RES_GRP_ADD       0x20000000
EDYUCM_PRIVILEGE_RES_GRP_UPDATE    0x40000000
EDYUCM_PRIVILEGE_RES_GRP_DELETE    0x80000000
```

Así por ejemplo :

```
SET SGM_ADM_PRIV=0x11111111
```

Permitirá solamente las operaciones de consulta.

```
SET SGM_ADM_PRIV=0x1111F111
```

Permitirá, adicionalmente, las operaciones de alta, baja y modificación de usuuarios.

Observe de todos modos, que el uso de esta variable solamente tiene sentido en entornos de administración cerrados, en los que el usuario no tiene acceso a líneas de comandos. Si vd. no especifica ningún valor para esta variable, entonces se permitirán todas las funciones de administración a cualquier usuario de tipo administrador.

Relacionadas con el Escritorio

SGM_WPS_LOADCLASS Esta variable no es obligatoria. Puede utilizarse para especificar las clases de WPS que deben cargarse antes de que se activen los perfiles SecureEntry durante la carga del WPS. Sólo debería definirse si hay definidos componentes que incluyen código de WPS que necesita ser inicializado antes de activar los perfiles del usuario. El valor de ésta variable debe ser una lista de nombres de clases separados por comas, sin blancos por en medio.

SGM_WPS_DISABLE Esta variable no es obligatoria, y sólo debería usarse durante la determinación de problemas. Cuando se establece a **YES**, o a cualquier otro valor que empiece por **Y**, se inhabilitan las clases de WPS de SecureEntry que reemplazan a las clases estándares.

SGM_WPS_TRACE Esta variable no es obligatoria, y sólo debería usarse durante la determinación de problemas. Permite definir el nivel de detalle de rastreo de diferentes subsistemas en el código del WPS. El valor debe ser una lista de subsistemas con su correspondiente nivel de detalle. Los subsistemas definidos y su nivel de detalle por defecto son: RES-3: Restricciones de Objetos CLS-3: Carga de Clases OBJ-3: Carga de Objetos POS-3: Gestión de la Posición de Objetos MGR-3: Gestión de Perfiles y Eventos DRG-3: Arrastrar y Soltar SHD-3: Carpetas Sombras MTX-5: Gestión de Semáforos Mutex ASY-5: Gestión de Eventos Asíncronos.

Ejemplos:

```
Si la variable no está definida y el nivel de rastreo de SNTOBJ es 1, ninguno de
los subsistemas rastreará sus acciones. Si el nivel de rastreo se cambia a 3,
todos los subsistemas excepto MTX y ASY rastrearán sus acciones.

Si la variable se establece a SGM_WPS_TRACE=RES-1,DRG-1,  y el nivel de rastreo de
SNTOBJ es 2, los subsistemas RES y DRG rastrearán sus acciones.
```

SGM_WPS_PRINTJOBS Esta variable no es obligatoria. Define cómo deberían aplicarse las restricciones sobre los trabajos de impresión. Sus valores posibles son: RESTRICT_NONE, RESTRICT_BY_TITLE, RESTRICT_BY_DEFAULT o RESTRICT_PRINTJOBS. Cuando se establece a RESTRICT_NONE, no se aplica ninguna restricción sobre los trabajos de impresión, sin tener en cuenta su título. Cuando se establece a RESTRICT_BY_TITLE, los trabajos de impresión se restringen con el mecanismo estándar: si se encuentra un título igual en el perfil de restricciones del Escritorio, se aplican las restricciones especificadas; si no se encuentra un título igual, se aplican las restricciones especificadas para la entrada DEFAULT; si no hay una entrada DEFAULT, no se aplica ninguna restricción. Cuando se establece a RESTRICT_BY_DEFAULT, a los trabajos de impresión se les aplica las restricciones impuestas por la entrada DEFAULT en el perfil de restricciones del Escritorio, sin tener en cuenta su título; si no hay una entrada DEFAULT, no se aplica ninguna restricción. Cuando se establece a RESTRICT_PRINTJOBS, todos los trabajos de impresión se tratan como si su título fuera RESTRICT_PRINTJOBS. Si el perfil de restricciones del Escritorio contiene una entrada RESTRICT_PRINTJOBS, se aplican sus restricciones para todos los trabajos de impresión, sin tener en cuenta su título; si no hay una entrada RESTRICT_PRINTJOBS, se utilizan las restricciones impuestas por la entrada DEFAULT; si no hay una entrada DEFAULT, no se aplica ninguna restricción. El valor por defecto es RESTRICT_BY_TITLE.

SGM_WPS_NONDESKTOP Esta variable no es obligatoria. Define cómo deberían aplicarse las restricciones sobre objetos que no están ni en el Escritorio actual ni en la carpeta de NoWhere ni en ninguna de sus subcarpetas. Sus valores posibles son: RESTRICT_NONE, RESTRICT_BY_TITLE, RESTRICT_BY_DEFAULT o RESTRICT_NONDESKTOP. Para evitar una degradación del rendimiento importante, las restricciones aplicadas a estos objetos sólo afectan a sus menús y a sus páginas de valores: no se aplica ningún cambio a sus estilos (visible o no, borrable o no...). Si se necesita restringir sus estilos se puede usar el mecanismo estándar del OS/2, ya sea a través de la instalación o a través de una Exit de Usuario si dichos estilos deben ser cambiados dinámicamente (por ejemplo, SysSetObjectData(ObjectPath,"NOTVISIBLE=YES;NODELETE=YES")). Cuando se establece a RESTRICT_NONE, a esos objetos no se les aplica ninguna restricción, sin tener en cuenta su título. Cuando se establece a RESTRICT_BY_TITLE, estos objetos se restringen según los mecanismos estándar: si se encuentra un título igual en el perfil de restricciones del Escritorio, se usan esas restricciones; en caso contrario se aplican las restricciones especificadas por la entrada DEFAULT; si no hay entrada DEFAULT, no se aplica ninguna restricción. El uso de este valor puede causar un retraso notable en el momento de abrir el cuaderno de valores de estos objetos o la hora de visualizar su menú. Cuando se establece a RESTRICT_BY_DEFAULT, estos objetos se restringen según las restricciones especificadas en la entrada DEFAULT en el perfil de restricciones del Escritorio, sin tener en cuenta su título; si no hay una entrada DEFAULT, no se aplica ninguna restricción. Cuando se establece a RESTRICT_NONDESKTOP, estos objetos son tratados como si su título fuera RESTRICT_NONDESKTOP. Si el perfil de restricciones del Escritorio contiene una entrada RESTRICT_NONDESKTOP, se utilizan sus restricciones para todos estos objetos, sin tener en cuenta su título; si no hay una entrada RESTRICT_NONDESKTOP, se aplican las restricciones especificadas en la entrada DEFAULT; si no hay una entrada DEFAULT, no se aplica ninguna restricción. El valor por defecto es RESTRICT_NONE.

SGM_WPS_BEEP Esta variable tampoco es obligatoria, y puede usarse para hacer que SecureEntry emita un pitido a través del altavoz en ciertos momentos y para propósitos de depuración. Se aceptan los valores:

REFRESH : suena un pitido al principio y al final del refresco de un escritorio.

EXIT : suena un pitido cada vez que el WPS termina.

TRAP : suena un pitido siempre que el código WPS de SecureEntry procesa un terminación anómala -trap- (valor por defecto).

SGM_WPS_SKIP_PREPOPULATE Esta variable controla si SecureEntry debe inhibir la población hecha por el sistema OS/2 en tiempo de arranque de las carpetas por defecto. El WPS de un sistema OS/2 WARP estándar pre-puebla las siguientes carpetas en tiempo de arranque:

<WP_TOOLS>

<WP_GAMES>

<WP_DRIVES>

<WP_CONFIG>

<WP_OS2SYS>

<WP_INFO>

<WP_PROMPTS>

<WP_SERVER>

Esta tarea puede tardar varios segundos, y bien puede ser que este conjunto de carpetas no sean precisamente las 'más utilizadas' en su sistema, en cuyo caso esto implica una pérdida de tiempo injustificada. Esto, junto con el hecho de que no fué hasta un parche reciente en el código de OS/2 en este 'paso de pre-población' que se arreglaba un problema interno de abrazo mortal (deadlock) a la hora de arrancar el WPS, fueron las razones que llevaron a la adición de la presente variable de entorno.

La variable puede tomar los siguientes valores:

ALL No poblar ninguna carpeta en tiempo de arranque

NONE Permitir la población de carpetas por defecto en tiempo de arranque (valor por defecto si la variable de entorno no está presente)

<ObjectId>..<ObjectId> Omitir la población de las carpetas listadas en tiempo de arranque

SecureEntry se instala a sí mismo estableciendo el valor **ALL** en el archivo config.sys.

SGM_EDYSC_DISABLE Esta variable puede usarse para inhabilitar todas las características SENTRY del WarpCenter, dejando la clase SmartCenter original de WPS. Los valores permitidos son **YES** y **NO**.

SGM_WPS_IGNORE_ADMIN Utilice esta variable de entorno con valor **YES** para que SecureEntry no haga ningún proceso especial a nivel de escritorio para aquellos usuarios definidos como administradores. Específicamente, al utilizar esta variable, SecureEntry no hará visible la carpeta de trabajo de SecureEntry, ni añadirá la entrada del menú emergente de las carpetas 'salvar posiciones'. Vd puede eliminar el efecto de esta variable de entorno ejecutando el archivo *EDYWPADM.CMD*, que se encuentra en la vía de acceso SecureEntry, subdirectorio TOOLS.

Relacionadas con otros Componentes

SGM_WIN_EXPLICITMENUS Establezca ésta variable a **NO** si desea que el componente sobre el comportamiento de las ventanas fuerce los valores del menú de sistema <DEFAULT> en todas las ventanas del sistema. El valor por defecto de esta variable es **YES**, por lo que los valores del menú de sistema sólo serán forzados en ventanas configuradas explícitamente. El valor **NO** hará que las

opciones de menú de sistema gestionadas por las aplicaciones estén activas/inactivas (según esté especificado), con lo que el resultado es impredecible a menos que se pruebe a fondo.

SGM_OVER_MK Esta variable puede usarse para controlar la información utilizada como semilla para el algoritmo de encripción del disquete dependiente de la Institución.

Si no se especifica o tiene el valor **NONE**, entonces el algoritmo de cálculo de la semilla la construirá a partir del nombre de la institución, el tipo de configuración, el nombre del servidor, y los indicadores de uso de UCM/RACF. El resultado final es que los disquetes encriptados de esta manera serán específicos de la oficina (dominio), si el nombre del servidor de dominio es único por oficina.

El valor **ALL** (valor por defecto establecido en tiempo de instalación) asegura que la semilla de encripción se genera solamente a partir del nombre de la Institución.

Cualquier otro valor implica el uso de todos los campos a excepción del nombre del servidor, que es entonces reemplazado por dicho valor.

SecureEntry se instala por defecto dando valor **ALL** a esta variable en el archivo *CONFIG.SYS*

Variables de entorno SecureEntry - warpcenter (ver componente warpcenter)

SGM_ROAM_LOGPATH Esta variable de entorno establece el camino al archivo EDYROAM.LOG , que mantiene información sobre la actividad del componente de Aplicaciones Públicas para entornos de LAN Server. Esta variable no la establece el proceso de instalación. Por defecto, si esta variable no está establecida, dicho archivo de anotación residirá en el camino apuntado por la variable SGM_SHELL, en su subdirectorio NOUSER.

Archivos de Configuración

SecureEntry 3.0 tiene una serie de archivos de control que definen su configuración y la versión instalada:

SENTRY.SIG Este archivo contiene información acerca del programa SecureEntry instalado. El siguiente contenido es una muestra:

```
PRODUCT=Secure Entry
VERSION=3.0
BUILD=69
BUNDLES=8
DATE=23 Sep 1996 20:46:05
```

Este archivo reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

SENTRY.CNF Este archivo contiene información sobre la configuración de SecureEntry. Se trata de un archivo que se explica casi por sí mismo, cuyo contenido se genera en el panel de configuración de la instalación. Sirva como muestra el siguiente ejemplo:

```
INSTITUTION=Banco de Juan
INSTALLPATH=C:\SGMSHELL
INSTALLFROM=A:\
CONFIGURATION=1
USERACF=0
USEUCM=0
INSTALLSOURCES=1
```

El único campo no tan obvio es el 'CONFIGURATION', que puede tener los siguientes valores:

1. Estación de Trabajo Aislada
2. Red IBM Lan Server
3. Instalación de Red no Lan Server.

Este archivo reside en la vía de acceso SecureEntry, subdirectorio INSTALL.

EDYSSLMP.DAT Este archivo describe la configuración de los LMP's (del inglés Logon Modular Procedures, Procedimientos de Conexión Modulares) que deben ser utilizados, así como el lugar de almacenamiento de las bases de datos de usuarios y de perfiles de seguridad. A pesar de que su formato es interno de SecureEntry, se trata de un archivo ASCII, por lo que puede ser visualizado o editado fácilmente. No modifique nunca el contenido de este archivo, a no ser que así lo especifique la documentación o el equipo de desarrollo de SecureEntry. Este archivo reside en la vía de acceso SecureEntry, subdirectorio NOUSER.

Para leer este archivo Vd. puede usar un editor ASCII, puesto que se trata de un archivo editable, y debe observar las siguientes reglas:

El archivo está dividido en dos bloques:

La lista de descripción de LMPs, donde se describen todos los procedimientos de conexión a través de su identificador único de dos letras:

1. **SS** LMP sincronizador de SecureEntry. Este LMP es obligatorio y siempre debe ser el primero.
2. **RF** LMP validador de RACF. Este LMP no es obligatorio, pero si está presente debe ser el segundo ya que sincroniza las contraseñas de todos los otros.
3. **UF** LMP emulador de RACF. Este LMP no es obligatorio, pero si está presente debe ser el segundo ya que sincroniza las contraseñas de todos los otros. Puede instalar el emulador de RACF de SecureEntry en lugar de la validación contra RACF.
4. **UC** LMP para el canal de UCM. Este LMP tampoco es obligatorio, pero si está presente debe estar a continuación del LMP de RACF o del LMP emulador de RACF. Su misión consiste en actualizar la configuración de la red en tiempo de conexión antes de que el LMP del LAN Server (o del Registro de SecureEntry) haga la conexión, para que este último encuentre la información del usuario en la red.
5. **LS** LMP para el LAN Server, en entornos de red. Éste es el LMP que controla la conexión al LAN Server.
6. **SR** LMP para el Registro de SecureEntry, en entornos de trabajo aislados.
7. **xx** Cualquier otra combinación representa un LMP escrito por el cliente y debe estar codificado en la DLL de nombre EDYxxLMP.DLL.

Los especificadores de descripción de base de datos contienen dos líneas que describen el lugar de almacenamiento de la base de datos de usuarios y el de la de perfiles de seguridad. Los únicos valores válidos son:

SR or LS Para USERS_DATABASE.

SR Para SCPRF_DATABASE.

Los LMPs de la lista aceptan unos parámetros opcionales que describen si ese LMP requiere un nombre de DOMINIO y el valor por defecto a mostrar en tiempo de conexión.

Sirva como muestra el siguiente archivo EDYSSLMP.DAT:

```
SS 1 SRVMAR
LS 1 SRVMAR
USERS_DATABASE LS
SCPRF_DATABASE SR
```

EDYREGDB.VLB Este archivo es en realidad una librería encriptada que contiene los perfiles de seguridad y/o la información de usuarios y grupos. Vd. no puede visualizar ni modificar su contenido, ya que está completamente gestionada por SecureEntry. Los usuarios administradores pueden usar la utilidad CREADB para regenerar una nueva librería vacía. Esta librería reside en la vía de acceso SecureEntry, subdirectorio NOUSER, en todas las estaciones de trabajo aisladas o en las estaciones de trabajo servidoras en entornos de red.

EDYKILL.NOT Este es un archivo ASCII que contiene una lista de procesos que no hay que terminar en un momento dado. En instalaciones convencionales de OS/2, hay una serie de procesos que se ejecutan en el fondo (background) que no contemplan el hecho de recibir una señal de terminación vía DosKillProcess, y que pueden terminar anormalmente o causar comportamientos inesperados si se terminan. Por otro lado, SecureEntry no puede afrontar el riesgo de no terminar todos los procesos que se ejecutan en contexto de superusuario/usuario en tiempo de conclusión/desconexión a no ser que explícitamente así se diga, puesto que cualquier programa PM podría teóricamente reanudar su ejecución, comprometiendo así la seguridad del sistema.

La idea es que si Vd. encuentra terminaciones anormales de un cierto proceso en tiempo de conclusión, tenga la oportunidad de añadir su nombre a la lista y dicho proceso no será terminado.

Un segundo propósito de este archivo es poder especificar una serie de comandos de 'cierre ordenado' siempre que SecureEntry deba finalizar un proceso dado. Esto es útil tanto por razones de rendimiento como cuando una aplicación no termina correctamente debido a dependencias existentes entre distintos procesos.

Después de aplicar una actualización a su versión de SecureEntry, el nuevo archivo EDYKILL.NOT proporcionado por defecto será copiado al directorio VíaDeAccesoSecureEntry\EXEC. Si el archivo VíaDeAccesoSecureEntry\NOUSER\EDYKILL.NOT no ha sido modificado para su instalación particular, este será entonces automáticamente actualizado; en otro caso, usted tendrá que actualizarlo manualmente para que los cambios surtan efecto.

Lea la sección de comentarios de este archivo para obtener más información sobre él. Este archivo reside en la vía de acceso SecureEntry, subdirectorio NOUSER, y acepta carácteres comodines en la especificación de los nombres de los procesos.

EDYSTART.CMD

Este archivo es la versión SecureEntry del archivo STARTUP.CMD y tiene exactamente el mismo propósito. La razón de que el nombre sea diferente se debe a que debe ser arrancado por SecureEntry para poder garantizar un arranque segura de la estación de trabajo. Lea el capítulo Proceso de arranque para obtener más información sobre su uso.

Objeto EdyStart

Este objeto, localizado en la vía de acceso SecureEntry, subdirectorio NOUSER, reemplaza a la tradicional carpeta de arranque de OS/2 y puede contener una lista de sombras. La diferencia con la carpeta de arranque del OS/2 radica en que SecureEntry garantiza que los programas arrancados en esta carpeta lo hacen en contexto de superusuario, esperando por esos objetos antes de proceder a la primera conexión (asumiendo que dichos objetos representan tareas asíncronas).

EDYUCFPW.DSC

Este es un archivo ASCII que contiene la lista del conjunto de carácteres válidos, la longitud mínima y máxima permitida para la validación de passwords del emulador de RACF. Por defecto, en este archivo, la longitud máxima de las passwords está puesta a 14 y la mínima a 4. El conjunto de carácteres permitidos por defecto son los siguientes:

```
A..Z, 0..9, a..z, @, # y $
```

Recuerde que si desea actualizar este archivo con sus propias restricciones para las passwords, también deberá actualizar las mismas definiciones en el Host de la corporación.

Archivos de Anotaciones de SecureEntry

Vd. puede seguir la actividad de SecureEntry en cualquier momento a través de los varios archivos usados para el propósito de rastreo o auditabilidad:

El archivo de anotaciones de instalación

Este archivo refleja toda la actividad del sistema en tiempo de instalación y servicio. Su nombre es 'SENTRY.LOG' y reside en la vía de acceso SecureEntry, directorio INSTALL. Sirva como muestra el siguiente ejemplo:

```
Inicio de instalación SecureEntry : 4 Mar 1998 22:10:25
Aplicando: SecureEntry Production Copy Versión: 3.0 Nivel: 191
Secure Entry start setup : 4 Mar 1998 22:11:47
Relocating base system files..
Creating SENTRY database..
Creating SENTRY logon configuration file..
Creating SENTRY STARTUP file..
Setting up default profiles
Setting up association types
Associated file :D:\SGMSHELL\TEMPLATE\EDYPAD.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYDD32.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYFLOPP.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYSES.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYWIN.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYWINS.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYDDSM1.CFG
Associated file :D:\SGMSHELL\TEMPLATE\EDYDDSM2.CFG
Associated file :D:\SGMSHELL\NOUSER\EDYFLOPP.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYWDLST.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDY_PER.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYMPER.INI
Associated file :D:\SGMSHELL\TEMPLATE\SHADOWS
Associated file :D:\SGMSHELL\EXEC\EDYSTART
Associated file :D:\SGMSHELL\TEMPLATE\EDYHOTK.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYCUSWP.INI
Associated file :D:\SGMSHELL\TEMPLATE\EDYSC.INI
Modifying CONFIG.SYS file..
Registering SYS_DLLs..
SecureEntry start crwrk : 4 Mar 1998 22:12:07
Se ha creado la carpeta 'SecureEntry:^Herramientas de Administración'
Se ha creado la sombra del objeto 'SecureEntry:^Herramientas de Administración'
Saving current launchpad..
Setting up syslevel file
Looking for setup hooks
SENTRY setup completed correctly..
You must shutdown now to activate changes and start Secure Entry.
La preparación del sistema terminó correctamente
```

El archivo de anotaciones del proceso de arranque

Este archivo contiene todos los mensajes enviados al proceso de arranque durante su ejecución. Su nombre es 'EDYLKINI.LOG' y reside en el mismo directorio que el archivo 'EDYSTART.CMD', es decir, el directorio raíz de la partición de arranque, a no ser que la variable de entorno 'SGM_INI_LOGPATH' en el archivo config.sys establezca otro lugar. Este archivo es útil para conocer qué fué mal en el arranque de la estación de trabajo en un entorno desatendido. Lea la descripción del proceso de arranque para obtener información más detallada.

El archivo de anotaciones de la administración

Este archivo refleja toda la función (API) de administración. Su nombre es 'EDYADMIN.LOG' y reside en la vía de acceso SecureEntry, subdirectorio NOUSER, en todas las estaciones de trabajo aisladas o en las estaciones de trabajo servidoras en entornos de red. Vd. puede cambiar su localización estableciendo la variable de entorno 'SGM_SL_LOGPATH' dentro del archivo config.sys. Sirva como muestra el siguiente ejemplo:

```
Date       Time   Computer User    Typ Process      Agent    Rc  Actn Subs ObjType Obj1 Obj2
Keys
-------------------------------------------------------------------------------------------
-
23/09/1996 22:50:14         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] ADD  SENT Group  GRUPO
LAN_DATA
23/09/1996 22:50:27         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] ADD  SENT User  LUIS
LAN_DATA
23/09/1996 22:50:28         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] ADD  SENT UserGroup LUIS,GRUPO
23/09/1996 22:51:57         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] UPDT SENT Group  GRUPO
FLOPPY_DISK
23/09/1996 23:01:34         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] ADD  SENT User   ADMIN2
LAN_DATA
23/09/1996 23:01:58         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] UPDT SENT User   ADMIN2
LAN_DATA
23/09/1996 23:02:26         EDYADMIN A EDYSNADM.EXE EDYSEAGT[ ] UPDT SENT User   EDYADMIN
LAUNCHPAD
```

El archivo de anotaciones de eventos de sesión

Este archivo refleja toda la actividad de sesión del sistema. Su nombre es 'EDYSLA.LOG' y reside en el camino OS2\SECURITY\SESDB de la partición de arranque del sistema. Vd. puede cambiar su localización estableciendo la variable de entorno 'SGM_SES_LOGPATH' dentro del archivo config.sys. Sirva como muestra el siguiente ejemplo:

```
  Date     Time      Event    Phase  Result   UserId              Additional info
-------- -------- ----------- ------ ------ -------- ---------------------------------------
11/21/99 11:43:13 DOMAIN      QUERY   [ ]            Default Domain:   SEDOMAIN
11/21/99 11:44:58 SHUTDOWN    START   [ ]
11/21/99 12:19:57 SHUTDOWN    END     [C]
11/21/99 11:45:05  LOGON       START   [ ]   U0000007 Domain:  SEDOMAIN
11/21/99 11:46:37  LOGON       END     [ ]   U0000007
11/21/99 11:47:33 LOCKUP      START   [ ]   U0000007
11/21/99 11:47:33 LOCKUP      END     [ ]   U0000007
11/21/99 11:47:38 UNLOCK      START   [ ]   U0000007
11/21/99 11:47:46 UNLOCK      END     [E]   U0000007 You typed and invalid Password. Try
again.
11/21/99 11:47:51 UNLOCK      END     [ ]   U0000007
11/21/99 11:48:21  LOGOFF      START   [ ]   U0000007
11/21/99 11:48:30  LOGOFF      END     [C]   U0000007
11/21/99 11:48:43 SHUTDOWN    START   [ ]   U0000007
11/21/99 11:48:49 SHUTDOWN    END     [C]   U0000007
```

El archivo de anotaciones de Treelock

El componente de Treelock puede configurarse para auditar los accesos del usuario al sistema de archivos en un archivo ASCII. Como este archivo se trata como cualquier otro componente, Vd. puede

ponerlo en el directorio NOUSER, o asignar uno en base a cada usuario. Lea la descripción del componente de Treelock para obtener más información sobre este archivo.

El archivo de anotaciones de aplicaciones públicas

Este archivo contiene los errores y mensajes encontrados por el componente de aplicaciones públicas durante su ejecución.

El archivo de anotaciones de datos distribuidos

Este archivo almacena la información relacionada con la actividad de actualización en línea de oficinas y con la actualización en línea de perfiles de seguridad. En este archivo encontrará si los procesos de actualización se ejecutaron correctamente. Su nombre es 'EDYDIS.LOG' y reside en la vía de acceso SecureEntry, subdirectorio NOUSER en la máquina servidora. Usted puede cambiar la ubicación estableciendo la variable de entorno SGM_UCM_LOGPATH en el archivo config.sys de la máquina.

Sirva como muestra el siguiente ejemplo:

```
10/28/98 12:16:48 < REFRESH BRANCH ONLINE BEGINS >

> REFRESH STATISTICS
    Buffer Length  : 34738
    Final Register found
>   Read Blocks    : 4
>   Correct Blocks : 4
>   Error Blocks   : 0
>   Number of Add Object Operations    : 1
>   Number of Update Object Operations : 2
>   Number of Delete Object Operations : 1

10/28/98 12:16:57 < REFRESH BRANCH ONLINE ENDED  >
```

Se puede controlar el tamaño de los archivos de anotaciones de SecureEntry, así como cualquier otro archivo ASCII utilizando la utilidad EDYLOGFS.

Acerca de los Procesos y los Contextos de Ejecución

En un sistema SecureEntry, todo proceso del sistema tiene un contexto de ejecución asociado a seguridad. Esto significa que el sistema toma nota del usuario que lanzó el proceso y sus privilegios. Básicamente, hay dos contextos de ejecución:

1. **Contexto de Superusuario** Todos los procesos arrancados en contexto de superusuario no tienen ningún tipo de restricción en el sistema de archivos (el treelock no hace ninguna validación en cuanto a sus accesos), ni son terminados en tiempo de desconexión de la sesión de usuario.
2. **Contexto de Usuario** Todos los procesos arrancados en contexto de usuario estarán sometidos a las restricciones del perfil de treelock actual en cuanto a sus accesos al sistema de archivos se refiere; además, estos procesos serán terminados en tiempo de desconexión de la sesión del usuario, a no ser que se especifique lo contrario en el archivo EDYKILL.NOT.

La pregunta inmediata que se desprende en este momento es cómo discernir qué procesos se ejecutan en un contexto u otro:

Los Procesos arrancados en el archivo CONFIG.SYS se ejecutan en contexto de superusuario.

Los Procesos arrancados en el archivo EDYSTART.CMD se ejecutan en contexto de superusuario.

Los Procesos arrancados en el objeto EDYSTART de la carpeta NOUSER se ejecutan en contexto de superusuario.

Los Procesos arrancados durante una sesión de usuario (entre la conexión y la desconexión) se ejecutan en contexto de usuario.

Los Procesos arrancados desde una Exit de usuario se ejecutan en el contexto asociado a dicha Exit de usuario:

Exit de usuario después del arranque: Contexto de Superusuario
Exit de usuario antes del dialogo de conexión: Contexto de Superusuario
Exit de usuario antes de la conexión: Contexto de Superusuario
Exit de usuario antes de la conexión a LMP: Contexto de Superusuario
Exit de usuario después de la conexión a LMP: Contexto de Superusuario
Exit de usuario anterior a la activación de perfiles: Contexto de Usuario
Exit de usuario después de la conexión: Contexto de Usuario
Exit de usuario después del PMSHELL : Contexto indefinido (depende del momento exacto)
Exit de usuario antes del bloqueo cancelable: Contexto de Usuario
Exit de usuario antes del bloqueo: Contexto de Usuario
Exit de usuario antes del dialogo de desbloqueo: Contexto de Usuario
Exit de usuario antes del desbloqueo: Contexto de Usuario
Exit de usuario después del desbloqueo: Contexto de Usuario
Exit de usuario posterior a un intento fallido de desbloqueo: Contexto de Usuario
Exit de usuario señal: Contexto indefinido (depende del momento exacto)
Exit de usuario antes de la desconexión cancelable: Contexto de Usuario
Exit de usuario posterior a la desactivación de perfiles: Contexto de Usuario
Exit de usuario antes de la desconexión inminente: Contexto de Usuario
Exit de usuario después de la desconexión: Contexto de Superusuario
Exit de usuario antes de la conclusión: Contexto de Superusuario
Exit de usuario antes de la desconexión desde el desbloqueo: Contexto de Usuario
Exit de usuario antes de la desconexión desde el desbloqueo: Contexto de Usuario
Exit de usuario antes de la desconexión a LMP: Contexto de Usuario
Exit de usuario después de la desconexión a LMP: Contexto de Usuario
Exit de usuario de apertura de carpeta: Contexto indefinido (depende del momento exacto)

Acerca de los IDs de los Objetos

A la hora de administrar SecureEntry, encontrará varios componentes que solamente aceptan objetos que tengan asignado un ID de objeto para poder realizar ciertas operaciones. Esto se debe a que el ID de un objeto es la única manera de identificar unívocamente un objeto del Escritorio que deba retener esta característica en cualquier estación de un grupo de trabajo SecureEntry.

Muchos objetos tienen ya definido un ID de objeto, por lo que Vd. no debe preocuparse por ello hasta que encuentre un problema. En el caso de quiera trabajar con un objeto para el que se requiere un ID de objeto, el siguiente pequeño programa en REXX le ayudará a asignarle uno:

```
/* */
Call rxfuncadd sysloadfuncs, rexxutil, sysloadfuncs
Call sysloadfuncs
```

```
/* asignar a CaminoObjeto el camino completo del objeto */

result=SysSetObjectData(CaminoObjeto,  'OBJECTID=<'||IdNuevo||'>')
```

Los IDs de objetos deben ser únicos. Deberá Vd. repetir este comando en todas las estaciones donde el objeto vaya a ser usado por SecureEntry.

Remítase a IDs de Objetos de Aplicaciones Públicas. para obtener más información sobre este tipo de objetos LAN Server.

Descripción del Proceso de Sesión de SecureEntry

Hasta este momento se ha estado describiendo SecureEntry como una serie de componentes separados, pero para tener una idea clara de lo que pasa 'entre bastidores', en términos de secuenciación de eventos, se describen a continuación todos los procesos.

En el momento de inicio del sistema, la secuencia de eventos es como sigue:

1. Inicio del sistema
2. Ejecución del código de inicio y proceso del archivo config.sys
3. Carga de los controladores de dispositivos de SecureEntry y activación de SES
4. Segunda pasada sobre el archivo config.sys, sirviendo las sentencias 'call='
5. Carga de los servicios de PM. Carga de los ganchos (hooks) PM de SecureEntry
6. Asíncronamente en este punto, y dependiendo de si así está configurado, OS/2 puede lanzar los programas de fondo (daemons) que acabaran por cargar el WPS. Siempre que el WPS se cargue y esté en un estado estable, SecureEntry servirá la Exit de usuario de después del PMSHELL. Esto ocurre generalmente no antes de que se completen varios de los siguientes pasos
7. Procesos SecureEntry contenidos en el archivo EDYSTART.CMD (proceso de arranque)
8. SecureEntry sirve la Exit de usuario de después del arranque
9. SecureEntry fuerza un evento de conexión SES
10. El SES devuelve el control de flujo a SecureEntry para procesar el evento de conexión
11. **(CONEXION)** Proceso del evento de conexión SES: SecureEntry sirve la Exit de usuario de antes del dialogo de conexión. Si el usuario decide hacer una conexión de Invitado, entonces ir a **INVITADO**
12. SecureEntry inspecciona el área de parámetros de la conexión y decide si presentar el panel de conexión o saltar el siguiente paso
13. Se muestra el panel de conexión. Si el usuario pulsa 'OK' ir al siguiente paso; si el usuario pulsa 'CONCLUIR' ir a **CONCLUSION**
14. SecureEntry sirve la Exit de usuario de antes de la conexión. Si el usuario decide realizar una conexión de Invitado, ir a **INVITADO**
15. SecureEntry sirve la Exit de usuario de antes de la conexión cambiando la contraseña si se ha solicitado un cambio de contraseña en esa conexión

16. SecureEntry realiza una conexión a la cadena de LMPs en el orden definido en el archivo EDYSSLMP.DAT, sincronizando las contraseñas si fuera necesario. Si hay un error, ir a **CONEXION**

17. SecureEntry obtiene los perfiles de seguridad para el usuario que acaba de realizar la conexión y los almacena en la vía de acceso SecureEntry, directorio WORK, anulando si fuera necesario los perfiles de grupo con los del usuario. Si hay un error, ir a **CONEXION**

18. SecureEntry activa cada componente para el que se obtuvo un perfil de seguridad, siguiendo la interfície definida en la base de datos del repositorio Si hay un error, ir a **CONEXION**

19. **(INVITADO)** SecureEntry sirve la Exit de usuario de después de la conexión

20. SecureEntry sirve la Exit de usuario de después de la conexión cambiando la contraseña si se solicitó un cambio de contraseña en esta conexión

21. Empieza la sesión de trabajo del usuario. Sólo una petición de desconexión o conclusión hará salir al sistema de este estado, y continuar con el siguiente paso. Cualquier proceso arrancado dentro de la sesión de usuario será tratado como proceso de usuario, por lo que será terminado en tiempo de desconexión

22. Se realiza una petición para la desconexión del usuario o conclusión del sistema. Se lanza el evento apropiado (desconexión o conclusión) al SES

23. SecureEntry sirve la Exit de usuario de antes de la desconexión cancelable. Si se recibe una cancelación, el control de flujo vuelve a la sesión de usuario (paso anterior). Sino, SecureEntry visualiza, si así está configurado, el dialogo de confirmación como última oportunidad para permanecer dentro de la sesión de usuario

24. SecureEntry sirve la Exit de usuario de antes de la desconexión inminente

25. SecureEntry termina todos los procesos ejecutándose en contexto de usuario

26. SecureEntry desactiva todos los componentes obtenidos en tiempo de conexión informándoles de que deben activar los perfiles almacenados en el subdirectorio NOUSER (perfiles de configuración por máquina)

27. SecureEntry guarda en el repositorio central cualquier perfil de componente que haya sido modificado por el usuario, y lo borra del subdirectorio de trabajo WORK

28. SecureEntry lanza la desconexión a la cadena de LMPs, llamando sólo a esos LMPs que se utilizaron en tiempo de conexión.

29. SecureEntry sirve la Exit de usuario de después de la desconexión

30. Si el evento que se ha procesado era un evento de desconexión, se lanza un evento de conexión de SES que causa un salto a **CONEXION**, y el evento de desconexión termina

31. **(CONCLUSION)** SecureEntry sirve la Exit de usuario de antes de la conclusión

32. SecureEntry termina todos los procesos aún vivos ejecutándose en primer plano

33. SecureEntry devuelve control al SES para que realice una conclusión del sistema, quien a su vez acabará llamando a la función (API) de conclusión del OS/2

Afinando SecureEntry. Consideraciones de Rendimiento

Hay varios factores que afectan al rendimiento en la operativa de SecureEntry. Siga este capítulo para hallar pistas sobre cómo afinar su sistema.

El afinado del rendimiento consigue sus mejores resultados si se centra Vd. primero en los 'cuellos de botella' del sistema. Son síntomas de tales cuellos de botella:

Tiempo de respuesta del sistema excesivamente lento, y posiblemente demasiada actividad de disco. Esto es en general un indicador de falta de memoria, y se acompaña por un tamaño excesivamente grande de archivos de intercambio (al compararlos con la cantidad de memoria instalada). Esta situación se merece una sesión completa de afinado del sistema y seguramente terminará por añadir más memoria al sistema.

Afinado general del rendimiento del sistema operativo

Problemas de rendimiento específicos en momentos muy puntuales, por ejemplo, en tiempo de conexión de la sesión. Este síntoma normalmente indicada otro tipo de problema, y si ocurre dentro de SecureEntry, podrá ser subsanado siguiendo las instrucciones bajo 'Afinado del rendimiento específico de SecureEntry'.

Afinado del rendimiento específico de SecureEntry

Afinado general del rendimiento del sistema operativo

A la hora de mejorar el rendimiento en un sistema OS/2, se pueden emprender las siguientes acciones:

Afinado Software

1. Archivo de intercambio: este archivo debería residir en la partición más usada del disco físico menos usado. También es conveniente preasignar su tamaño a uno para el que no deba ser contraído ni expandido dinámicamente. Utilice la sentencia SWAPPATH del archivo config.sys, tal y como sigue:

   ```
   SWAPPATH=D:\ 8192 16384

   Establezca el archivo de intercambio en el directorio raíz de la
   unidad D, con un tamaño inicial de 16Mb, haciendo que el sistema
   envíe una alerta en el caso de que el espacio libre sea de menos
   de 8Mb
   ```

2. Antememoria en disco: generalmente un tamaño de antememoria en disco lo suficientemente grande también mejora el rendimiento. Utilice la sentencia DISKCACHE para unidades FAT, y/o las sentencias CACHE/IFS para unidades HPFS. No olvide establecer los valores de grabación diferida para conseguir un rendimiento óptimo!!
3. Desinstale programas/drivers que no utilice. Por ejemplo, extensiones multimedia, o drivers HPFS si Vd. no utiliza este sistema de archivos.
4. Recuerde inhabilitar los rastreos y/o verificar los conmutadores en los entornos de ejecución de usuario final. Otros artilugios como la 'animación de ventanas' pueden ralentizar el sistema.
5. Intente mantener su disco desfragmentado, y si es posible utilice particiones formateadas bajo el sistema de archivos HPFS en lugar de FAT, especialmente para particiones grandes.
6. Realice un afinado de las sentencias LIBPATH, SET PATH, y SET DPATH del archivo config.sys, poniendo primero esos directorios a los que se acceden más frecuentemente.

7. En máquinas rápidas, y especialmente si se trata de servidores, puede ser conveniente reducir los parámetros de configuración de reparto de tiempos entre procesos : **TIMESLICE** y **MAXWAIT**, para mejorar la repuesta media del sistema (por ejemplo, poniendo TIMESLICE=32,512 y MAXWAIT=1).
8. Si utiliza aplicaciones de Windows, puede ser una buena idea establecer el valor de Carga Rápida de WINOS2 (esta acción se realiza en la página Sesión 3.1 del cuaderno de valores del objeto Configuración de Win-OS2), y ejecutar todas las aplicaciones Windows desde la misma sesión.
9. Para afinar el rendimiento en tiempo de arranque, Vd. puede hacer lo siguiente:

   Mantener optimizados los archivos .INI del sistema (OS2.INI y OS2SYS.INI). Existen varias utilidades que pueden ayudarle en esto. En concreto, SecureEntry provee la utilidad : EDYCLINI.

   Recuerde desactivar el archivado de sus archivos críticos en cada arranque. Dicho archivado sólo debería hacerse cuando se hacen actualizaciones importantes en el sistema. Esta acción se realiza en la página Archivador del cuaderno de valores del Escritorio.

Afinado Hardware

1. En general, la manera de mejorar el rendimiento consiste en añadir más memoria. Empiece con las estaciones de trabajo servidoras.
2. Considere también añadir antememoria L2 a su sistema, si su hardware lo soporta.
3. Por supuesto, procesadores y discos más rápidos también ayudan mucho.
4. Piense en aumentar las velocidades de conexión al host, especialmente si usa UCM.
5. En instalaciones basadas en red, tenga en cuenta el rendimiento de la red y problemas de contención, que pueden solventarse dividiendo la red o aportando cambios en el hardware.

Afinado del rendimiento específico de SecureEntry

A pesar de que SecureEntry se instala con la mayoría de las opciones establecidas para un mejor rendimiento, las siguientes reglas le ayudaran para mejorar el tiempo de respuesta aún más:

SecureEntry no tiene un requisito mínimo de memoria física. Sin embargo, debe Vd. considerar que el tamaño aproximado del conjunto de trabajo (working set) del código está alrededor de los 3Mb, siendo esta la cantidad de memoria física que debería Vd. añadir al sistema si su objetivo es conseguir el mismo nivel de rendimiento que tendría sin SecureEntry y con el mismo hardware. Tenga en cuenta también que SecureEntry mantiene constantemente un mínimo de 15 pasos de ejecución activos, por lo que Vd. debería incrementar en esta cantidad la sentencia THREADS del archivo config.sys.

En entornos de LAN Server, tenga en cuenta que la mayor parte del tiempo dedicada a la conexión la realiza el propio LAN Server, por lo que, en general, afinar el rendimiento del LAN Server producirá una mejoría notable en el rendimiento de SecureEntry.

También para entornos de red, eche un vistazo a los parámetros de protocolo de su archivo PROTOCOL.INI, que reside en el directorio IBMCOM. Los programas de base de red normalmente se instalan con unos parámetros por defecto excesivamente conservadores para entornos tan simples tales como la típica red de oficina bancaria. Esto explica por qué simplemente cambiando el parámetro NETBIOSTIMEOUT de 2000 a 500 milisegundos puede Vd. reducir significativamente el tiempo de conexión en 20 segundos. Otro parámetro que le ayudará a mejorar el tiempo de respuesta en redes rápidas sin puentes (bridges) es el NETBIOSRETRIES; redúzcalo a 2 o 3.

Si tiene Vd. problemas en tiempo de conexión, cronometre lo que tarda todo un proceso de conexión (no en la primera conexión), y verifique si la mayor parte del tiempo se consume en uno de los siguientes supuestos:

1. Cuando el panel de conexión es visible, pero la ventana 'Conexión en curso... Por favor, espere' aún no ha aparecido. En este caso, inspeccione su código de Exit de usuario o alguna otra actividad realizada por el sistema al mismo tiempo.
2. Cuando el panel de conexión es visible y ventana 'Conexión en curso... Por favor, espere' ya ha aparecido. En este caso, el tiempo se reparte entre la validación a RACF, la obtención de perfiles del UCM y la validación y conexión al LAN Server. Estos son los componentes que hay que inspeccionar.
3. Cuando el panel de conexión ha desaparecido. Inspeccione en este caso en qué se gasta el tiempo una vez se han activado los perfiles de seguridad individuales.

Evite usar excesivo código de Exit de usuario cuando sea posible. Las Exits de usuario son un mecanismo muy potente, y al mismo tiempo caro. Una excepción a esta regla se da cuando es necesario terminar alguna aplicación. Siempre será más eficiente hacerlo utilizando el comando más adecuado que dejar esa tarea a SecureEntry, que desconoce los mecanismos internos de los procesos que componen un paquete de software particular. Utilice para ese propósito el archivo EDYKILL.NOT o la Exits de usuario de antes de la desconexión inminente y/o la Exit de usuario de antes de la conclusión.

Intente utilizar componentes asignados a máquina (en el directorio NOUSER) antes que componentes asignados a grupo o usuario, ya que esto ahorrará tiempo al no tener que activar/desactivar los mismos perfiles a cada conexión/desconexión.

Considere la posibilidad de establecer la variable de entorno 'SGM_WPS_FASTLOAD' en el archivo config.sys. Tenga en cuenta entonces los riesgos expuestos bajo Variables de Entorno. Esta variable de entorno sólo modifica la 'percepción' de conexiones más rápidas, puesto que la población del Escritorio se anticipará unos segundos.

No cambie el valor por defecto de la variable de entorno RESTARTUSERSHELL ('NO'), excepto cuando así lo requiera su instalación. Rearrancar el WPS en cada conexión retrasará el tiempo de conexión fácilmente unos segundos.

Sitúe la vía de acceso SecureEntry tan al principio como sea posible en las sentencias LIBPATH y SET PATH del archivo config.sys.

Deje también la variable de entorno 'SGM_WPS_SKIP_PREPOPULATE' con el valor establecido por la instalación de SecureEntry ('ALL').

Suprima todas las anotaciones/rastreos innecesarios. Por ejemplo, establezca el nivel de rastreo a 0 añadiendo a su archivo EDYSTART.CMD:

```
EDYTRSET /A:0
```

Dos consideraciones para el componente de la barra de herramientas personalizadas:

1. Intente establecer barras de herramientas que contengan sólo objetos con ID de objeto. Añadir objetos a una barra de herramientas (cuando se crea), consume mucho más tiempo si los objetos a añadir no tienen ID de objeto.
2. Si se instala en una máquina antigua, es decir, el OS/2 ha estado instalado en la máquina desde hace mucho tiempo, puede ser una buena idea 'limpiar' el directorio Nowhere con una herramienta como la suministrada EDYCLINI. Las sombras de barras de herramientas antiguas

(no SecureEntry) acaban en este directorio y jamás son borradas por el propio sistema, haciendo que el acceso a objetos que residen en este lugar sea más lento.

AVISO: Haga esto sólo si Vd. encuentra muchos objetos en la carpeta NoWhere.

Si los archivos de mapas de imágenes de fondo o de salvapantallas son grandes, tenga en cuenta que no tan sólo ocuparán mucho espacio en disco, sino que además su lectura será costosa en tiempo, y se puede generar cierta actividad de intercambio, por lo que se trata de obtener un compromiso entre la calidad de la imágen y el tiempo de respuesta. Si finalmente decide usar mapas de imágenes grandes, entonces intente utilizar archivos del mismo tamaño en pixels/colores que la resolución de su Escritorio, puesto que esto evitará funciones de remapeo del color y de cambio de tamaño que se demuestran caras en proceso.

Códigos y Mensajes de Error

Errores y Mensajes de Control de Sesión

Los siguientes errores pueden aparecer durante la ejecución normal y en funciones de control de sesión, es decir, conexión, desconexión, bloqueo... Algunos de ellos pueden aparecer también a través de las funciones (APIs) de administración.

Número de Mensaje	Mensaje	Descripción
EDY0001E	La contraseña es incorrecta.	La palabra clave proporcionada no es válida para este usuario durante una operación de conexión o desbloqueo.
EDY0002E	Error interno.	Se ha producido un error de sistema operativo genérico. El mensaje puede contener información adicional. Inspeccione los archivos de rastreo o de anotaciones para obtener mayor información.
EDY0003E	Subsistema %s no disponible.	Un subsistema requerido no estuvo disponible en el momento de realizar la conexión. (SR: Registro de SecureEntry, LS: LAN Server, UC: UCM, RF: RACF..).
EDY0004E	Error en el Archivo de Control (EdyxxLmp.dat).	Inspeccione la integridad del archivo *EDYSSLMP.DAT*. Probablemente ha sido alterado.
EDY0005E	Estación en estado de desconexión: ningún usuario está conectado.	Una operación que necesitaba de una conexión encontró que ningún usuario la tenía establecida (típicamente puede ocurrir en tiempo de desconexión si se realizó una desconexión del LAN Server durante la sesión de usuario).
EDY0006E	Usuario desconocido.	El ID de usuario no se encontró en el subsistema al que se intentó conectar.
EDY0007E	Ya existe un usuario conectado en esta estación de trabajo.	EL subsistema de conexión encontró a un usuario ya conectado durante el proceso de conexión.
EDY0008E	La contraseña ha expirado.	La contraseña ha expirado. Vd. debe cambiar la

		contraseña para continuar.
EDY0009E	La nueva contraseña es inválida.	La nueva contraseña es inválida. Es demasiado corta, demasiado larga, contiene carácteres inválidos, o es idéntica a una de las últimas contraseñas utilizadas.
EDY0010E	Alguno de los datos de entrada es incorrecto.	Error interno. Contacte con el personal de soporte del servicio.
EDY0011E	Usuario con conexión denegada.	La cuenta de usuario ha sido revocada. Contacte con su administrator del sistema.
EDY0012E	No se ha podido cargar la DLL %s.	No se pudo encontrar la DLL especificada durante la inicialización del subsistema de conexión.
EDY0080E	Error general en la manipulación de los Perfiles de Seguridad.	Error interno. Contacte con el personal de soporte del servicio.
EDY0081E	Error al acceder a la memoria compartida.	Inspeccione los recursos del sistema y/o contacte con el personal de soporte del servicio.
EDY0082E	Memoria compartida llena.	Error interno. Contacte con el personal de soporte del servicio.
EDY0083E	Información no disponible en la memoria compartida.	Error interno. Contacte con el personal de soporte del servicio.
EDY0084E	La memoria reservada para los datos de salida es insuficiente.	Error interno. Contacte con el personal de soporte del servicio.
EDY0085E	Error leyendo archivo INI.	Error interno. Contacte con el personal de soporte del servicio.
EDY0086E	Etiqueta no encontrada en archivo INI.	Error interno. Contacte con el personal de soporte del servicio.
EDY0087E	Archivo no encontrado.	El archivo solicitado no existe.
EDY0088E	Error copiando archivo.	El archivo solicitado no pudo ser copiado.
EDY0100W	Conexión en estado de emergencia: (el subsistema %s no está disponible). No se permite realizar un cambio de Contraseña.	Los subsistemas de conexión básicos están disponibles, pero el subsistema principal (típicamente el RACF) falló. Está Vd. conectado en modo de emergencia. Debido a ello, no se permite realizar un cambio de Contraseña.
EDY0101W	Archivo de Control: se ha llegado al final de archivo.	Inspeccione la integridad del archivo *EDYSSLMP.DAT*. Probablemente ha sido alterado.
EDY0102W	Archivo de Control: línea vacía.	Inspeccione la integridad del archivo *EDYSSLMP.DAT*. Probablemente ha sido alterado.
EDY0103W	Petición pendiente.	Error interno. Contacte con el personal de soporte del servicio.
EDY0104W	Archivo de Control: línea que indica la localización de la Base de Datos de usuarios.	Inspeccione la integridad del archivo *EDYSSLMP.DAT*. Probablemente ha sido alterado.
EDY0105W	Archivo de Control: línea que indica la localización de la Base de Datos de perfiles de seguridad.	Inspeccione la integridad del archivo *EDYSSLMP.DAT*. Probablemente ha sido alterado.

EDY0110E	Fallo general de Lan Server.	El Lan Server estaba disponible pero falló. Causas posibles son un error interno de Lan Server, demasiados nombres en el archivo de control de accesos, error de acceso al archivo NET.ACC, y otros.
EDY0111E	Error de configuración de Lan Server.	Se ha encontrado un error relacionado con la configuración de Lan Server o nivel de código. O no se encontró el nombre de camino a la red, o la petición de una función (API) no está soportada, o el nombre del equipo no es válido, o el servidor está configurado erróneamente.
EDY0112E	Algunos de los servicios de Lan Server todavía no han sido arrancados.	Este error no debería aparecer en ningún caso. En todo caso podría aparecer el error EDY0003.
EDY0113E	Dominio incorrecto. Entre un nuevo dominio.	No se pudo obtener el nombre del servidor de dominio. Contacte con su administrador de sistema.
EDY0114E	Son necesarios privilegios de Administrador para realizar esta operación.	El Lan Server desautorizó la petición expresamente.
EDY0115E	El Identificador de usuario y/o la contraseña son incorrectos.	Probablemente el programa EDYSRV no está ejecutándose en la estación de trabajo controladora del dominio. Debido a ello, no se pudo refinar más el código de error y se devolvió este, que es más genérico.
EDY0116E	Lan Server: Este usuario ya está conectado en la LAN.	Su Lan Serverno está configurado para aceptar múltiples conexiones, y Vd. está intentando conectarse mientras ya lo está en otra máquina.
EDY0117E	Lan Server: En proceso de Conexión/Desconexión, o el Lan Requester está activo.	En estos momentos está en curso otra operación de conexión o desconexión.
EDY0118E	Lan Server: La cuenta del usuario ha expirado.	La cuenta del usuario ha expirado. Contacte con su administrador de sistema.
EDY0119E	Lan Server: La nueva contraseña es demasiado corta.	Autoexplicativo.
EDY0120E	Lan Server: La nueva contraseña es muy reciente.	Autoexplicativo.
EDY0121E	Lan Server: La contraseña no puede ser cambiada.	Autoexplicativo.
EDY0122E	Lan Server: Hora de conexión inválida.	Autoexplicativo.
EDY0123W	Controlador de dominio principal no disponible. Se esta usando el controlador de reserva.	Informativo: No se encontró el controlador de dominio principal. Un controlador de dominio secundario (de backup) ha tomado su papel.
EDY0201E:	Conexión a demasiados subsistemas.	Error interno. Contacte con el personal de soporte del servicio.
EDY0202E:	El identificador del	Error interno. Contacte con el personal de soporte

	subsistema %s es incorrecto.	del servicio.
EDY0203E:	Petición no autorizada. Acceso denegado.	El Registro de SecureEntry informó que la petición no está autorizada.
EDY0204E:	El usuario %s ya existe.	No se pudo añadir el grupo/usuario puesto que ya estaba definido como usuario en el Registro de SecureEntry.
EDY0205E:	El grupo %s ya existe.	No se pudo añadir el grupo/usuario puesto que ya estaba definido como grupo en el Registro de SecureEntry.
EDY0206E:	El componente %s ya existe.	No se pudo añadir el perfil de un componente puesto que ya existía.
EDY0207E:	El grupo %s no existe.	El grupo solicitado no existe en el Registro de SecureEntry.
EDY0208E:	El grupo %s no está vacío.	No se puede borrar un grupo del Registro de SecureEntry mientras haya usuarios definidos en él.
EDY0209E:	No se puede borrar al usuario actualmente conectado.	El usuario conectado no puede ser dado de baja.
EDY0210E:	El nombre de componente %s es inválido.	El componente no se ha registrado como componente válido al Registro de SecureEntry, o la sintaxis del nombre es inválida.
EDY0211E:	El componente %s no existe.	El perfil del componente no se ha podido modificar/borrar porque no está definido para el usuario/grupo especificado.
EDY0212E:	No se pudo cargar la DLL %s.	El Registro de SecureEntry no pudo cargar la DLL especificada. Asegúrese de que existe y que está accesible a través de la sentencia LIBPATH del archivo config.sys.
EDY0213E:	No se pudo encontrar la dirección de %s.	Error interno. Contacte con el personal de soporte del servicio.
EDY0214E:	La Base de Datos de Usuarios no está definida sobre el Registry (EdyRegDB.vlb).	La operación solicitada sólo es válida para configuraciones aisladas.
EDY0215E:	La Base de Datos de Perfiles de Seguridad no está definida sobre el Registry (EdyRegDB.vlb).	Inspeccione la sintaxis y la integridad del archivo EDYSSLMP.DAT.
EDY0216E:	Error en la función (API) %s.	El Registro de SecureEntry obtuvo un error al solicitar información de configuración a EDYAPI. Inspeccione el error obtenido en esta misma tabla.
EDY0217E:	No se ha encontrado el subsistema del Sentry.	Probablemente hubo un error durante la instalación. Contacte con el personal de soporte del servicio.
EDY0218E:	Lista de componentes vacía.	Error interno. Contacte con el personal de soporte del servicio.
EDY0219E:	Error sintáctico en la lista de componentes: %s .	La lista de componentes registrados es errónea. Inspeccione el archivo SENTRY.DSC y vuelva a

		registrar los componentes a través de la utilidad UPDATEDB.
EDY0220E:	Componente %s desconocido.	El componente no está registrado como componente válido al Registro de SecureEntry.
EDY0221E:	El componente obligatorio %s no está presente.	Falta este componente obligatorio. El usuario no puede conectarse.
EDY0222E:	Error desconocido en EdyReg %d.	Se ha reportado un error desconocido al Registro de SecureEntry. Inspeccione el mensaje de error.
EDY0223E:	Clase de error desconocida en EdyReg %d.	Error interno. Contacte con el personal de soporte del servicio.
EDY0224W:	El nuevo componente es igual que el antiguo. No se almacenó de nuevo.	Informativo.
EDY0330E:	Error interno.	Error interno. Contacte con el personal de soporte del servicio.
EDY0331E:	Se ha producido un error de seguridad debido a una violación de integridad. El sistema iniciará el proceso de Conclusión.	Error interno. Contacte con el personal de soporte del servicio.
EDY0332E:	La longitud del Identificador de Usuario es incorrecta. Entre un nuevo valor.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0333E:	La longitud de la Contraseña es incorrecta. Entre un nuevo valor.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0334E:	La longitud del Dominio es incorrecta. Entre un nuevo valor.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0335E:	La Contraseña nueva y la de verificación no coinciden.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0337E:	La Contraseña es inválida. Entre un nuevo valor.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0338E:	Cambio de contraseña inválido. Contacte con el Administrador del Sistema.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0341E:	No tiene autorización para conectarse. Contacte con el Administrador del Sistema.	Error producido durante la validación sintáctica en los paneles de conexión y/o desbloqueo.
EDY0347E:	Se ha producido un Error de Inicialización Grave. Módulo: %s. Función: %s. línea: %d. Error de Sistema: %#X. El sistema concluirá.	Anote toda la información suministrada por el mensaje. Contacte con el personal de soporte del servicio.
EDY0349E:	El archivo de inicialización de OS/2 contiene una aplicación inválida. El programa que arregla este	El archivo de inicialización especificado por la variable de entorno USER_INI, normalmente el archivo OS2.INI que reside en el subdirectorio OS2 de la partición desde la que se arrancó el sistema

	problema no se pudo ejecutar. El sistema concluirá. Contacte con el Administrador del Sistema.	operativo, contiene el par *SYS_DLLS*/*Load* con un valor de llave inválido. Este error puede ser debido a que se hayan reemplazado los archivos de inicialización del sistema por otros que no contienen la información necesaria. El programa que utiliza SecureEntry para solventar este problema no pudo ejecutarse. Contacte con el personal de soporte del servicio.
EDY0350E:	El archivo de inicialización de OS/2 contiene una aplicación inválida. El programa que arregla este problema terminó de manera inesperada. El sistema concluirá. Contacte con el Administrador del Sistema.	El archivo de inicialización especificado por la variable de entorno USER_INI, normalmente el archivo OS2.INI que reside en el subdirectorio OS2 de la partición desde la que se arrancó el sistema operativo, contiene el par *SYS_DLLS*/*Load* con un valor de llave inválido. Este error puede ser debido a que se hayan reemplazado los archivos de inicialización del sistema por otros que no contienen la información necesaria. El programa que utiliza SecureEntry para solventar este problema acabó su ejecución de manera anómala. Contacte con el personal de soporte del servicio.
EDY0351E:	El archivo de inicialización de OS/2 contiene una aplicación inválida. El programa que arregla este problema no pudo corregirlo. El sistema concluirá. Contacte con el Administrador del Sistema.	El archivo de inicialización especificado por la variable de entorno USER_INI, normalmente el archivo OS2.INI que reside en el subdirectorio OS2 de la partición desde la que se arrancó el sistema operativo, contiene el par *SYS_DLLS*/*Load* con un valor de llave inválido. Este error puede ser debido a que se hayan reemplazado los archivos de inicialización del sistema por otros que no contienen la información necesaria. El programa que utiliza SecureEntry para solventar este problema no pudo corregir el problema. Contacte con el personal de soporte del servicio.
EDY0352E:	El archivo de inicialización de OS/2 contiene una aplicación inválida. El problema ha sido arreglado. El sistema concluirá. Contacte con el Administrador del Sistema si continúa teniendo el mismo problema.	El archivo de inicialización especificado por la variable de entorno USER_INI, normalmente el archivo OS2.INI que reside en el subdirectorio OS2 de la partición desde la que se arrancó el sistema operativo, contiene el par *SYS_DLLS*/*Load* con un valor de llave inválido. Este error puede ser debido a que se hayan reemplazado los archivos de inicialización del sistema por otros que no contienen la información necesaria. SecureEntry arregló la llave inválida del archivo de inicialización. Se hace necesario un re-arranque del sistema para que los valores válidos del surtan efecto. La reiteración de este error en el siguiente arranque del sistema indica un reemplazo automático de los archivos de inicialización del sistema operativo en algún momento del arranque.

Errores de función (API) de administración

A pesar de que estos errores se encontrarán normalmente trabajando directamente con la función (API) de administración, es posible obtener alguno de ellos cuando se usen las herramientas de administración. La idea es mirar el tipo de error y buscarlo en la lista de errores que dependen del componente último que causa la condición de error, tal y como sigue:

Tabla de Tipos de Errores

Código de Error	Tipo de Error	Descripción
xxxx	RXUC	La DLL de la capa de REXX encontró un error. Busque en el mensaje apropiado para obtener más información.
xxxx	SLAG	Error del agente selector de SecureEntry. Esto significa que dicho agente, es decir, el punto de entrada común a la función (API) de administración, encontró un error. Remítase a la tabla de errores de los agentes para obtener más información referente al código xxxx.
xxxx	SEAG	Error del agente de administración de SecureEntry. Esto significa que dicho agente encontró un error. Remítase a la tabla de errores de los agentes para obtener más información referente al código xxxx.
xxxx	SESR	Error del componente Registro de SecureEntry. Los agentes de administración del subsistema SecureEntry/UCM recibieron un error del Registro de SecureEntry. Busque en el mensaje asociado para obtener más información. Remítase a la tabla de errores de los agentes para obtener más información referente al código xxxx.
xxxx	LSAP	Error xxxx del agente de Lan Server. Esto significa que dicho agente encontró un error. Remítase a la tabla de errores de los agentes para obtener más información referente al código xxxx.
xxxx	LSER	Error xxxx de función (API) de Lan Server. Esto significa que el agente de Lan Server recibió un error de la función (API) de Lan Server. Remítase a la documentación de Lan Server para obtener más información del error xxxx. Si se trata de un error común, es posible que mensaje de error asociado contenga información útil. PISTA: la mayoría de errores de Lan Server son también errores de base de OS/2, con lo que HELP SYSxxxx también puede serle de ayuda.
xxxx	REGT	Error xxxx en la función (API) del Registro de SecureEntry. Esto significa que el agente de Lan Server recibió un error del Registro de SecureEntry. Busque en el mensaje asociado mayor información. Remítase a la tabla de Errores y mensajes de control de sesión para obtener más información referente al código xxxx. PISTA: El agente de Lan Server sólo utiliza el Registro de SecureEntry para almacenar información referente a las asignaciones de conexión por grupo, por lo que el error debe estar relacionado con una operación de este tipo.
xxxx	UCAG	Error del agente de administración de UCM. Esto significa que dicho agente encontró un error. Remítase a la tabla de errores de los agentes para obtener más información referente al código xxxx.
xxxx	UCSQ	Un error de función (API) de SQL ha sido devuelto al agente del subsistema de UCM. Remítase a la la de códigos de errores de SQL para obtener más información referente al código xxxx.
xxxx	UCAP	Un error de función (API) de UCM sido devuelto al agente del

		subsistema de UCM. Remítase a la tabla de errores de los agentes para obtener más información referente al código xxxx.
xxxx	UCME	Este es un error de memoria devuelto por la función (API) de UCM al agente de administeación de UCM. Una petición de asignación de memoria falló, ya fuera en el host o en la estación de trabajo.

Tabla de Errores de los Agentes

Número de Error	Nombre del Error	Descripción
001	INFOOK	Mensaje informativo. En realidad no ha habido ningún error, y el mensaje asociado contiene información de un evento que debía ser relatada.
002	INVALID_KEYWORD_SIZE	Una de las palabras claves proporcionadas (atributos del objeto) era, o demasiado corta o demasiado larga.
003	INVALID_OBJTYPE	El agente recibió un tipo de objeto inválido a través de la función (API).
004	INVALID_OPERATION	La operación (alta, baja, modificación) no es válida en este momento.
005	INVALID_PARAMETERS	Error genérico indicativo de que los parámetros enviados al agente a través de una llamada a función (API) eran inválidos.
006	EXISTS_OBJ	El objeto ya existe.
007	NEXISTS_OBJ	El objeto requerido no existe.
008	EXPECTED_KWD	Se esperaba una palabra clave obligatoria para este objeto.
009	NEXPECTED_KWD	Se recibió una palabra clave inesperada para este objeto.
010	NEXIST_KWD	La palabra clave no existe.
011	EXIST_KWD	La palabra clave ya existe.
012	INCORRECT_KWD	Genérico. La palabra clave es incorrecta.
013	NOT_ALL_KWD	No se pudieron devolver todas las palabras clave.
014	MANY_ROWS_FETCHED	Se obtuvieron demasiadas filas. La función (API) de UCM está configurada con un número máximo de tuplas en respuesta a una petición. Utilice la variable de entorno EDY_UCM_MAXROWS para ajustar este número máximo a sus necesidades.
015	NROWS_FETCHED	No se obtuvo ninguna fila. El resultado está vacío puesto que no se encontró ninguna fila que cumpliera con el criterio de búsqueda.
016	DEL_USR_UCM	No se pudo dar de baja al usuario del subsistema de UCM. Sigue estando definido en otros subsistemas.
017	DEL_SUB_UCM	No se pudo dar de baja el subsistema de UCM. Este debe ser el último a dar de baja.
018	NEXIST_DEFKWD	La palabra clave requerida por defecto 'Id PalabraClave' no se encontró en el subsistema UCM.

960	PRVERR	Operación no permitida desde esta máquina por falta de privilegio. Verifique la variable de entorno SGM_ADM_PRIV.
961	LOGERR	Fué imposible abrir el archivo de anotaciones de administración para escritura. Se proporciona el código de error de sistema operativo devuelto.
962	DYNERR	Fué imposible abrir el módulo de librería especificado para su linkedición dinámica. Se proporciona el código de error de sistema operativo devuelto.
963	MAXERR	Ya se han cargado el máximo permitido de librerías de subsistema. Contacte con el soporte SecureEntry si encuentra este error.

Errores y Mensajes del Editor de Procesos Auditables

Los siguientes mensajes pueden aparecer en tiempo de ejecución normal del editor.

Número del Error	Mensaje del Error	Descripción del Error
EDY1000	Error en Inicialización.	Una tarea de inicialización no se pudo llevar a cabo. Esto se puede deber a una carencia de recursos del sistema o a la corrupción de la imagen del editor en disco. Verifique que los otros programas del sistema se ejecutan sin problemas y que la imagen ejecutable del editor en el disco no está corrupta.
EDY1001	Error en creación de ventana principal.	El diálogo principal del editor no pudo ser creado. Esto se puede deber a una carencia de recursos del sistema o a la corrupción de la imagen del editor en disco. Verifique que los otros programas del sistema se ejecutan sin problemas y que la imagen ejecutable del editor en el disco no está corrupta.
EDY1002	No se pudo abrir el archivo de entrada.	El archivo especificado es de sólo lectura, o está bloqueado por otro proceso, o el archivo no existe, o el nombre del camino completo al archivo no existe, o se trata en realidad de un directorio, o el disco duro está lleno, o el sistema se ha quedado sin identificadores internos (handles). En este último caso, espere a que otro programa termine su ejecución y reintente la operación.
EDY1003	No se pudo abrir el archivo de salida.	El archivo especificado es de sólo lectura, o está bloqueado por otro proceso, o el nombre del camino completo al archivo no existe, o se trata en realidad de un directorio, o el disco duro está lleno, o el sistema se ha quedado sin identificadores internos (handles). En este último caso, espere a que otro programa termine su ejecución y reintente la operación.
EDY1004	Error en la carga del gestor de ayuda.	El gestor de ayuda estandar de OS/2 no pudo encontrar el archivo EDYEXECE.HLP. Verique que este archivo reside en la vía de instalación a SecureEntry, subdirectorio HELP.
EDY1005	Error en la carga de una	El editor no pudo encontrar una línea de texto. Verifique

	línea de texto.	que el archivo EDYERROR.MSG reside en la vía de instalación a SecureEntry, subdirectorio EXEC, y que la imagen ejecutable del editor en el disco no está corrupta.
EDY1006	Error en la visualización de un panel de ayuda.	El editor no pudo encontrar un panel de ayuda. Contacte con el equipo de soporte de SecureEntry.
EDY1007	No se pudo cargar el proceso de la Lista de Salida.	La rutina de terminación del editor no pudo ser registrada. Esto se puede deber a una carencia de recursos del sistema. Verifique que los otros programas del sistema se ejecutan sin problemas.
EDY1008	Error obteniendo información del archivo.	Una llamada a la validación del gestor de almacenamiento intermedio de impresión (spooler) o a las rutinas de búsqueda del sistema de archivos terminó produciendo un error. Contacte con el equipo de soporte de SecureEntry.
EDY1009	No hay memoria suficiente.	Carencia de memoria en el sistema. Reduzca el número de programas en ejecución, o los valores de las variables BUFFERS=, TRACEBUF=, DISKCACHE=, THREADS=, RMSIZE=, o DEVICE=VDISK.SYS del archivo CONFIG.SYS y luego rearranque el sistema, o elimine archivos innecesarios del archivo de intercambio y luego rearranque el sistema.
EDY1010	Error leyendo de archivo.	Una llamada a la validación del gestor de almacenamiento intermedio de impresión (spooler) o a las rutinas de lectura del sistema de archivos terminó produciendo un error. Contacte con el equipo de soporte de SecureEntry.
EDY1011	Error escribiendo a archivo.	Una llamada a la validación del gestor de almacenamiento intermedio de impresión (spooler) o a las rutinas de escritura del sistema de archivos terminó produciendo un error. Contacte con el equipo de soporte de SecureEntry. Para una operación de exportación, este error indica que no se ha exportado toda la información correctamente, aunque tal vez sí una parte.
EDY1012	Formato de archivo de entrada inválido.	El archivo de entrada no es un perfil Processes Auditor de SecureEntry. Reintente la operación con un perfil Processes Auditor de SecureEntry real.
EDY1013	No se ha proporcionado el nombre del proceso a auditar.	Usted no proporcionó el nombre del proceso a auditar al intentar añadir un nombre de proceso nuevo a la lista de procesos a auditar. Proporcione un nombre de proceso y reintente la operación.
EDY1014	El nombre del proceso a auditar es inválido.	El nombre de proceso a auditar que intentó añadir contiene uno o más de los siguientes carácteres inválidos: 01-1F hex " + , / ; < = > [ ] | Elimine los carácteres inválidos y reintente la operación.
EDY1015	El nombre del proceso a auditar ya existe.	Usted intentó añadir un nombre de proceso que ya existe. Proporcione un nombre de proceso distinto y reintente la operación.
EDY1016	No se ha proporcionado el número de invocaciones.	Usted especificó que hay que controlar el número de invocaciones del proceso seleccionado, pero no indicó el límite superior. Especifíquelo y reintente la operación.

EDY1017	El número de invocaciones debe ser un número.	Usted especificó que hay que controlar el número de invocaciones del proceso seleccionado, pero el límite superior no es un número. Especifíquelo y reintente la operación.
EDY1018	El número de invocaciones debe estar en el rango 1 a 65535.	Usted especificó que hay que controlar el número de invocaciones del proceso seleccionado, pero el límite superior está fuera de rango. Especifíquelo en un rango de 1 a 65535 y reintente la operación.
EDY1019	No se pudo probar el archivo. Código de error devuelto: %u	La activación o desactivación de un perfil Processes Auditor de SecureEntry no se realizó satisfactoriamente. Anote el código de retorno devuelto y contacte con el equipo de soporte de SecureEntry.

Los mensajes siguientes pueden aparecer durante las operaciones de importación. Note que cualquier error detendrá la operación de importación por completo.

Número del Error	Mensaje del Error	Descripción del Error
EDY1040	Comilla doble no esperada en la línea %u del archivo de entrada. Proceso de importación abortado.	Las comillas dobles deben englobar sólo nombres de procesos que contengan espacios en blanco. Elimine la comilla doble de la línea especificada del archivo de importación y reintente la operación.
EDY1041	Comilla doble no encontrada en la línea %u del archivo de entrada. Proceso de importación abortado.	Las comillas dobles deben englobar sólo nombres de procesos que contengan espacios en blanco. Añada la comilla doble en la línea especificada del archivo de importación y reintente la operación.
EDY1042	Fín de línea no esperado en la línea %u del archivo de entrada. Proceso de importación abortado.	La línea especificada del archivo de importación no está completa. Elimínela o coméntela, o añada la información que falte, y reintente la operación.
EDY1043	El número de invocaciones en la línea %u del archivo de entrada debe ser un número en el rango 1 a 65535 o la palabra 'Todas'. Proceso de importación abortado.	Cambie el número de invocaciones a auditar en la línea especificada del archivo de importación a un número que se encuentre en el rango 1 a 65535 o a la palabra 'Todas' (sin comillas). Luego reintente la operación.
EDY1044	Valor para Invocaciones Son Sesiones de Trabajo no esperado en la línea %u del archivo de entrada. Proceso de importación abortado.	Cambie el valor para Invocaciones Son Sesiones de Trabajo en la línea especificada del archivo de importación a 'Sí' o 'No' (sin comillas). Luego reintente la operación.
EDY1045	Valor para Descartar Usos de CPU con Valor Cero no esperado en la línea %u del archivo de entrada. Proceso de importación abortado.	Cambie el valor para Descartar Usos de CPU con Valor Cero en la línea especificada del archivo de importación a 'Sí' o 'No' (sin comillas). Luego reintente la operación.
EDY1046	La fecha de inicio en la línea %u del archivo de entrada es	Cambie el formato del texto que conforma la fecha de inicio en la línea especificada a una fecha de inicio válida i reintente la operación.

	inválida. Proceso de importación abortado.	
EDY1047	La hora de inicio en la línea %u del archivo de entrada es inválida. Proceso de importación abortado.	Cambie el formato del texto que conforma la hora de inicio en la línea especificada a una hora de inicio válida i reintente la operación.
EDY1048	La fecha de finalización en la línea %u del archivo de entrada es inválida. Proceso de importación abortado.	Cambie el formato del texto que conforma la fecha de finalización en la línea especificada a una fecha de finalización válida i reintente la operación.
EDY1049	La hora de finalización en la línea %u del archivo de entrada es inválida. Proceso de importación abortado.	Cambie el formato del texto que conforma la hora de finalización en la línea especificada a una hora de finalización válida i reintente la operación.
EDY1050	La fecha y hora de finalización en la línea %u del archivo de entrada son o menos recientes o idénticas a su fecha y hora de inicio. Proceso de importación abortado.	Cambie la fecha y hora de finalización a una más reciente, o bien cambie la fecha y hora de inicio a una menos reciente, y reintente la operación.
EDY1051	La fecha y hora de inicio y el ID de proceso de la línea %u del archivo de entrada ya han sido procesados en el archivo. Proceso de importación abortado.	Está usted intentando importar una línea de detalle cuya llave, compuesta por fecha y hora de inicio e ID de proceso, ya existían en el archivo de importación. Modifique ligeramente dicha llave en la línea especificada en el archivo de importación cambiando las centésimas de segundo y reintente la operación, o comente la línea en cuestión y reintente la operación.
EDY1052	El ID de proceso especificado en la línea %u del archivo de entrada es inválido. Proceso de importación abortado.	El ID de proceso no pudo ser entendido como un valor en hexadecimal. Cámbielo en la línea especificada a uno válido y reintente la operación.
EDY1053	No hay memoria suficiente para el proceso de importación a partir de la línea %u del archivo de entrada. Proceso de importación abortado.	Carencia de memoria en el sistema. Reduzca el número de programas en ejecución, o los valores de las variables BUFFERS=, TRACEBUF=, DISKCACHE=, THREADS=, RMSIZE=, o DEVICE=VDISK.SYS del archivo CONFIG.SYS y luego rearranque el sistema, o elimine archivos innecesarios del archivo de intercambio y luego rearranque el sistema.
EDY1054	Demasiados procesos a partir de la línea %u del archivo de entrada. Proceso de importación abortado.	El número máximo de elementos que se pueden almacenar en la lista de procesos a auditar es de 32767. Intente dividir el archivo de entrada en archivos más pequeños, o intente separar el perfil actual en perfiles con menos elementos.
EDY1055	La fecha y hora de inicio y el ID de proceso de la línea %u del archivo de entrada ya	Está usted intentando importar una línea de detalle cuya llave, compuesta por fecha y hora de inicio e ID de proceso, ya existe en el perfil en curso. Modifique

	existen en el perfil actual. Proceso de importación abortado.	ligeramente dicha llave en la línea especificada en el archivo de importación cambiando las centésimas de segundo y reintente la operación, o comente la línea en cuestión y reintente la operación.

Temas específicos de UCM

UCM permite que SecureEntry proporcione una administración centralizada a nivel corporativo. Para crear la estación de administración centralizada lea la sección Configuración de la estación administradora de UCM.

Todo lo que se ha explicado hasta ahora sigue siendo completamente válido en este entorno, salvo algunas pequeñas diferencias:

Deben usarse las herramientas de administración a través del comando UCMADM, para redireccionar todas las operaciones de administración hacia el sistema principal. Así, por ejemplo, para ejecutar la herramienta de administración interactiva deberá invocar el comando:

```
UCMADM EDYSNADM
```

Si usted tiene instalada la funcionalidad de validación de passwords contra RACF, no podrá cambiar las contraseñas desde las herramientas de administración de SecureEntry. Deberá hacerlo a través del RACF.

Si usted tiene instalada la funcionalidad de emulación de RACF, deberá utilizar las herramientas de administración de SecureEntry para cambiar las contraseñas de los usuarios.

Todos los cambios efectuados sobre la base de datos central serán actualizados en la LAN en tiempo de conexión de los usuarios afectados. Los cambios sobre grupos o definiciones de recursos deberán ser procesados por el programa **EDYUCDIS** antes de poder ser efectivos en el entorno LAN.

Puede especificar que todos los cambios realizados sobre la base de datos central que afecten a grupos y definiciones de recursos sean actualizados automáticamente en el entorno LAN a través de un proceso asíncrono (Actualización en línea de oficinas). Este es un método alternativo al programa **EDYUCDIS**. En este caso, desde cualquier estación puede usar la utilidad **EDYBRNVW.EXE** para ver los datos de sincronización de la oficina. Este método se activa desde las herramientas de administración UCM. Con estas herramientas puede especificar la política de refresco para todas las oficinas de la corporación.

Puede permitir la administración paralela (permitir la administración LAN normal), pero en este caso la base de datos central no conocerá los cambios efectuados en el entorno LAN, y por lo tanto no se recomienda.

Actualización en línea de las oficinas

La actualización en línea de las oficinas es un procedimiento que permite actualizar las definiciones de grupos y recursos en cada una de las oficinas de la corporación. Este procedimiento se ha integrado en el programa EDYSRV.EXE que actualiza entornos LAN dinámicamente.

Éste es un método alternativo a los procesos desatendidos del sistema principal, que recogen información sobre los cambios de la base de datos de UCM (tablas de cambios), y a los procesos desatendidos de LAN, que actualizan esa información en la base de datos local del servidor de SecureEntry.

Para poder activar la actualización en línea de una oficina, el programa EDYSRV debe ser cargado con un parámetro específico (policy). Este parámetro se explica en el apartado **EDYSRV y EDYFREE** de la sección Utilidades SecureEntry de Mantenimiento .

El archivo EDYDIS.LOG registra información sobre toda la actividad de actualización de la oficina. Está ubicado donde apunta la variable de entorno SGM_UCM_LOGPATH, como se explica en el apartado dedicado a las variables de entorno **específicas de UCM** dentro de la sección Variables de entorno.

SecureEntry permite actualizar fácilmente las definiciones de grupos y recursos. Este capítulo explica como hacerlo. Las páginas siguientes proporcionan más información sobre este proceso.

Políticas de refresco

Las diferentes estrategias para realizar la actualización en línea de las oficinas se conocen con el nombre de políticas de refresco.

La actualización en línea, al ser activada, establece el nivel de actualización de la oficina contrastando la información contenida en la base de datos local con la contenida en la base de datos central. Una vez hecho esto, si el nivel asignado a la oficina no coincide con el más reciente posible, se inicia una transferencia de datos desde el sistema principal hasta la oficina para que así sea. De esta manera la oficina se inicializa con los datos más recientes.

La política de refresco puede ser modificada según las necesidades que más convengan a la corporación, y guardada en la base de datos UCM. Esto se hace a través de las herramientas de administración de UCM. Nótese que después de la instalación este procedimiento no queda activado, sino que debe ser establecido explícitamente por el administardor.

Cada oficina pregunta una vez por día al sistema principal por la política de refresco que debería aplicar para poder sincronizarla en caso de que haya sido cambiada en la base de datos local.

La política de refresco puede tomar los siguientes valores:

Conexión: los cambios, si existen, se bajan desde el sistema principal en tiempo de CONEXIÓN.

Ipl: los cambios, si existen, se bajan desde el sistema principal en tiempo de IPL.

Nunca: nunca se actualizan los cambios. No se bajan datos desde el sistema principal.

Tiempo: los cambios, si existen, se bajan desde el sistema principal a una hora y minuto concreto del día.

Purga de las tablas de cambios

Desde las herramientas de administración de UCM se puede especificar el número de oficinas de la corporación que serán almacenadas en la base de datos corporativa. La purga de las tablas de cambios se activa si este número no es cero. Esto quiere decir que cuando los cambios se bajan hacia las oficinas de la compañía, también son eliminados de las tablas de cambios pendientes de ser realizados.

Sobreseimiento de la política de refresco

Puede configurar EDYSRV para que ignore la política de refresco almacenada en la base de datos corporativa para la oficina. Para ello, debe cargar EDYSRV con un parámetro específico.

Este parámetro puede tomar los siguientes valores:

Conexión: los cambios, si existen, se bajan desde el sistema principal en tiempo de CONEXIÓN.

IPL: los cambios, si existen, se bajan desde el sistema principal en tiempo de IPL.

Nunca: nunca se actualizan los cambios. No se bajan datos desde el sistema principal.

Tiempo: los cambios, si existen, se bajan desde el sistema principal a la hora y minuto especificados.

Periódicamente: se bajan los datos de forma periódica con el periodo especificado (en minutos) En tiempo de arranque, los cambios de la oficina, si existen, se bajan desde el sistema principal.

Registro de la actividad de UCM

Desde las herramientas de administración puede activar el registro de la actividad de UCM. En este caso, todas las operaciones serán registradas en el sistema principal en la tabla de LOG de UCM y después podrán ser gestionadas a través del programa EDYEXLOG en el entorno del sistema principal. Para más información sobre este programa remítase a la sección de Proceso desasistido EDYEXLOG en la Guía de administración UCM.

Herramienta de recuperación UCM

Si el proceso de Actualización en línea de las oficinas falla debido a una definición incorrecta de datos de oficina (grupos, recursos,...), vd. puede corregir la definición mediante la utilidad de administración SecureEntry para UCM y después ejecutar el proceso EDYRVUCM en la estación administradora de UCM para compactar y corregir las tablas de cambios envueltas en el error.

Esta herramienta chequea las tablas de cambio de la Base de Datos de UCM localizando la información errónea y sobrante que ha de ser eliminada. Si desea obtener más información sobre esta utilidad remítase al capítulo de Herramienta de recuperación UCM en el manual de administración UCM.

Emulación de RACF

El emulador de RACF le permite validar las passwords de los usuarios contra la base de datos de UCM en lugar de utilizar el subsistema de seguridad que usted podría tener instalado en el Host de la corporación.

Puede especificar el conjunto de carácteres válidos y las longitudes máxima y mínima de las passwords a ser usadas por los usuarios de la corporación.

Desinstalación SecureEntry

Si alguna vez quiere desinstalar SecureEntry 3.0 después de haberlo instalado, puede usar el comando 'UNINSTAL.CMD' ubicado en el subdirectorio INSTALL de su directorio SecureEntry. Este comando eliminará por completo SecureEntry 3.0 de su máquina. La sintaxis del comando es como sigue:

```
UNINSTAL [BATCH] [SHUTDOWN]
```

El parámetro *BATCH* sirve para ejecutar el comando desatendidamente, y el de *SHUTDOWN* fuerza que se apague el sistema una vez el comando se haya completado.

Tenga en cuenta que antes de empezar a desinstalar deberá eliminar a mano la protección de arranque de su máquina si es que ésta ha sido instalada.

Observe también que después de haber concluido el proceso de desinstalación, se le invitará a rearrancar la máquina, y que el arranque inmediatamente posterior a la desinstalación puede ser más largo de lo habitual porque es el momento en el que los archivos de SecureEntry son físicamente eliminados del disco.

Diferencias respecto a SecureEntry 2.0

Esta versión de SecureEntry incorpora muchísimas mejoras sobre las versiones anteriores, proporcionando, básicamente, una extensión mejorada de las funcionalidades ya conocidas:

1. Se basa en la arquitectura SES (Security enabling services), lo cual mejora la estabilidad y la seguridad, a parte de adoptar la estrategia escogida por IBM para el OS/2 en cuestiones de seguridad.
2. Integración transparente de nuevos componentes:

   El componente de comportamiento de las ventanas (menús de sistema), permite determinar la posición inicial de cualquier ventana de aplicación, además de desactivar cualquier menú de sistema.

   El componente de la lista de tareas, permite controlar el comportamiento y el aspecto de la lista de tareas.

   El componente de restricciones del disquete, permite restringir el acceso a la unidad de disquete a cualquier grupo/usuario, así como criptografiar los contenidos del disquete.

   El componente de comportamiento del SES, permite escoger entre diversas funciones a nivel de sistema según el grupo/usuario, incluyendo la acción a realizar ante un Ctrl-Alt-Del, qué archivos de imágen usar, y como configurar la función del salvapantallas.

   El componente de acceso a archivos (TreeLock), permite restringir los accesos a los archivos y/o directorios a nivel del sistema de archivos.

   El componente de barra de herramientas personalizada (launchpad) de SecureEntry permite configurar modelos de barras de herramientas personalizadas (launchpad) para diferentes grupos/usuarios.
3. Más entornos soportados. Ahora SecureEntry permite tres tipos básicos de instalación, desde monoestación hasta administración centralizada a nivel corporativo, sin ser imprescindible el servidor de LAN si no se desea. (se incorpora una base de datos propia de grupos y usuarios).
4. Una nueva arquitectura de Procedimientos Modulares de Conexión, que permite al usuario escribir módulos particularizados para unificar el proceso de verificación/autentificación de los usuarios con otros subsistemas de red.
5. Herramientas de administración reescritas (tanto las desatendidas como las interactivas), que permiten configurar fácilmente la base de datos de grupos y usuarios para cualquier estación. (Ahora se puede administrar desde cualquier estación, siempre que el usuario conectado sea administrador las funciones de administración estarán disponibles). Además las herramientas de administración son homogéneas e independientes del entorno de instalación desde el que se ejecutan.
6. Una granularidad más fina. Ahora puede asignar un componente de seguridad a cualquier grupo o usuario, forzándose siempre, en caso de coincidencia, el componente de seguridad del usuario por encima del de grupo.
7. Rutinas de instalación mejoradas, permitiendo tanto instalaciones desatendidas como interactivas.
8. Soporte de UCM reescrito. Para instalaciones administradas de forma centralizada, el UCM ha sido reescrito , así como los componentes que soportan esta solución alternativa, consiguiendo más estabilidad, una mayor flexibilidad y un rendimiento superior. Nótese que UCM no está incluído en este paquete.

Respuestas a preguntas habituales

La siguiente lista es un compendio de consejos y respuestas relacionados con las preguntas más habituales:

Consejos para la Instalación

Esta sección ofrece soluciones a los problemas más habituales relacionados con la instalación de SecureEntry 3.0

¿Cuál es el mejor modo de preparar el sistema para instalar SecureEntry 3.0?

Si usted quiere poder disponer de los servicios de seguridad del OS/2 (Security Enabling Services) debe tener en cuenta que SecureEntry 3.0 necesitará el OS/2 WARP, el SES y un nivel de fixpack 17 o superior, y que los fixpacks de OS/2 son acumulativos y también facilitan código para SES, por lo tanto, para máquinas nuevas, la secuencia más rápida para dejar la estación lista para instalar SecureEntry 3.0 es:

1. Instalar el OS/2 Warp
2. Instalar el SES
3. Instalar el fixpack del OS/2 más reciente

Obsérvese que si la instalación se realizara en el orden inverso se podrían perder los módulos del fixpack del OS/2 relacionados con el SES.

Obtengo el error 'UNPACK32 ERROR' o similar...¿Qué falla?

Si obtiene errores de desempaquetamiento mientras está instalando, ello puede ser debido a una de estas dos causas:

1. Los archivos de empaquetamiento originales de SecureEntry están dañados, o
2. El programa desempaquetador no 'entiende' los archivos de empaquetamiento de SecureEntry

El primer caso es fácil de detectar verificando la corrección de los datos contenidos en los disquetes de instalación de SecureEntry... El segundo caso sólo puede ocurrir si el proceso de instalación está usando una versión antigua de la librería FTCOMP.DLL como ocurriría si en la misma máquina en la que se pretende instalar SecureEntry se hubiese instalado previamente el BranchCare o cualquier otro producto que usara esta

DLL. En cualquier caso, la solución pasa por reemplazar la librería FTCOMP.DLL con la que viene en el primer disquete de instalación de SecureEntry.

¿Después de la instalación qué nombre de usuario y contraseña debo utilizar?

Por favor, lea el capítulo de este manual titulado Qué hacer después de instalar.

¿Cómo puedo saber el nivel de empaquetamiento del producto que he instalado?

Aparte de leerlo en la ventana de instalación/actualización que aparece mientras se instala/actualiza SecureEntry, usted siempre puede editar el archivo 'SENTRY.SIG' ubicado en el subdirectorio INSTALL de su directorio SecureEntry.

¿Cómo puedo integrar mis propios perfiles de usuario o mis funcionalidades añadidas en la instalación de SecureEntry?

Lea el capítulo Personalización de la instalación

¿Puedo actualizar una máquina que tenga instalado un SecureEntry con una versión diferente de NLS?

Sí, pero los títulos de los objetos contenidos en la carpeta 'Herramientas de Trabajo de SecureEntry' no aparecerán en el nuevo lenguaje. Para ello, tendrá que borrar la sombra de la carpeta 'Herramientas de Trabajo de SecureEntry' y los objetos que contiene y crearlos de nuevo usando la utilidad 'EDYCRWRK.CMD' ubicada en el subdirectorio INSTALL de su directorio SecureEntry.

Después de instalar/actualizar faltan objetos en la carpeta 'Herramientas de Trabajo de SecureEntry'

Normalmente esto indica una corrupción menor de los archivos INI del OS/2. Puede usar el programa EDYCLINI para intentar corregir el problema, y después de rearrancar, borre la carpeta 'Herramientas de Trabajo de SecureEntry' y los objetos que contiene para crearlos de nuevo usando el comando 'EDYCRWRK.CMD' ubicado en el subdirectorio INSTALL de su directorio SecureEntry.

El procedimiento de actualización se cuelga. ¿Qué debo verificar?.

Hay un caso en el que el procedimiento de actualización parecerá haberse colgado. Ocurre cuando hay activado un perfil de Treelock que no permite lanzar cmds de pantalla completa. En este caso el subsistema responsabilizado de lanzar la cmd recibe el mensaje 'Acceso Denegado' y su reacción es tratar de lanzar de nuevo la cmd. Para solucionar el problema tendrá que rearrancar la máquina, quitar el perfil de Treelock y volver a lanzar el proceso de actualización.

Durante la instalación tengo problemas con el copiado de los archivos o recibo mensajes del estilo 'demasiados archivos abiertos' o 'número de manejadores (handles) insuficiente'...

Podría ocurrir que la máquina en la que está intentando instalar SecureEntry tuviera instalado un software que estuviera utilizando la mayor parte de los manejadores (handles) de archivo disponibles para el WPS. Para solucionar este problema, edite su config.sys y añada la línea:

```
SET SHELLHANDLESINC=30
```

Estoy instalando sobre Warp 4.0, ¿hay algún problema?

El soporte para Warp 4.0 (Merlin) ha sido completado. SecureEntry funcionará correctamente. Sólo recuerde que si quiere utilizar SES en vez del emulador que SecureEntry proporciona, debe instalarlo antes de empezar a instalar SecureEntry. Esto puede hacerse escogiendo el componente de seguridad desde la lista de instalación seleccionable de componentes del sistema operativo (Instalación selectiva en la carpeta de configuración OS/2).

Es posible que la máquina se cuelgue durante el arranque inmediatamente posterior a la instalación de SecureEntry. Se supone que este problema lo soluciona el FP1 de Merlin, en cualquier caso, el rearrancar de nuevo la máquina será suficiente para eliminar el error y poder continuar trabajando.

Acabo de instalar. Donde esta mi barra de herramientas ?

SecureEntry por defecto no crea launchpad alguno después de instalar, pero copia la barra de herramientas original en la carpeta *SecureEntry : Herramientas de instalación* Vd. puede añadir una sombra del mismo al objeto *EdyStart* (para que la barra de herramientas se abra durante el proceso de arranque), o bien crear un perfil de launchpad personal y asignarlo a usuarios/grupos, o como perfil por defecto en la carpeta *NOUSER*.

Después de desinstalar faltan objetos o bien están escondidos

Versiones anteriores de SecureEntry adolecían de un problema que podía causar que algunos de los estilos originales de los objetos no fueran restaurados correctamente. Para solucionar este problema:

1. Instale SecureEntry en modo monoestación.
2. Cree un perfil binario con el atributo de visibilidad por defecto puesto a visible para todos los objetos.
3. Ejecute EDYCLASS /U nombre_de_perfil para activar el perfil editado en el punto anterior.
4. Desinstale SecureEntry

Como instalar SecureEntry junto con otras aplicaciones que usan SES (p.e, Tivoli)

Tan sólo la coexistencia con dichas aplicaciones está soportada de momento. Se trata básicamente de instalar el emulador de SES de SecureEntry de tal modo que no interfiera con la operativa normal del SES real. Antes de instalar deberá vd. decidir cual de los dos productos será el encargado de controlar el flujo de sesión (conexión, desconexión, bloqueo,...).

Si vd. decide que el flujo de control de sesión debe ser manejado por SecureEntry, entonces deberá encontrar la manera de inhabilitar o automatizar dicho control de flujo en la otra aplicación. Una vez solucionado este

punto, podrá vd. instalar SecureEntry en modo coexistencia usando la opción 1, tal como se indica más abajo.

Si por el contrario, el flujo de control de la sesión será gestionado por la otra aplicación, entonces y además de instalar SecureEntry en modo de coexistencia, deberá definir una serie de variables de entorno que eviten los diálogos y paneles que SecureEntry presenta normalmente. utilice entonces la opción 2 de instalación en modo coexistencia.

Instalando en modo de coexistencia con otras aplicaciones SES

Use siempre las siguientes opciones :

1. **NO** instale el soporte de treelock
2. Use el emulador de SES

Defina la variable de entorno *SET SGM_STEALSES=x* , donde x is la opción que escogió antes de instalar (1 para control de sesión SecureEntry , 2 para control de sesión externo), y proceda con la instalación.

Note que la opción 2 se activará también automáticamente en tiempo de instalación, independiéntemente de la variable *SGM_STEALSES* si se detecta al SES instalado y en ejecución durante el proceso de instalación SecureEntry, siempre que su instalación use el emulador de SES. Clarificando, si la otra aplicación ya está instalada y funcionando, es probable que vd. no necesite definir la variable de entorno antes de instalar SecureEntry.

La única diferencia entre ambos tipos de instalación (opciones 1 y 2), es que la segunda definirá en su archivo *config.sys* las siguientes variables de entorno :

```
set sgm_edylk_show=no
set sgm_back_bitmap=no
set sgm_ses_cad=yes
set sgm_ses_inactivity=no
set sgm_hide_wait_dlgs=yes
```

Una vez instalado, y en caso de usar la opción 2, vd. probablemente querrá definir un archivo de exits de usuario *edycust.cmd* que realice la conexión automática del usuario deseado sin presentar ningún diálogo de interrogación (lea como hacerlo en Programando exits de usuario). En caso de que decida vd. utilizar el usuario por defecto de la instalación desatendida, observe que este está dado de alta con la contraseña expirada, y por lo tanto deberá cambiarse en la primera conexión (utilizando el parámetro /N en la llamada a EDYUTIL desde dicha exit de usuario). Por último, es probable que desee vd. también definir un perfil de control de sesión (EDYSES.INI) en la carpeta de restricciones por defecto *NOUSER* que inhiba el bloqueo automático SecureEntry en la máquina, así como un perfil de restricciones de escritorio (EDYDESK.INI) que suprima la entrada SecureEntry de desconexión del menú emergente del escritorio.

Recuerde que puede vd. automatizar este proceso para instalaciones desatendidas tal y como se detalla en Instalaciones personalizadas.

Como utilizar el soporte de NSC/2 para sincronizar contraseñas

SecureEntry provee un procedimiento de conexión para que las contraseñas de sus usuarios sean validadas, en primera instancia, por NSC/2. En esta sección se describe como instalarlo y utilizarlo:

INTRODUCCIÓN

Este procedimiento de conexión le permite integrar la herramienta de productividad **NSC/2** (Network SignOn Coordinator/2) con la conexión de SecureEntry para que actúe como sincronizador de contraseñas. Usted debe utilizar siempre este subsistema como principal, es decir actuando como sincronizador de

contraseñas, ya que el **NSC/2** no dispone de las APIs adecuadas para conseguir que se fuerce la password, con lo que resultaría imposible utilizarlo como subsistema SecureEntry supeditado a otro.

Cuando se realice una conexión, un cambio de contraseña o una desconexión de SecureEntry, estaremos realizando, respectivamente, una conexión, un cambio de contraseña o una desconexión a los sistemas definidos a tal efecto en el archivo de configuración del **NSC**.

Mediante la variable de entorno SGM_NC puede decidir qué sistemas de los definidos en el **NSC** actuarán como sincronizador de contraseñas para el resto de LMPs. Si se define más de un subsistema de los configurados en el **NSC** como sincronizador, solo se forzarán las contraseñas si todos ellos finalizan correctamente.

INSTALACIÓN

Para instalar el LMP correspondiente al **NSC/2** siga las siguientes instrucciones:

1. Defina este LMP en el archivo **EDYSSLMP.DAT** ocupando la segunda posición tras la definición del LMP de **SS**. Para definir este LMP utilice el identificador **NC** y como parámetro **0**. Una vez incluido este subsistema el fichero **EDYSSLMP.DAT** debe presentar el siguiente aspecto:
2. *SS 1 EDYDOM*
3. *NC 0*
4. *...*
5. *Resto de subsistemas*
6. Especifique en su archivo **CONFIG.SYS** la variable de entorno SGM_NC con el valor apropiado.
7. Especifique en su fichero **CONFIG.SYS** la variable de entorno SGM_LS_IFLOGGED con el valor **FORCEUSE**.
8. Reinicialice la máquina.

ALGUNAS CONSIDERACIONES IMPORTANTES

Si usted decide utilizar este procedimiento de conexión deberá de tener en cuenta los siguientes aspectos:

Proteja los ficheros de configuración del **NSC** contra escritura para que únicamente puedan ser modificados por el administrador y evitar que su manipulación cree fisuras en la seguridad durante el proceso de conexión. Puede utilizar, por ejemplo, el componente de **Treelock** para restringir el acceso a estos archivos.

La conexión a dominio de *LAN SERVER* siempre se realizará contra el dominio especificado en el diálogo de conexión de SecureEntry y no contra el dominio especificado en el archivo de configuración del **NSC**.

En algunos casos puede encontrarse con que las contraseñas de los sistemas sincronizadores del **NSC** no estén sincronizadas. Esta situación puede ser consecuencia, por ejemplo, de solicitar un cambio de contraseña y que alguno de estos sistema no estuviera disponible. Con las contraseñas de los sistemas sincronizadores del **NSC** desincronizadas, evidentemente, no podremos realizar una conexión de SecureEntry, por tanto necesitamos volver a sincronizarlas. Para volver a disponer de las contraseñas de los sistemas sincronizadores sincronizadas puede seguir el siguiente procedimiento:

1. Asegurese de que todos los sistemas sincronizadores NSC están disponibles.
2. Intente una conexión de SecureEntry pidiendo un cambio de contraseña. Como contraseña proporcione la del subsistema que esta desincronizado y como nueva contraseña la correspondiente a los subsistemas ya sincronizados. Observará que se le devuelve el mensaje se *contraseña incorrecta*, sin embargo el cambio de contraseña se habrá realizado con éxito en el

sistema desincronizado. Ahora las contraseñas están sincronizadas. Repita el proceso para todos los sistemas NSC desincronizados.

3. Intente la conexión nuevamente, esta deberia realizarse sin problemas.

Relacionados con el arranque, conexión y desconexión de usuarios

Esta sección ofrece soluciones a los problemas más habituales relacionados con el manejo de los eventos de sesión con SecureEntry.

Durante la inicialización de sesión obtengo un error indicando que no se puede abrir el archivo 'EDYREGDB.VLB'. ¿Qué falla?

Este archivo tiene que estar físicamente accesible justo después de la validación del usuario para poder extraer de él los perfiles de seguridad. Verifique los siguientes puntos :

Que vd. ha instalado ya SecureEntry en el servidor de perfiles de su dominio (controlador de dominio), especificándolo en dicha instalación, bien respondiendo afirmativamente al diálogo interactivo, o si utilizó el comando de instalación desatendida, por medio del parámetro *SERVER*. Si vd. no está seguro, por favor compruebe que exista el archivo *EDYREGDB.VLB* en su servidor de perfiles, en la vía de acceso SecureEntry, directorio *NOUSER*. Este archivo solamente es creado por la instalación en los servidores de perfiles SecureEntry.

Que el usuario con el que intenta conectarse esté definido como administrador, o

Que el usuario pertenezca a un grupo SecureEntry (el nombre de grupo debe empezar por las letras 'SG').

En caso de que el usuario pertenezca a un grupo SecureEntry, y el error persista, entonces deberá vd. verificar que dicho grupo tenga un acceso definido al recurso 'SGMSHELL' del controlador de dominio, con derechos de acceso 'RWA' (lectura, escritura y cambio de atributos). Este acceso se genera automáticamente al crear un grupo SecureEntry vía las herramientas de administración del mismo, pero podría no estar definido si vd. ha desinstalado y reinstalado el producto en el servidor después de definir el grupo, o utilizó las herramientas Lan Server de administración para definir dicho grupo.

Asegúrese así mismo de que el recurso 'SGMSHELL' del controlador de dominio esté siendo compartido en el momento de la conexión.

Finalmente, este error puede producirse también por un antiguo problema existente en el código de soporte de los protocolos de transporte de red (MPTS). Asegúrese en este caso de que vd. tiene instalado el nivel de actualización WR08610 o superior.

Durante la inicialización de sesión obtengo un error indicando que el servidor de LAN ha fallado. ¿Qué ocurre?

La causa más probable de este error es que el programa edysrv.exe no se esté ejecutando en el servidor de dominio. Este programa debe ser lanzado con una sentencia de 'detach' desde el archivo 'EDYSTART.CMD' del servidor de dominio. La instalación de SecureEntry añade automáticamente esta línea. Sin embargo, recuerde que la sentencia correcta para lanzar edysrv.exe en un entorno IBM servidor de LAN es:

```
DETACH EDYSRV.EXE /N:EDYnombre_de_dominio

donde nombre_de_dominio es el nombre se su dominio.
```

Otra posible causa es que el programa peticionario de LAN no se esté ejecutando en la máquina cliente, o que el servidor no pueda ser localizado como consecuencia de una rotura física o lógica de la LAN.

Y aún otra causa para este tipo de problema podría surgir de un conflicto entre las reglas de manejo de contraseñas del IBM LAN server y el RACF en el caso de que se utilice éste último. Por ejemplo, el RACF permite reutilizar una contraseña que se haya usado dos semanas atrás, mientras que el IBM LAN server no lo permite porque la contraseña coincide con una de las contraseñas memorizadas para el usuario. Por este motivo, cuando se usa RACF, se recomienda reconfigurar el IBM LAN server para que implemente una gestión de contraseñas menos restrictiva de la que implementa el RACF, especificando, por ejemplo, la longitud de contraseña mínima y máxima, el factor de unicidad (memoria histórica para contraseñas ya utilizadas), etc.. Puede modificar estos parámetros a través del comando NET ACCOUNTS después de conectarse como administrator. Observe que si se da esta situación de conflicto, el único modo de poder conectarse con el usuario 'problemático' es borrar su definición de LAN usando EDYERASE y cambiar su contraseña de RACF.

Si ninguna de las explicaciones anteriores soluciona el problema, por favor verifique las definiciones de usuario en la base de datos de UCM porque probablemente el problema sea causado por alguna de ellas que no siga las reglas requeridas por el IBM LAN server.

¿Cómo puedo depurar el procesamiento de EDYSTART.CMD ?

Puede depurarlo normalmente desde una sesión de usuario usando la utilidad EDYLKINI.EXE. Pero para aquellos casos en los que los errores sólo suceden durante el arranque, puede hacer lo siguiente:

1. Renombre el archivo 'EDYLKSTR.DLL' ubicado en el subdirectorio DLL del directorio SecureEntry
2. Desde ahora la máquina arrancará ejecutando STARTUP.CMD
3. Cree un STARTUP.CMD que contenga :

   ```
   EDYLKINI /NOMODAL
   ```

4. Ahora puede arrancar y depurar el procesamiento de EDYSTART.CMD

   No olvide dejar las cosas tal y como estaban una vez esté seguro de que el procesamiento de EDYSTART es el correcto.

No puedo iniciar una sesión de usuario, o la máquina no arranca. ¿Qué puedo hacer?

Siendo como es SecureEntry un producto de seguridad, puede resultar especialmente difícil resolver este tipo de problemas, ya que los mecanismos que protegen la máquina durante la operativa normal interferirán ahora también en el diagnóstico y la corrección del error.

Para empezar, tendrá que eliminar la protección de arranque de la máquina en el caso de que ésta hubiera sido instalada. Remítase al capítulo apropiado para obtener más información al respecto.

Una vez hecho esto, podrá, como mínimo, iniciar el proceso de arranque de la máquina desde un disquete de arranque DOS o OS/2 (disquetes de instalación 1 y 2), hasta el punto en que se le permita editar su archivo config.sys, para añadir la siguiente línea:

```
Call=c:\os2\cmd.exe
```

Entonces, y después de rearrancar, podrá investigar un poquito más. Primero de todo, verifique lo siguiente :

Que la sentencia LIBPATH en su archivo *CONFIG.SYS* contenga las entradas correspondientes a la vía de acceso SecureEntry y al SES (siempre que lo esté usando) en la primera posición.

Que la imágen definida como fondo del escritorio vía perfil de personalización SecureEntry **no** sea un bitmap (mapa de bits) de 4 bits por pixel. Estos archivos no los trata correctamente el OS/2 y pueden bloquear la máquina.

Que no tenga vd. instalada una versión muy antigua de SecureEntry de evaluación ya expirada.

Que no se hayan modificado los archivos de configuración base SecureEntry, que son : SENTRY.CNF, SENTRY.SIG, EDYSSLMP.DAT y EDYSLA.INI. Observe que algunos de estos residen en el directorio NOUSER.

Que las DLLs de sistema requeridas por SecureEntry para un arranque correcto estén registradas en su archivo *OS2.INI* actual, tal y como se detalla en EDYWINI. (Estas DLLs podrían quedar desinstaladas después de recrear dichos archivos vía MAKEINI, por ejemplo).

Que no tenga vd. puesto código en las exits de usuario o el proceso de arranque que entre en ciclos de ejecución sin fin.

Que no haya actualizado o instalado SecureEntry sobre el OS/2 Warp 4.0 (Merlin). Si éste es el caso, y usted no ha aplicado el FixPack 1 de Merlin, entonces bastará con rearrancar la máquina y el error no reaparecerá.

Borre todas las ocurrencias de los archivos 'EDYTRDSP.INI' y 'EDYTRC.DAT' que puedan haber en la máquina, y reintente arrancar. Si ha estado jugando con las utilidades de rastreo y sus perfiles han quedado en un estado inconsistente debido a un IPL fallido, es posible que la máquina esté cíclicamente tratando de abrirlos.

Si el error persiste, entonces continúe investigando asegurándose de que :

1. se haya procesado por completo el archivo EDYSTART.CMD. Mire el archivo 'EDYLKINI.LOG' que el proceso de arranque utiliza para este propósito. Recuerde que en este archivo verá también los mensajes que su propio edystart lanza a través del comando edylkmsg.

   Una vez haya solucionado el problema con el proceso de arranque, tendría que poder ver el diálogo de inicio de sesión, y poder inicializar una sesión. Si este no es el caso, verifique los puntos de la siguiente lista :

2. que el nombre de usuario y la contraseña con los que trata de iniciar la sesión sean válidos, estén correctamente configurados y activos. Quizá tenga que acudir a las definiciones de RACF y UCM, o a la administración de IBM LAN server para ello. Si no está seguro, trate de iniciar una sesión con un usuario del que sepa que tiene acceso.
3. En entorno IBM LAN server y/o UCM, verifique que el módulo EDYSRV se esté ejecutando en la máquina servidora. Éste es el módulo que se comunica con el sistema principal antes de la verdadera validación del usuario al iniciar la sesión.

4. También, en entorno IBM LAN server, verifique que el usuario con el que se está conectando, tenga acceso al alias 'SGMSHELL'. Este alias es el que define el encaminamiento a la base de datos que contiene los perfiles de seguridad.
5. Asegúrese de que las exits de usuario se comporten correctamente. Puede añadir 'beeps' o puntos de rastreo en el archivo EDYCUST.CMD para saber si se han alcanzado los puntos relacionados con el inicio de sesión.
6. En entornos UCM, edite el archivo EDYADMIN.LOG para conocer las operaciones realizadas durante el inicio de sesión de usuario. Es una buena idea editar su config.sys para asignar el valor 'TEST' a la variable de entorno SGM_SL_LOGMODE y obtener así la máxima información disponible a este respecto.
7. Si todo lo anterior ha fallado, puede lanzar las funciones de rastreo (traces) de SecureEntry desde su archivo EDYSTART.CMD, y analizar el archivo de rastreo resultante o enviarlo al laboratorio.

Lanzo el IBM LAN requester y los IBM Peer Services desde sesión de usuario y no puedo reinicializar después de finalizar la sesión.

Cuando finaliza la sesión, SecureEntry hace lo que buenamente puede para matar las tareas inicializadas desde la sesión de usuario que finaliza. Desgraciadamente, si se carga software base o de sistema durante la sesión de trabajo (i.e, no durante el proceso de arranque, sino después de validado el usuario), es posible que este software no pueda ser matado de una manera ordenada, o incluso, que no se deje matar, como podría ocurrir si uno de estos programas fuera un proceso que corre en el fondo ejecutándose en nivel de privilegio 0 (ring 0). Este es el caso del proceso WKSTAHLP de los IBM Peer Services. La única manera de matarlo con garantías es a través de un comando de IBM LAN requester. Por lo tanto, si desea que los usuarios puedan arrancar los IBM Peer Services, debe añadir la siguiente línea en la exit de usuario 'antes de desconexión inminente' ('before imminent logoff'):

```
NET STOP REQ /Y
```

Remítase al manual de referencia de los comandos del IBM LAN requester para obtener más información sobre este comando.

Rendimiento en la Inicialización/Finalización de sesión de usuario. Cómo ajustarlo.

Antes que nada lea Afinando SecureEntry, para saber qué se puede hacer para mejorar el rendimiento.

Entonces, si quiere contrastar su rendimiento, y teniendo en cuenta que los números pueden variar mucho dependiendo del hardware y software disponible, hemos obtenido las siguientes estadísticas:

Entorno	MonoEstación	IBM LAN server	IBM LAN server+UCM
Tiempo arranque de sesión	10 segundos	20 segundos	30 segundos

Nótese que estos números han sido obtenidos sobre máquinas con procesador 486 DX2 y sin restricciones de memoria.

En la máquina servidora o en sistemas sobrecargados la desconexión de sesión se cuelga, u otros errores durante la inicialización de sesión.

Si está usando IBM LAN server 4.0, asegúrese de que ha instalado el nivel de PTF IP08227 para este producto. De igual modo, para IBM LAN server 5.0, el nivel IP08260 es imprescindible.

Obtengo 'Hay otro usuario ya conectado en esta máquina'

En entornos IBM LAN server sólo se permite una conexión simultánea por dominio en cada máquina. Si se ha conectado al dominio desde el archivo edystart.cmd o desde una exit de usuario, SecureEntry notificará este error cuando trate de conectarse de nuevo. También puede ocurrir que la máquina fuerce una conexión a dominio al lanzar un determinado comando NET (i.e NET SHARE IPC$) si ya existe una conexión local. Para evitarlo, puede forzar una desconexión de dominio (LOGOFF /D) justo antes de que SecureEntry intente la conexión, o bien cambiar el valor de la variable de entorno SGM_LS_IFLOGGED para dejar que SecureEntry se encargue de esta tarea.

Consejos para la Administración y Configuración

Esta sección ofrece soluciones a los problemas más habituales que puedan surgir durante la administración de SecureEntry.

¿Cómo puedo acceder desde un único cliente a diferentes LANs de SecureEntry?

En entorno IBM LAN server, si se quiere poder conectar a diferentes LANs de SecureEntry desde una misma estación, debe seleccionarse durante la instalación la opción de 'Permitir cambio de dominio al iniciar la sesión'. Obsérvese que esta opción sólo permite conectarse a otros dominios de SecureEntry 3.0 que tengan una configuración similar al dominio especificado durante la instalación de SecureEntry en la máquina cliente desde la que se accede a otros dominios de SecureEntry (mismo nombre de institución y mismas características de administración).

¿Cómo puedo añadir mis propios componentes?

Puede editar, antes de la instalación, el archivo 'SENTRY.DSC' ubicado en el primer disquete de instalación para añadir los componentes apropiados, o , si quiere actualizar una estación que ya tenga SecureEntry instalado, usar el comando UPDATEDB ubicado en el subdirectorio INSTALL de su directorio de SecureEntry. La sintaxis de este comando es:

```
UPDATEDB nombre_archivo

Donde nombre_archivo es su archivo SENTRY.DSC modificado.
```

Tenga en cuenta que :

Tiene que estar conectado como administrador.

La modificación de la base de datos de componentes de SecureEntry puede provocar que no se reconozcan componentes que ya han sido asignados a grupos o usuarios.

¿Puedo cambiar la fecha de expiración de la contraseña, el número máximo de intentos de conexión, o la longitud mínima de las contraseñas?

Sí. Para ello,

> Si su instalación es en entorno monoestación (sin IBM LAN server), edite el archivo 'SENTRY.DSC' ubicado en el primer disquete de instalación de SecureEntry 3.0, asigne los valores apropiados e instale SecureEntry. Si quiere modificar una estación que ya tenga SecureEntry instalado, haga lo mismo y utilice la utilidad UPDATEDB para actualizar los cambios.
>
> Remítase al punto anterior para la sintaxis de invocación y advertencias.
>
> Si su instalación es en entorno IBM LAN server, remítase a la documentación apropiada de este producto (Manual : *Tareas del administrador*, Capítulo : *Administración de usuarios y grupos*).

¿Cómo puedo escribir mis propias exits de usuario?

Puede programarlas en C (en el subdirectorio API\SOURCES\EDYCUST de su directorio de SecureEntry puede hallar los archivos necesarios y un esqueleto de archivo fuente), o en REXX (el esqueleto está ubicado también en el subdirectorio API\SOURCES\EDYCUST). Si escribe una EDYCUST.DLL, ésta debe ser ubicada en el subdirectorio DLL de su directorio de SecureEntry. Si escribe las exits de usuario en REXX, entonces debe ubicar el archivo 'EDYCUST.CMD' resultante en el subdirectorio EXEC de su directorio de SecureEntry.

Todo esto está plenamente detallado en *Programando exits de usuario*.

¿Cómo puedo cambiar los archivos de imágen de arranque?

Edite un perfil de comportamiento de SES, especifique los archivos de imágen de fondo, de bloqueo de sesión y de arranque que desee, y cópielo con el nombre 'EDYSES.INI' (el nombre por defecto del perfil de comportamiento de SES) al subdirectorio NOUSER de su directorio de SecureEntry. Serán usados en el próximo arranque.

Obtengo el error 'LS API Error 53' al acceder a definiciones de grupo. ¿Qué está pasando?

El error 53 significa nombre de recurso de red no encontrado. Probablemente tenga un alias apuntando a un nombre que no exista.

No puedo ver el contenido de los objetos de la clase WPDisk al abrirlos con la vista en árbol.

El problema se deriva del hecho de que los objetos de la clase WPDisk son objetos del desktop mientras que los objetos que conforman su contenido no lo son. Así pues, si el estilo de visibilidad del objeto por defecto es no visible, cuando el WPS abre una vista en árbol no ve ningún objeto a partir del cual poder expandir el árbol, y por lo tanto no lo expande. Si no quiere este tipo de comportamiento, la solución es añadir a su perfil de restricciones del escritorio una entrada para cada objeto WPDisk que quiera hacer visible (con el estilo de visibilidad puesto a visible) y cambiar el estilo de visibilidad por defecto de los objetos del escritorio a visible.

Observe que modificar el perfil para que no aplique restricciones a objetos que no son del escritorio no solucionaría el problema, puesto que, como ya se ha dicho, los objetos WPDisk son objetos que pertenecen al escritorio.

Los objetos de una carpeta personalizada con abertura automática no se abren

Probablemente los objetos sean no visibles, y por lo tanto, el paso de ejecución (thread) de autoarranque encargado de abrirlos no puede verlos dentro de la carpeta. Si quiere que los objetos sean invisibles y a la vez puedan ser abiertos, debería hacerlos visibles e incluirlos en una carpeta invisible. De esta manera el usuario no podría encontrarlos a pesar de ser visibles, y el paso de ejecución de autoarranque podría abrirlos.

¿Cómo se manejan las posiciones de los objetos del escritorio?

Lea la sección Controlando las posiciones de los objetos.

¿Cómo puedo cambiar los paneles por defecto de conexión y desbloqueo de sesión?

Debe programar las exits de usuario de 'conexión de sesión' y de 'bloqueo de sesión' para que muestren su propio panel, y utilizar el comando 'EDYUTIL' para rellenar los campos de entrada de su panel y lanzar los eventos de sesión apropiados. Tenga en cuenta que sus paneles (conexión, desbloqueo de sesión) deben ser modales de sistema (system modal), y que la función de salvapantallas estará activa durante el proceso. Una vez finalice el proceso de sus paneles, no olvide devolver la modalidad a la ventana que la tuviese anteriormente.

Las exits de usuario en las que vd. puede presentar un diálogo e interactuar con el usuario son :

```
EDY_USER_EXIT_AFTER_STARTUP
EDY_USER_EXIT_BEFORE_LOGON_DIALOG
EDY_USER_EXIT_BEFORE_LOGON
EDY_USER_EXIT_BEFORE_LOGON_CHANGING_PASSWORD
EDY_USER_EXIT_BEFORE_UNLOCK_DIALOG
EDY_USER_EXIT_BEFORE_UNLOCK
EDY_USER_EXIT_AFTER_UNSUCCESSFUL_UNLOCK
EDY_USER_EXIT_AFTER_UNLOCK
EDY_USER_EXIT_BEFORE_LOGOFF_FROM_UNLOCK
EDY_USER_EXIT_BEFORE_SHUTDOWN_FROM_UNLOCK
```

Para finalizar, puede vd. además especificar el nombre los procesos que reemplazan los diálogos por defecto con ayuda de la variable de entorno **SGM_USER_DLGS**, para así conseguir mayor robustez en el mecanismo de sobreseimiento de los diálogos por defecto.

¿Cómo puedo controlar los menús emergentes de los objetos que no son del escritorio?

Lea el capítulo que describe las variables de entorno de SecureEntry, con especial atención a la variable de entorno SGM_WPS_NONDESKTOP.

¿Cómo puedo controlar las restricciones sobre objetos de cola de 'spool'?

Lea el capítulo que describe las variables de entorno de SecureEntry, con especial atención a la variable de entorno SGM_WPS_PRINTJOBS.

Estoy intentando hacer distribución o administración remota. ¿Qué problemas encontraré?

Los programas de administración o distribución remota suelen cargar un proceso que corre en el fondo que es quien realmente hace el trabajo. Si está usando un perfil de Treelock cerrado y no está arrancando este proceso como un proceso de superusuario, lo primero que debe hacer es descubrir el nombre de este proceso y darle acceso a todos los recursos de su sistema a través del perfil de Treelock. Esto permitirá que el proceso que corre en el fondo pueda tocar archivos como el config.sys, etc, puesto que las restricciones implícitas y de usuario de SecureEntry no se le aplicarán.

Para el NDM/2, lea la sección NDM ACTIVATE que describe cómo evitar que el comando activar falle si se está usando un perfil de restricciones de disquete.

¿Cómo puedo abrir objetos del WPS desde una exit de usuario?

Remítase a Ejemplo de implementación de exits de usuario para ver un ejemplo de como utilizar la función de REXX SysOpenObject.

Obsérvese que si lo que se quiere es abrir un objeto al arrancar o al iniciar la sesión, puede resultar mucho más sencillo editar el objeto *EDYSTART* ubicado en el subdirectorio NOUSER con el editor de listas de sombras y soltar sobre él una sombra del objeto; o bien, si quiere personalizarlo para el usuario, hacer lo mismo con una carpeta personal dinámica y después asignarla al usuario.

¿Cómo puedo eliminar la opción de menú 'Original' de los menús de los objetos sombra?

Puede hacerlo desde la exit de usuario 'después de la conexión' lanzando la cadena de inicialización (setup string) apropiada al objeto a restringir. Así pues, por ejemplo:

```
/* */
If RxFuncQuery('SysLoadFuncs')  Then Do
  Call RxFuncAdd 'SysLoadFuncs',  'REXXUTIL',  'SysLoadFuncs'
  Call SysLoadFuncs
End


call SysSetObjectData  '<SGM_MAIN_WB_SHADOW>','EDYMENUITEM=REMOVE,ORIGINAL;'
```

Eliminaría la opción de menú 'Original' del menú de la carpeta 'Herramientas de Trabajo de SecureEntry'.

Obsérvese que éste es un método alternativo a usar el editor de restricciones de ventanas para la misma tarea.

Parece que el archivo de imágen de fondo o el del salvapantallas no funciona

Esto puede ser causado por uno de estos dos motivos:

- El perfil de comportamiento del SES no está activo (o bien no ha sido asignado al usuario o grupo, o bien no está ubicado en el subdirectorio NOUSER, o bien no está en modo 'test'),
- O el archivo de imágen referenciado no existe o el nombre especificado es incorrecto.

Vea también el siguiente apartado,

He configurado un perfil de NOUSER, pero no se activa

SecureEntry no garantiza que todos los perfiles de máquina ubicados en el subdirectorio NOUSER sean activados al desconectar una sesión, tan sólo se activan aquellos perfiles que son del mismo tipo que alguno de los perfiles que el usuario o grupo del usuario que se desconecta tiene asignados. Ahora bien, después de la siguiente reinicialización del sistema los perfiles del NOUSER serán los perfiles por defecto. Se ha escogido está política para obtener un mejor rendimiento en las máquinas de producción.

Otros puntos que vale la pena verificar, son:

Que el perfil tenga el nombre del perfil por defecto. (el mismo que el modelo asociado en la carpeta de modelos)

Que el perfil sea del tipo correcto.

¿Cómo puedo desactivar las nuevas opciones de menú que puedan aparecer para los objetos del escritorio o para éste mismo?

SecureEntry, como cualquier otro producto, siempre está pendiente de los nuevos desarrollos en software intentando 'cazar' las últimas funcionalidades incorporadas al sistema operativo. Por otro lado, la arquitectura SOM permite que terceros añadan fácilmente nuevas funcionalidades sobre las funcionalidades estándar del WPS, por ejemplo, incorporando nuevas opciones de menú para los objetos. Este hecho no siempre es deseable en un entorno protegido como el que proporciona SecureEntry. Sin embargo, siempre puede usar el componente Restricciones de las ventanas para desactivar las entradas deseadas por nombre.

¿Qué tipo de archivos imágen puedo usar?

Exceptuando el archivo imágen de fondo del escritorio utilizado por el componente de SES, que sólo acepta archivos de imágen estándares de OS/2, en general, los siguientes formatos son aceptados:

archivos de imágen de OS/2 y de Windows

Los archivos con extensiones .BMP, .VGA, .BGA, .RLE, .DIB, .RL4, and .RL8 son reconocidos como archivos de imágen de OS/2 1.1, 1.2, 2.0 y Windows 3.0. El nuevo formato multimedia de Windows que permite 16 y 32 bits por plano no está soportado. Los archivos se guardan en formato de archivo imágen de OS/2 2.0/Windows 3.0.

El formato CompuServe Graphics Interchange

Un archivo con extensión .GIF es reconocido como un archivo GIF.

El formato ZSoft PC Paintbrush Image File

Un archivo con extensión .PCX es reconocido como un archivo de Paintbrush.

El formato Microsoft/Aldus Tagged Image File

Un archivo con extensión .TIF o .TIFF es reconocido como un archivo TIFF.

El formato Truevision Targa/Vista

Un archivo con extensión .TGA, .VST, o .AFI es reconocido como un archivo Targa/Vista. Esta clase de archivos de imágen solo soportan imágenes de 8 bits por plano y de 24 bits por plano.

El formato Amiga IFF/ILBM Interleaved

Un archivo con extensión .IFF o .LBM es reconocido como un archivo de imágen Amiga IFF/ILBM Interleaved.

El formato de archivo imágen de X Windows

Un archivo con extensión .XBM es reconocido como un archivo de imágen de X windows. Esta clase de archivos de imágen soporta archivos de imágen de 1 bpp X10 y X11. Algunos de los archivos .XBM que contienen texto aparecen como iconos o motivos móviles y por lo tanto no están soportados.

El formato IBM Printer Page Segment

Un archivo con extensión .PSE, .PSEG, .PSEG38PP o .PSEG3820 es reconocido como un archivo PSEG. Esta clase de archivos se usan para incluir datos visuales en documentos BookMaster y sólo contienen 1 bit-por-plano, y por lo tanto son siempre en blanco y negro.

No puedo ejecutar EDYSWLV. cuelga la sesión

Verifique que EDYSWL2.EXE esté ubicado en un directorio que sea accesible desde la variable de entorno del OS/2 PATH.

No puedo configurar un objeto porque no tiene ID de objeto

Lea la sección Acerca de los IDs de los Objetos.

Como suprimir la función WarpCenter

Si vd. no desea utilizar nunca el WarpCenter, haga los siguientes cambios a su archivo *CONFIG.SYS*.

Quite la palabra *WARPCENTER* de la línea *SET AUTOSTART*

Añada la línea *SET SGM_EDYSC_DISABLE=YES*.

Con esto conseguirá vd. que en su máquina no haya nunca un WarpCenter abierto en arranque o conexión.

Sin embargo, si algunos de sus usuarios sí desean esta función, y otros no, entonces la única opción será la de borrar el perfil *EDYSC.INI* de la carpeta *NOUSER* y asociar el perfil de warpcenter deseado a los usuarios/grupos para los cuales esta función sea requerida.

Otros consejos

Esta sección proporciona consejos de carácter general para trabajar con SecureEntry.

¿En qué orden se activan/acceden los componentes de seguridad?

Cada componente tiene su perfil por defecto. Este perfil por defecto es sustituido por cualquier perfil del componente que se ubique en el subdirectorio NOUSER, que a su vez es sustituido por el perfil del componente que tenga asignado el usuario o grupo del usuario actualmente conectado, que a su vez es sustituido por cualquier perfil del componente que se asigne directamente al usuario.

¿Cómo puedo implementar una política de administración centralizada o desatendida?

Pregunte por UCM. UCM es un añadido de SecureEntry para la administración corporativa que le permite, entre otras funcionalidades, administrar sus LANs desde un sistema principal.

¿Cómo puedo integrar mi propia red de la forma más transparente posible?

Si no dispone de IBM LAN server, puede seleccionar la opción 'otras redes' que SecureEntry proporciona en tiempo de instalación, pero no acaba ahí el soporte de SecureEntry para otras redes. Si su red tiene una interfície para la conexión/desconexión de usuarios, resulta bastante fácil programar un módulo LMP (Procedimiento Modular de Conexión) que le permita conectarse a su red a la vez que se conecta a SecureEntry, mediante la sincronización de la contraseña de su red con la contraseña que SecureEntry guarda en su base de datos. Lea el manual de referencia del programador para saber como implementar esta solución.

¿Hay algún archivo de registro de la actividad de administración?

Sí. El archivo se llama EDYADMIN.LOG y está ubicado allí donde apunta la variable de entorno SGM_DB. Es un archivo de texto que quizá quiera purgar periódicamente. Observe que puede especificar qué información quiere registrar mediante la variable de entorno SGM_SL_LOGMODE desde su config.sys:

```
SET SGM_SL_LOGMODE=ALL      : registrar toda la actividad
SET SGM_SL_LOGMODE=UPDATES  : registrar sólo la actividad que modifique la base de
                              datos (Es el valor por defecto)
SET SGM_SL_LOGMODE=NONE     : no registrar nada
```

Creando una copia de seguridad de una estación SecureEntry

Sólo tiene que copiar de las máquinas servidoras (y monoestación), los siguientes archivos:

SecureEntryPath\NOUSER*.*

SecureEntryPath\INSTALL\SENTRY.CNF

SecureEntryPath\DLL\EDYCUST.DLL (si existe)

SecureEntryPath\DLL\EDYFILT.DLL (si existe)

SecureEntryPath\EXEC\EDYCUST.CMD (si existe)

El resto de archivos no son archivos específicos de su instalación.

¿Qué entradas del config.sys relacionadas con el SES puedo modificar?

Las variables soportadas por SecureEntry, son, básicamente:

GUESTNAME

Esta variable de entorno define el nombre de usuario que SecureEntry reconoce como usuario invitado. El valor por defecto es 'GUEST'.

AUTOGUEST

Esta variable de entorno, cuando toma por valor 'YES', fuerza que el SES arranque abriendo una sesión de usuario invitado. Esta sesión se abre sin que se lance un verdadero evento de conexión de sesión. Como el SLA de SecureEntry requiere un verdadero evento de conexión de sesión para poder activar y desactivar los perfiles de seguridad, se recomienda no cambiar el valor por defecto de ésta variable (valor='NO'), a no ser que se trabaje con un programa SLA propio. Si se quieren obtener resultados idénticos a los que se obtienen asignando a ésta variable el valor 'YES', puede utilizarse

cualquier exit de usuario apropiada que sea anterior a la de conexión para forzar una conexión de invitado.

TRUSTEDPATH

Esta variable de entorno, cuando toma por valor 'YES', fuerza que después de finalizar el evento de desconexión/bloqueo de la sesión se lance automáticamente un evento de conexión/desbloqueo de la sesión complementario . Si el valor es 'NO' el evento de conexión/desbloqueo no se lanza hasta que el usuario apriete una tecla.

RESTARTUSERSHELL

Esta variable de entorno define las condiciones en las que el segundo PMSHELL debe ser reinicializado. El valor 'YES' implica que el PMSHELL tiene que ser reinicializado cada vez que se realice una conexión de sesión. El valor 'NO' (valor por defecto para SecureEntry) indica que el PMSHELL debe ser reinicializado una sólo vez, en tiempo de arranque. Normalmente, éste es el valor que proporciona un mejor rendimiento.

Remítase a la documentación de SES para una explicación más amplia de ésta variable de entorno.

¿Hay más información disponible?

Estas son otras fuentes de información relacionadas con SecureEntry :

No olvide leer el arcivo readme.doc que viene junto al presente software.

El manual en línea 'Guía del administrador de UCM' proporciona información para poder instalar el UCM y solucionar problemas relacionados con este último.

La mayoría de los programas con interfície gráfica que SecureEntry proporciona, disponen de una detallada ayuda en línea para facilitar su manejo.

Hay también una versión impresa de este documento que puede explicar más detalladamente algunas de las funcionalidades aquí comentadas.

La documentación de IBM LAN server puede serle útil para conocer mejor los asuntos relacionadas con la configuración y administración en este tipo de entornos.

La documentación de SecureEntry 2.0 es una buen documento de referencia para las restricciones del escritorio, las utilidades VDM, y el proceso de arranque.

¿Cómo puedo proporcionar soporte NLS para otro lenguaje distinto del instalado?

Tiene todo el material necesario en el subdirectorio API\NLS de su directorio de SecureEntry. Se trata de realizar las traducciones que se requieran y luego generar el código objeto. Observe, sin embargo, que si sólo quiere traducir el entorno de ejecución (paneles de control de sesión), sólo tiene que traducir el archivo EDYERROR.TXT y generar un nuevo archivo de errores EDYERROR.MSG usando MKMSGF, que deberá ubicar en el subdirectorio EXEC de su directorio de SecureEntry.

¿Cómo puedo arrancar sesiones de comunicación CM/2 independientes según el usuario?

La regla de oro que SecureEntry utiliza para aislar dos sesiones de usuario distintas es la de matar, en tiempo de desconexión, todos aquellos procesos que fueron arrancados durante la sesión de usuario que finaliza. Esta política puede no ser del todo adecuada en algunos casos en los que exista un software base que deba estar siempre listo y ejecutándose (como es el caso de las emulaciones 3270) o de cualquier otra aplicación que

tenga un tiempo de arranque bastante alto que penalizaría seriamente el tiempo de inicio de sesión si tuviera que ser arrancada en cada conexión. La manera de manejar este tipo de aplicaciones es programar la exit de usuario 'antes de logon' para que finalice y reinicialice tales aplicaciones. De ésta manera se asegura la finalización y reinicialización de la aplicación cada vez que se procese un evento de desconexión. Por ejemplo, en el caso de los emuladores CM/2 3270 puede usarse la utilidad 'EDYE3270' que SecureEntry proporciona para realizar esta finalización/inicialización de forma automática.

Otra alternativa es usar el comando 'CMLINKS' de CM/2 para parar y reactivar los enlaces de comunicación, asegurando así el cierre de todas las sesiones lógicas que el usuario tenía abiertas. Se recomienda usar los comandos:

```
CMLINKS H *       para desactivar los enlaces
CMLINKS A *       para activar los enlaces
```

Obsérvese que este comando reinicializará todos los enlaces de la máquina, por lo tanto tenga cuidado si lo utiliza en máquinas servidoras de comunicaciones (gateways). i.e, especifique solamente aquellos enlaces que quiere cerrar en vez del asterisco.

¿Cómo puedo evitar que los usuarios arranquen con la combinación ALT-F1?

Puede emplear diferentes métodos para evitar el ALT-F1 :

1. Si quiere evitarlo por completo y no le importa recibir un mensaje de error, entonces, sólo tiene que renombrar los archivos \OS2\BOOT\ALTF1*.SCR.
2. Pero si quiere evitar el mensaje de error, entonces:
    1. No toque los archivos *.SCR
    2. Modifique el archivo \OS2\BOOT\ALTF1.CMD para que sólo procese las entradas que desee (tiene control sobre las opciones V,M,1...). Este archivo es un archivo CMD normal, y por lo tanto bastará con introducir un 'goto end' en el cuerpo de la rutina que no se quiera ejecutar.
    3. Si también quiere evitar la opción 'C' (ir a la línea de comandos), observe que esta opción usa el archivo \OS2\BOOT\CONFIG.X, por lo tanto, renombrándolo impedirá que la función se ejecute, y modificándolo para que se lance un evento de conexión de sesión garantizará plenamente la seguridad.
    4. También puede modificar el archivo ALTF1TOP.SCR para que muestre sólo las opciones que quiera tener activadas.

No puedo ejecutar el comando ACTIVATE de NDM/2

Antes de aceptar un comando ACTIVATE, NDM verifica si hay algún disquete en la unidad de floppy; si SecureEntry está restringiendo el acceso al floppy esta verificación suele fallar y devolver un error de severidad grave que fuerza al NDM a cancelar el comando...por si acaso.

Para evitar que el NDM realice esta verificación, defina en la máquina objetivo la siguiente variable de entorno :

```
SET ANXCHECKBOOT=NO
```

Otro aspecto que puede suponer un problema es el hecho de que el comando ACTIVATE necesita poder modificar el archivo config.sys. Esto sólo será un problema si el proceso de NDM que corre en el fondo se está ejecutando en contexto de usuario (i.e, no ha sido arrancado desde el config.sys, ni desde edystart.cmd,...). En este caso deben usarse perfiles de Treelock que den a los procesos de NDM los derechos de acceso necesarios para poder modificar el archivo config.sys. Puede añadir la siguiente línea a sus perfiles de Treelock :

```
F NdmPath\ANXCMCLx.EXE
```

Donde *NdmPath* es la ruta hacia los ejecutables de NDM, y *x* es 'C' para las máquinas NDM clientes, 'S' para las máquinas NDM servidoras.

Situaciones comunes en UCM

Esta sección contiene recetas y soluciones para los errores y situaciones más comunes cuando se trabaja con UCM.

Obtengo 'SQL error -805' cuando intento arrancar las utilidades de administración

Asegúrese que ha creado los empaquetamientos correspondientes y que ha vinculado correctamente los planes de acceso de UCM, tal y como se explica en Configuración de la estación administradora de UCM Tenga en cuenta que si ha actualizado la estación gestora de UCM puede que necesite revincular los planes con la base de datos del sistema principal.

Obtengo 'SLAG -8002E: Dynalink error' al ejecutar las aplicaciones de administración de UCM

```
SLAG -8002E: Dynalink error EDYUCM01.
```

Este error significa que usted no dispone de una licencia de DDCS/2. Debe procurarse una licencia de DDCS/2 y actualizar el archivo nodelock ubicado en directorio DB2/2.

Obtengo 'SQL error -204...' al ejecutar las aplicaciones de administración de UCM

```
SQL error -204 "Name" is an undefined name.
```

El programa no encuentra las tablas UCM en la base de datos DB2/MVS.

Debe verificar los sinónimos definidos en el MVS. Puede usar el miembro UCM.V30.DB2(CREASYNR) como modelo de entrada con SPUFI.

Obtengo 'SLAG -1013E: Dynalink error' al ejecutar las aplicaciones de administración de UCM

```
SLAG -1013E:  Dynalink error EDYUCM01.
```

Podría significar que se ha intentado acceder a un alias de base de datos que no ha podido ser encontrado. Asegúrese de que el directorio de la base de datos del sistema DDCS/2 esté correctamente configurado. Verifique que la variable de entorno SGM_UCM_DBDFT esté definida en el archivo UCMADM.CMD o en un archivo análogo y que tenga asignado un valor correcto.

Por supuesto, no olvide verificar que el archivo EDYUCM01.DLL sea accesible desde su libpath.

¿Hay algún ajuste que pueda mejorar el rendimiento de UCM?

Si tiene bastantes estaciones de trabajo y bastantes oficinas en su escenario UCM, puede ajustar los siguientes parámetros:

En la definición del nodo principal VTAM para UCM en SYS1.VTAMLIST o en la librería apropiada, defina EAS = 3999. Este parámetro especifica el número máximo de sesiones en esa LU. Esta definición no malgasta recursos en absoluto.

Opcionalmente, durante la instalación del Communications Manager/2, en la configuración DLC, puede seleccionar la opción "Free unused links". Esto permite liberar las sesiones inactivas. Observe que este parámetro puede acarrear problemas si se usan sesiones CP-CP, porque estas sesiones no deben ser liberadas.

Además, hay una serie de consideraciones y posibilidades de mejora del rendimiento específicas de UCM, que se detallan en el capítulo correspondiente de la guía de administración UCM.

¿Cómo puedo administrar a la vez entornos monoestación y Lan Server con UCM ?

Si vd. usa el procedimiento Actualización en línea de oficinas, entonces puede hacerlo sin problemas. EDYSRV ignorará la información relativa a recursos y accesos cuando baje las definiciones de oficina y de usuarios.

¡¡NOVEDADES!!

Este capítulo pretende ser una 'guía rápida' para usuarios que provengan de versiones o paquetes anteriores de SecureEntry y que quieran ponerse al día. Es una lista de las nuevas funcionalidades añadidas al producto, ordenadas cronológicamente (de más reciente a menos reciente), con enlaces hacia los puntos de la documentación que las describen en mayor detalle. Sin embargo, para una referencia completa de parches y añadidos, se recomienda leer el archivo README ubicado en el primer disquete de instalación, porque la lista que sigue a continuación sólo incluye las nuevas funcionalidades que se consideran más importantes para el producto.

Nuevo Examinador de archivos de anotación SecureEntry.

Nuevo soporte para restringir el acceso a los dispositivos del sistema a través del componente treelock. (recuerde especificar el nombre de dispositivo interno al escribir este tipo de restricciones, p.e, PCMCIA$ en vez de PCMCIA.SYS).

Soporte para clientes IBM Network Station de la serie 2800 bajo WorkSpace On-Demand

Nuevo tutorial SecureEntry/2. (distribuido por separado)

Nuevo componente de Definición de Procesos Auditables para mediciones de uso de CPU.

Nuevo LMP asociado a NSC/2 para sincronización de contraseñas.

Nuevo Soporte para WorkSpace On-Demand.

Nuevo soporte para la coexistencia con otras aplicaciones clientes de SES (p.e, Tivoli).

Nuevo soporte para instalaciones UCM con seguridad de acceso controlada por SecureEntry en el host, por medio del nuevo emulador de RACF (LMP UF).

Nuevo componente de Definición de Aplicaciones Públicas para entornos con LAN Server.

Nuevos diálogos de ejemplo de conexión y desbloqueo

Una nueva utilidad, EDYRVUCM, para poder corregir las tablas de cambios de la Base de Datos UCM.

Una nueva utilidad, EDYQRYBR, para poder consultar el nivel de todas sus oficinas.

Una nueva utilidad, EDYPHOTO, que obtiene un archivo imágen de la configuración de la máquina para facilitar actualizaciones del producto y el reporte de errores.

Un nuevo método de UCM de Actualización en línea de las oficinas para actualizar las definiciones de grupos y recursos en IBM Lan Server y una nueva funcionalidad para el Registro de la actividad UCM.

Una nueva funcionalidad de emulación de SES (Security Enabling Services emulation). Ahora puede instalar SecureEntry sin el código real de SES. Sin embargo, el FP17 o superior sigue siendo imprescindible si quiere poder utilizar el componente de Treelock.

Un nuevo componente de WarpCenter para los sistemas Merlin : El componente WarpCenter.

Nuevas funcionalidades dentro del componente de SES. Ahora puede configurar el fondo del escritorio y evitar o capturar las teclas especiales de sistema. Vea el capítulo Características del SES.

Una nueva sección en este documento sobre Códigos y mensajes de error.

Un nuevo componente, el Definición de objetos con activadores.

Una nueva utilidad, EDYDUMP.

La función mejorada Acerca de los procesos y contextos de ejecución.

Una nueva utilidad de chequeo de la integridad de los archivos SAF2GEN.

El componente de Treelock tiene más documentación y nuevas funcionalidades, incluído un editor gráfico de perfiles.

Una nueva utilidad de Salvaguarda del sector de arranque : EDYRWMBR.

El componente de Restricciones del escritorio ahora puede propagar estilos dentro de directorios, y soporta nuevas opciones de menús de Merlin, así como la opción de eliminar completamente el menú emergente de los objetos.

Una nueva utilidad de traducción de disquetes dentro del componente de Restricciones de la disquetera .

El nuevo componente de Definición de combinaciones de acceso rápido.

Una nueva utilidad, EDYLOGFS, para controlar automáticamente el tamaño de los archivos de registro.

El nuevo componente de Definición de escritorios personalizados.

En la sección Preparación de un controlador de dominio secundario (backup) para instalaciones Lan Server encontrará como preparar una máquina para que proporcione este nuevo tipo de soporte.

El nuevo componente de Restricciones de la lista de tareas.

Además, y sobre todo si es usted un integrador de SecureEntry, es recomendable leer las secciones Variables de Entorno y Programando exits de usuario, porque frecuentemente se añaden nuevas variables de entorno y exits de usuario.

Direcciones de contacto

Si tiene algún comentario que hacer o ha encontrado algún problema no documentado en los párrafos anteriores, le rogamos nos lo comunique...Por favor, diríjase a los siguientes IDs:

Dirección del equipo de SecureEntry

Fernando Velasco	Interno :	Fernando Velasco Benavente/Spain/IBM @ IBMES
	Externo :	VELASCO @ es.ibm.com

Responsable de solución

Fernando Trius	Interno :	Fernando Trius Chassaigne/Spain/IBM @ IBMES
	Externo :	FTRIUS @ es.ibm.com

Coordinación Técnica

Ramon Gonzalez	Interno :	Ramon Gonzalez Compta/Spain/IBM @ IBMES
	Externo :	RAMON_GONZALEZ @ es.ibm.com