



Edicom AS2 Server Manual de Usuario



Título del documento:	EDICOM AS2 SERVER
Nombre del fichero:	ES EAS Manual de Usuario v2.2.odt
Versión:	2.2
Estado:	VIGENTE
Fecha:	27/10/2011
Autor:	Departamento de I+D

Revisión, Aprobación

Revisado por:	Santiago Bellosta	Fecha: 27/10/2011
Aprobado por:	Santiago Bellosta.	Fecha: 07/11/2011

Historial de cambios

Versión	Fecha	Descripción de la acción	Páginas
1.0		Versión inicial.	
2.0	18/04/2011	Se modifica el documento para reflejar EAS sobre base de datos y nuevos requisitos mínimos.	Pág. 7
2.1	27/10/2011	Se incluye la descripción de los estados de situación de los mensajes en la descripción de las carpetas. Ya que ahora son equivalentes. Se elimina la explicación de la estructura de directorios ya que a partir de ahora no es necesaria. Se añade la descripción del proceso de instalación y el anexo Tabla de la base de datos.	Pág.18 , Pag. 61 y sig.
2.2	10/12/2013	Se añade configuración integración EBI en las propiedades de usuario propio.	Pág. 28

Índice de contenido

Capítulo 1. EAS, EDICOM AS2 Server.....	4	4.5 Certificados X509.....	35
1.1 Introducción.....	4	4.6 Alarmas	38
1.2 El proceso de la transmisión.....	4		
1.3 Beneficios de la tecnología AS2.....	5	Capítulo 5. Edicom AS2 Batch.....	44
1.4 Diferencias entre la tecnología AS1 y la tecnología AS2.....	6	5.1 Introducción.....	44
		5.2 Comandos Básicos envío y recepción.....	44
Capítulo 2. Instalación.....	7	5.3 Funciones de usuarios.....	47
2.1 Herramientas y Ejecutables.....	7	5.4 Funciones de certificados.....	51
2.2 Requisitos mínimos.....	7	5.5 Comentarios adicionales.....	52
2.3 Instalación del producto.....	8		
Capítulo 3. EDICOM AS2 Viewer.....	14	Capítulo 6. Envío y recepción de mensajes.....	53
3.1 Introducción.....	14	6.1 Introducción.....	53
3.2 Barra de Herramientas.....	16	6.2 Envío de mensajes de modo interactivo.....	53
3.3 Menú Contextual.....	17	6.3 Recepción de mensajes de modo interactivo.....	55
3.4 Mensajes de entrada.....	17	6.4 Envío de mensajes desde línea de comandos.....	55
3.5 Mensajes de Salida.....	18	6.5 Recepción de mensajes desde línea de comandos.....	55
3.6 Árbol de carpetas (Situación de un mensaje).....	18		
3.7 Listado de mensajes.....	19	Capítulo 7. Información adicional de un mensaje.....	57
3.8 Opción Configuración cliente.....	20	7.1 Introducción.....	57
		7.2 Propiedades de control.....	57
Capítulo 4. Configuración del Servidor.....	22	Capítulo 8. Anexo: logs de EDICOM AS2 Server.....	60
4.1 Introducción.....	22	8.1 Introducción.....	60
4.2 Configuración General.....	22		
4.3 Configuración Protocolos transporte.....	24	Capítulo 9. Anexo: Guía rápida de puesta en marcha EAS.....	61
4.4 Configuración de Dominios/Usuarios.....	26		
		Capítulo 10. Anexo: Estructura Base de datos EAS.....	62
		10.1 Introducción.....	62
		10.2 Tablas EAS.....	62

CAPITULO 1. EAS, EDICOM AS2 SERVER

1.1 Introducción

El EAS (EDICOM AS2 Server) es la solución implementada por EDICOM para intercambiar documentos empresariales a través de Internet de forma segura utilizando el protocolo HTTP con los formatos XML, Binary, Electronic Data Interchange (EDI –tanto ASC, X12 como UN/EDIFACT-) y otros datos codificables en MIME y utilizados en el intercambio de datos Empresa a Empresa.

Los datos se empaquetan utilizando los “content-types” estándar de MIME. La autenticación y la privacidad se consiguen utilizando S/MIME (Cryptographic Message Syntax). Los acuses de recibo autenticados se realizan mediante respuestas de tipo “multipart/signed” al mensaje HTTP original .

Hasta ahora los estudios y desarrollos relativos a “EDI sobre Internet” se habían centrado en especificar los “content-types” de datos EDI en mensajes MIME normalmente utilizando como transporte el protocolo SMTP, tal y como se especifica en la recomendación AS1 del EDIINT Working Group del IETF.

La tecnología AS2 completa los estudios anteriores del EDIINT ampliando su uso al protocolo HTTP e intentando reutilizar los estándares existentes en Internet para ello como son:

- [RFC 2616 Hyper Text Transfer Protocol](#)
- [RFC 1767 EDI Content Type](#)
- [RFC 2376 XML Media Types](#)
- [RFC 1847 Security Multiparts for MIME](#)
- [RFC 1892 Multipart/Report](#)
- [RFC 2045 to 2049 MIME RFC's](#)
- [RFC 2298 Message Disposition Notification](#)
- RFC [2630](#), [2633](#) S/MIME v3 Specification

1.2 El proceso de la transmisión.

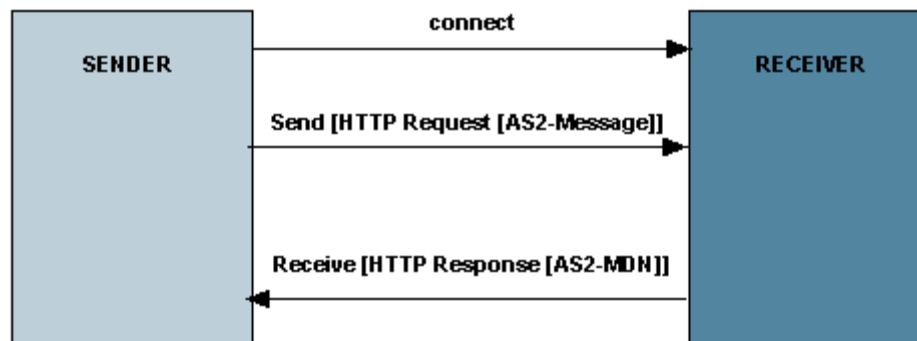
Se utiliza una operación HTTP POST para enviar los datos EDI, XML o cualquier otro dato empresarial. La dirección URI especificada en la operación (Request-URI) identifica un proceso que se encargará de desempaquetar y tratar el mensaje así como de generar una respuesta al cliente que contendrá un mensaje de acuse de recibo, firmado o no, o cualquier otra transacción relacionada.

Este intercambio transaccional de tipo “petición/respuesta” proporciona un medio de transporte seguro, fiable y autenticado a través de Internet utilizando HTTP. La estructura básica de un mensaje AS2 consiste en un formato MIME al cual se le han añadido algunas cabeceras AS2 específicas dentro de un mensaje HTTP.

Se contemplan dos posibilidades en la recepción del acuse de recibo en AS2:

1.2.1 ACUSE SÍNCRONO.

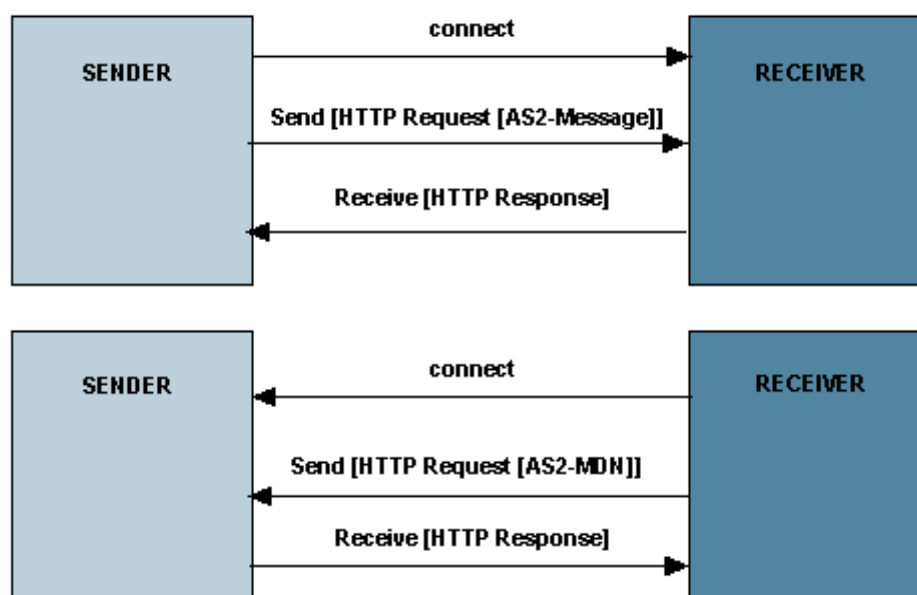
Synchronous AS2-MDN



En esta situación en la misma conexión se envía el mensaje y se recibe el acuse de recibo.

1.2.2 ACUSE ASÍNCRONO.

Asynchronous AS2-MDN



1.3 Beneficios de la tecnología AS2.

Los beneficios más claros de la tecnología AS2 son:

- AS2 proporciona unas transferencias de datos mucho más rápidas, casi instantáneas desde el origen hasta el destino, reduciendo por tanto los puntos de error en las transmisiones.

- AS2 proporciona mayor fiabilidad y velocidad, aumentando la eficiencia en la cadena de suministro.
- Disponibilidad teórica 24x7.
- Diseñado para enviar y recibir datos de forma segura por la red Internet
- Utilizando encriptación se garantiza que sólo el destinatario puede leer la información del mensaje.
- Utilizando firma electrónica se asegura la autenticación del origen.
- AS2 es capaz de detectar si el documento se ha alterado durante la transmisión.
- Los acuses de recibo firmados garantizan que el destinatario ha recibido el mensaje sin alteraciones.

1.4 Diferencias entre la tecnología AS1 y la tecnología AS2.

La diferencia más importante entre AS1 y AS2 es que AS1 utiliza como protocolo de transporte SMTP (el mismo utilizado en servidores de correo) y AS2 utiliza el protocolo HTTP (el mismo que se usa en los servidores web). Otra diferencia importante es que AS1 no permite la utilización de MDNs síncronos ni compresión de los mensajes. Actualmente la tecnología AS2 está más extendida que la AS1. El EDICOM AS2 Server también permite intercambiar mensajes mediante la tecnología AS1.

CAPITULO 2. INSTALACIÓN

2.1 Herramientas y Ejecutables

La distribución del EAS está formada por las siguientes herramientas ejecutables.

- **EDICOM AS2 Configuración BBDD** (*EAS2C.exe*). Permite la configuración de la Base de datos que soporta el servidor.
- **EDICOM AS2 Server** (*EAS2S.exe*). Es el servidor propiamente dicho. El EDICOM AS2 Server se puede lanzar de forma manual o instalar como un servicio del sistema operativo.
- **EDICOM AS2 Viewer** (*EAS2V.exe*): Panel de control visual para la configuración del servidor AS2 y el envío/recepción de mensajes de forma interactiva.
- **EDICOM AS2 Batch mode** (*EAS2B.exe*). Modo Batch (Desasistido) que permite configurar y lanzar los procesos necesarios para el envío/recepción de mensajes desde el sistema de gestión del usuario.
- **EBI Agent** (*EBIAGENT.exe*). Servicio encargado de lanzar de forma automática el servidor al iniciar el sistema operativo y de mantenerlo activo.

2.2 Requisitos mínimos

- Un PC compatible con IBM con un procesador Intel Core 2 Duo 2GHz o AMD equivalente.
- Disco Duro con 2 GB de espacio libre.
- Mínimo 2GB de memoria en RAM. Recomendable 4GB de RAM.
- Windows 2000 o superior (EAS sólo funcionará sobre plataformas gráficas de 32/64 bits)

En realidad las necesidades de EAS no son más de las requeridas por Windows, el recomendar una configuración como la apuntada es en aras de conseguir una velocidad adecuada.

La tecnología AS2 requiere además que el ordenador donde se instala el EAS (Servidor) disponga de:

- IP pública fija.
- Conexión permanente a Internet.
- Certificado para firma/encryptación de código.
- Certificado para conexiones HTTPS.

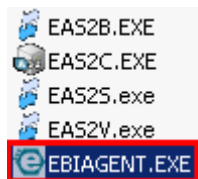
Importante: Si se desea intercambiar mensajes mediante el protocolo AS1 (SMTP), se necesita además un nombre de dominio SMTP registrado.

2.3 Instalación del producto

Los pasos para la instalación del producto consisten en:

1. Preparar el arranque del servidor como un servicio del Sistema operativo.
2. Configurar la conexión entre el servidor y la base de datos.
3. Configurar los datos de conexión del Servidor.
4. Configurar los datos de conexión entre el Servidor y el panel de control EDICOM AS2 Viewer.

2.3.1 ARRANQUE DEL SERVICIO.



Para iniciar el proceso de instalación el usuario debe seguir estos pasos:

- **Paso 1.-** Descomprimir los archivos de la distribución en un directorio del disco duro, por ejemplo C:\EAS\
- **Paso 2.-** Iniciar el servicio EBIAGENT.EXE con una instancia del EAS. ejecutando:

```
EBIAgent.exe -INSTALL -INSTANCIA "EAS"
```

El control del arranque automático del servidor realizado por el EBIAGENT.EXE se realiza desde los siguientes archivos de configuración.

INIS/EBIAGENT.INI

```
[EXES]
EAS=1
EAS_EBIMAP=0

[EAS]
ExeName=EAS2S.EXE
IPCF=1
DelayStart=0

[EAS_EBIMAP]
DirExename=C:\EAS\
ExeName=EBIMAPSj.EXE
IPCF=0
KillFlag=ebimap.kill
```


EBIAGENT_MULTIPROCES.INI

```

[EXES]
EAS_SOAP=1
EAS_SEND=1
EAS_RECEIVE=1
EAS_EBIMAP=0

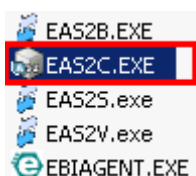
[EAS_SOAP]
ExeName=EAS2S.EXE
IPCF=1
DelayStart=0
ParamExe=-SENDOFF -RECEIVEOFF  RUTALOGS=C:\EAS\LOGS\SOAP\
KillFlag=SOAP.KILL

[EAS_SEND]
ExeName=EAS2S.EXE
IPCF=1
DelayStart=0
ParamExe=-RECEIVEOFF -SOAPOFF  RUTALOGS=C:\EAS\LOGS\SEND\
KillFlag=SEND.KILL

[EAS_RECEIVE]
ExeName=EAS2S.EXE
IPCF=1
DelayStart=0
ParamExe=-SENDOFF -SOAPOFF  RUTALOGS=C:\EAS\LOGS\RECEIVE\
KillFlag=RECEIVE.KILL

[EAS_EBIMAP]
DirExename=C:\EAS\
ExeName=EBIMAPSj.EXE
IPCF=0
KillFlag=ebimap.kill


```

2.3.2 EAS2C.EXE - CONFIGURACIÓN INICIAL DE LA BASE DE DATOS.

Una vez arrancado el servicio se debe configurar la base de datos que dará soporte a todo el servidor.

Para configurar la base de datos:

- **Paso 1.-** Se debe lanzar el ejecutable **EAS2C.EXE**.
- **Paso 2.-** Se debe completar la información del panel de configuración de la Base de datos. Un panel similar al siguiente.

- **Nombre de alias.** Permite indicar el nombre de Alias del acceso a la base de datos.
 - **Usuario/Password.** Permite indicar los datos de identificación para acceder a la base de datos.
 - **Tipo de alias.** Permite seleccionar el tipo de alias de acceso. Cada tipo tiene asociados distintos parámetros de configuración dependiendo de la base de datos.
- **Paso 3.-** El EAS2C.EXE genera por defecto una base de datos Access vacía a partir del archivo BASE.DAT distribuido con la Build del EAS. Esta base de datos por defecto puede cambiarse desde la configuración inicial seleccionando el icono  junto al campo **Configuración**. De este modo se accede a una segunda ventana con todos los datos de configuración para acceder a la nueva base de datos. En este último caso el EAS2C almacenará esta información en el archivo **INIS/EAS2S.INI**
 - **Paso 4.-** Una vez configurada las opciones se debe seleccionar el botón Aplicar Cambios y salir.

Importante: Versiones anteriores del EDICOM AS2 Server eran soportadas por un sistema de ficheros. Ahora toda la información del servidor y de los documentos se guarda en Base de datos. Para más información consultar el Anexo [Estructura Base de datos EAS](#)

INIS/EAS2S.INI

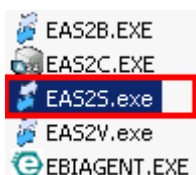
Se distribuye con la build del EAS un fichero llamado BASE.DAT que es una base de datos Access vacía para poder hacer una instalación inicial. Si no se modifica la configuración por defecto no se creará ningún fichero INI.

Sin embargo si se ha configurado una nueva base de datos, esa configuración personalizada se guardará en el archivo INIS/EAS2S.INI con un formato como este:

```
[ALIAS]
Nombre=EASBD
Usuario=EASADMIN
Config=SQLSERVER_N|SERVER_EAS|BD_EAS|dbnetlib,SERVER_EAS
PasswordE=4763148232602644722047733
[General]
Idioma=
```

Nota: *EAS2C.EXE* volverá a generar la base de datos Access por defecto si no encuentra este fichero o el segmento ALIAS en el directorio INIS.

2.3.3 EAS2S.EXE - CONFIGURACIÓN INICIAL DEL SERVIDOR.



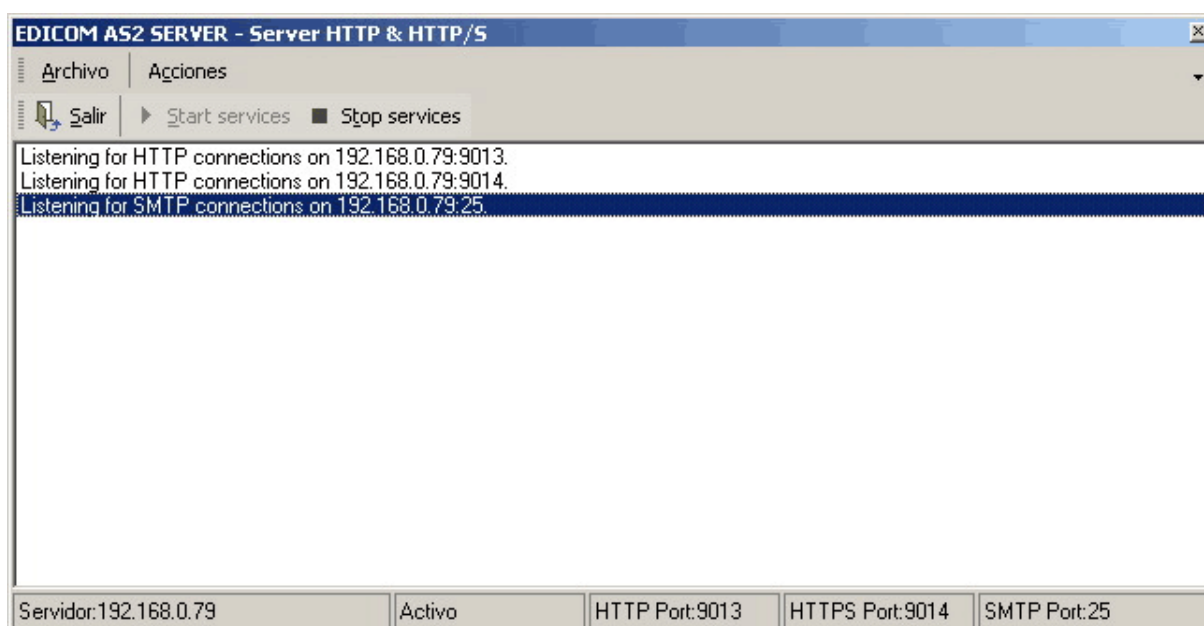
Una vez configurada la base de datos se debe arrancar el servidor EAS con el ejecutable **EAS2S.EXE**.

El **EDIWIN AS2 Server** puede lanzarse de dos formas:

- **Modo Interactivo.** El usuario debe lanzar manualmente el ejecutable EAS2S.EXE.
- **Modo Automático.** El servidor se instala como un servicio del sistema operativo y se inicia al iniciar el sistema.

Inicio del EAS en Modo interactivo

Para lanzar el **EDICOM AS2 Server** en modo interactivo, se ejecuta el archivo *EAS2S.exe*, visualizándose la siguiente pantalla con la actividad del servidor. En la barra de estado se visualiza información sobre la IP del servidor o los puertos utilizados para HTTP, HTTPS y SMTP.



En modo interactivo es posible detener el servicio con el botón **Parar Servicios** y reanudarlos de nuevo con **Comenzar servicios**.

Inicio del EAS en Modo servicio

Para realizar la instalación del **EDICOM AS2 Server** como un servicio del sistema operativo se utiliza la herramienta **EBIAGENT** (**EBIAGENT.EXE**) que se distribuye con el servidor. Desde Inicio/Ejecutar se lanza el siguiente comando:

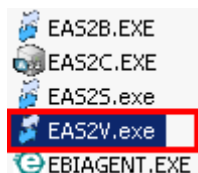
```
EAS_PATH/EBIAgent.exe -INSTALL -INSTANCIA "EAS"
```

Nota: "EAS_PATH" es el directorio donde se ha instalado el EAS.

A partir de este momento el **EBI Agent** se encarga de lanzar el EAS cada vez que se inicie el sistema operativo. La descripción del servicio instalado será "EBI Agent (EAS)". Si se desea parar o reiniciar el servidor, solo se tiene que parar o reiniciar el servicio instalado.

Nota: Más información en la opción [Configuración del Servidor](#).

2.3.4 EAS2V.EXE - CONFIGURACIÓN INICIAL DEL PANEL DE CONTROL



El **EDICOM AS2 Viewer** (**EAS2V.exe**) es una la interfaz de usuario visual que permite realizar la mayoría de las acciones que el usuario tiene disponible. Al iniciar el producto por primera vez es necesario configurar los parámetros básicos de conexión con el servidor **EDICOM AS2 Server**.

- **Paso 1.-** Lanzar **EDICOM AS2 Viewer** con el ejecutable **EASV.EXE**.
- **Paso 2.-** Aparecerá un formulario donde completar la información de conexión entre el **EDICOM AS2 Viewer** y el servidor EAS.

La información de conexión entre el EAS2V y el EAS puede modificarse posteriormente con la opción **Configurar cliente**.

EASV.ini

La información de configuración se aloja en el EASV.Ini

```
[SOAP]
DIRLOCAL=C:\EAS\VIEWER\
SERVER=127.0.0.1
PORT=9015
COMPRESSION=1
SECURE=0
USERSOAP=EAS
PASSSOAP=4762648200512584767648200

[GENERAL]
ADMINISTRACION=1
MODOSUPERVISOR=1
```

CAPITULO 3. EDICOM AS2 VIEWER.

3.1 Introducción

El **EDICOM AS2 Viewer** es una la interfaz de usuario visual que permite realizar la configuración del Servidor EAS: Creación de usuario, carga de certificados, parametrización de Envío y recepción, etc. y también enviar y recibir mensajes.

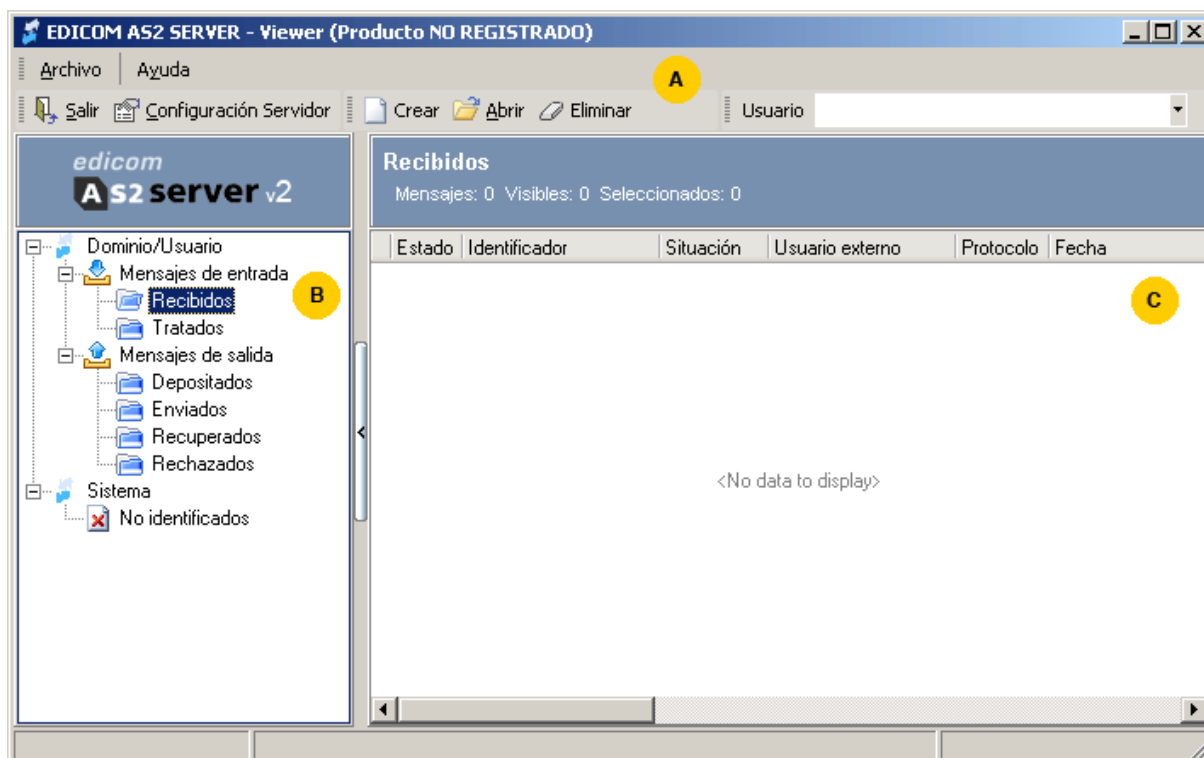
Las funciones del panel de control son

- Realizar la motorización de los documentos entrantes y salientes a través de una serie de carpetas que reflejan el estado de los documentos.
- Importar o exportar archivos entre la aplicación y el disco duro.
- Realizar el envío o recepción de archivos de forma manual.
- Permitir la configuración de la conexión entre el EDICOM AS2 Viewer y el EDICOM AS2 Server.
- Permitir la configuración del servidor. EDICOM AS2 Server.

3.1.1 PANEL DE CONTROL

Importante: El panel de control puede visualizarse como un usuario **Propio** o **Externo**. Eso se selecciona en el campo Usuario de la barra de herramientas. Los usuarios Externos tienen ciertas funcionalidades del menú inhabilitadas.

En el panel de control se distinguen las siguientes secciones.



- A) Menú principal en la parte superior del panel de control, con las opciones principales de la aplicación. Las opciones pueden variar según:
- Se haya seleccionado la carpeta de mensajes entrantes o salientes.
 - Se visualice el panel como usuario Propio o Externo.
- B) Árbol de carpetas con dos nodos diferenciados para los mensajes de entrada y salida.
- C) Área principal con el listado de mensajes asociado al dominio seleccionado en cada momento en el árbol de carpetas. Cada una de las filas corresponde a un mensaje individual.

3.1.2 MENÚ PRINCIPAL "ARCHIVO"

Configuración del servidor. Permite acceder a la pantalla de configuración del EDICOM AS2 Server. para más información consultar el capítulo [Configuración del Servidor](#)

Configuración del cliente. Permite acceder a la configuración del EDICOM AS2 Viewer.

Reconectar. Permite volver a conectar con el servidor.

Salir. Cierra el **EDICOM AS2 Viewer**. Si hay mensajes pendientes de enviar se enviarán de todos modos ya que el Servidor sigue funcionando.

Sub-menú "Mensajes AS1/AS2"

Crear. Permite crear y enviar un mensaje. No está habilitado para usuario Externo.
Abrir. Permite acceder a la información de envío/recepción del mensaje seleccionado.
Eliminar. Permite eliminar el mensaje seleccionado.
Refrescar. Permite refrescar la lista de los mensajes.
Buscar mensaje. Permite buscar un mensaje de la lista.

(Usuario propio ,nodo mensaje de entrada.)

Retraducir: Vuelve a analizar el mensaje AS2 y extrae de nuevo el contenido EDI del mensaje, sobrescribiendo cualquier información anterior.
Enviar MDN. Envía nuevamente el acuse de recibo para el mensaje recibido. El MDN y sus valores NO se vuelven a calcular.
Retraducir y enviar MDN. Realiza las dos opciones antes comentadas, con la diferencia de que además el MDN y sus valores SÍ son vueltos a calcular.

(Usuario propio ,nodo mensaje de salida.)

Reenviar. Permite reenviar el mensaje saliente seleccionado.

3.2 Barra de Herramientas

La barra de herramientas contiene las mismas opciones que el menú principal Archivo, además de las siguientes funciones.

3.2.1 SELECCIÓN Y CONFIGURACIÓN DE USUARIO.

Permite seleccionar el filtro de usuario con el cual vemos los mensajes. Solo vemos los mensajes asociados a dicho usuario.

El tipo de usuario activo en cada momento es importante. Si se selecciona un usuario externo alguna de las funcionalidades descritas en este punto no estarán disponibles.

3.2.2 CONFIGURACIÓN DE USUARIOS.

Permite acceder al panel de configuración de usuarios.

3.2.3 N° MENSAJES.

Permite indicar el número máximo de mensajes visibles en el área principal al mismo tiempo.

3.3 Menú Contextual

El menú contextual aparece al hacer clic derecho del ratón sobre el área principal de documentos. las opciones pueden estar inhabilitadas si se está visualizando el panel como un usuario Externo.

Crear. Permite crear y enviar un mensaje. No está habilitado para usuario Externo.
Abrir. Permite acceder a la información de envío/recepción del mensaje seleccionado.
Eliminar. Permite eliminar el mensaje seleccionado.
Refrescar. Permite refrescar la información visualizada por pantalla.
Seleccionar todos. Permite seleccionar todos los documentos visibles.
Importar. Permite importar documentos a la aplicación. No está habilitado para usuario Externo.
Exportar. Permite exportar documentos a un directorio local.
Buscar mensajes. Permite buscar documentos en el grid.
Agrupar. Permite activar a agrupación de documentos para organizar el listado de documentos.

Algunas de las opciones del menú contextual son distintas según se esté viendo el nodo Mensajes de entrada o Mensajes de salida. Estas opciones controlan los cambios de estado de los documento.

3.4 Mensajes de entrada

Retraducir: Vuelve a analizar el mensaje AS2 y extrae de nuevo el contenido EDI del mensaje, sobrescribiendo cualquier información anterior.
Enviar MDN. Envía nuevamente el acuse de recibo para el mensaje recibido. El MDN y sus valores NO se recalculan.
Retraducir y enviar MDN. Realiza las dos opciones antes comentadas, con la diferencia de que además el MDN y sus valores SÍ son recalculados.

3.5 Mensajes de Salida

Retraducir. Permite reenviar el mensaje saliente seleccionado.

3.6 Árbol de carpetas (Situación de un mensaje).

En la parte izquierda se visualiza el árbol de carpetas. La estructura de carpetas del árbol corresponde con la situación de un mensaje

3.6.1 NODO MENSAJES DE ENTRADA.

Esta carpeta los mensajes de entrada al dominio/usuario propio.

Recibido (REC). Indica, para los mensajes entrantes, que se ha recibido correctamente el mensaje del interlocutor externo y se ha conseguido extraer el fichero EDI original.

Tratado (TRA). indica, para los mensajes entrantes, que el mensaje ha sido procesado, pasando al sistema de gestión interna. Los mensajes tratados pasan de forma automática al *Histórico de documentos*.

Si el mensaje se encuentra en estado erróneo, se marcará con un aspa roja en la lista del **EDICOM AS2 Viewer**.

5. Errores de transporte durante el envío del mensaje.
6. No llega el acuse de recibo correspondiente.
7. El MIC del acuse de recibo no coincide con el MIC del mensaje enviado

3.6.2 NODO MENSAJES DE SALIDA.

Esta carpeta contiene los mensajes enviados del dominio/usuario propio. Cada uno de los mensajes puede

Depositado (DEP). Indica que el mensaje está listo para ser enviado, se enviará automáticamente. Este estado es un estado temporal, Si permanece durante mucho tiempo en este estado puede ser señal de algún problema de conexión o envío.

Enviado (ENV). Indica que el mensaje ha sido Enviado al destinatario, estando a la espera del acuse de recibo.

Recuperado (RCP). Indica que el mensaje ha sido Recuperado. Un mensaje pasa de situación *Enviado a recuperado* cuando se recibe el acuse de recibo. Este es el estado final positivo del proceso de envío.

Rechazado (RCH). Indica que el mensaje ha sido Rechazado. Un mensaje pasa de situación *Enviado* a *Rechazado*, si ha habido algún tipo de error con el envío/recepción del mensaje. Este es el estado final erróneo del proceso de envío y requiere atención. Un mensaje puede pasar a la *situación Rechazado RCH* por los siguientes motivos:

8. Errores de transporte durante el envío del mensaje.
9. No llega el acuse de recibo correspondiente.
10. El MIC del acuse de recibo no coincide con el MIC del mensaje enviado.

Nota: Para saber como obtener información adicional de un mensaje, como por ejemplo los logs de conexiones, [Información adicional y errores](#)

3.6.3 NODO SISTEMA.

Esta carpeta contiene mensajes que presentan alguna anomalía, por ejemplo mensajes que han sido recibidos por un protocolo no permitido para ese usuario, o mensajes que han sido recibidos pero que están dirigidos a un usuario propio que no existe.

3.7 Listado de mensajes

En la parte central se listan los mensajes correspondientes a cada carpeta seleccionada. La lista se actualiza automáticamente cuando el usuario cambia de carpeta en el árbol o si se utiliza la opción **Refrescar**.





3.7.1 DESCRIPCIÓN DE LAS COLUMNAS

- **Estado.** Estado del documento **OK** para documentos correctos y **ERR** para documentos en los que se ha detectado algún tipo de error.
- **Identificador.** Nombre identificador del fichero.
- **Situación.** Indica la situación en la que se encuentra el mensaje.
- **Usuario externo.** Indica el usuario externo que es el origen/destino del mensaje. Si el usuario que visualiza el listado es un usuario externo también estará visible el valor de Usuario propio.
- **Protocolo.** Indica el protocolo de comunicaciones utilizado que puede ser SMTP (AS1) o HTTP/HTTPS (AS2).
- **Fecha.** Indica la fecha y hora de creación del documento.
- **Certificado.** Indica si este mensaje ha sido firmado con las opciones de seguridad configuradas para el usuario.
- **Cifrado.** Indica si este mensaje ha sido Cifrado
- **Comprimido.** Indica si el mensaje a sido Comprimido.

- **MDN Solicitado.** Indica si para este mensaje se ha solicitado un MDN de respuesta.
- **Tipo MDN** Tipo de acuse, A/S para Asíncrono o SYNC para Síncrono.
- **Asunto.** Indica el asunto del mensaje.
- **Formato.** Indica el formato del mensaje enviado (X12, XML o EDI)
- **Fichero EDI.** nombre del fichero EDI a partir del cual se ha generado el mensaje AS2
- **Identificador Remoto.** Propiedades de control. Identificador remoto.
- **Fecha creación.** Fecha de creación del mensaje.
- **Transmisión.** Fecha de transmisión del mensaje.
- **Transmisión MDN.** Fecha de transmisión del MDN correspondiente.
- **Siguiente envío.** Fecha del siguiente envío de este mensaje.

3.7.2 ICONOS ASOCIADOS A UN MENSAJE

Asociados a cada documento puede haber un conjunto de iconos que representan sus propiedades. Esta información se refleja en las columnas correspondientes

	Certificado. Indica que el mensaje está firmado.
	Cifrado. Indica si el mensaje está cifrado.
	Comprimido. Indica si el mensaje está comprimido.
	MDN. Indica si el mensaje solicita un acuse de recibo (MDN) al destinatario.

3.8 Opción Configuración cliente.

La opción Configuración cliente permite configurar los parámetros con que el EDICOM AS2 Viewer se comunica con el servidor.

3.8.1 DATOS LOCALES

- **Directorio local.** Permite indicar el directorio donde se almacenarán los ficheros temporales creados durante la conexión al servidor.

3.8.2 CONEXIÓN VÍA WEB SERVICES.

Estos parámetros indican la configuración necesaria para que el **Edicom AS2 Viewer** pueda acceder vía WebServices al servidor **EAS**. Todos estos parámetros se pueden consultar en la configuración del EAS.

- **Servidor.** IP donde está instalado el **EDICOM AS2 Server**.
- **Puerto.** Puerto de acceso WebService del **EDICOM AS2 Server** (9015 por defecto)
- **Conexión segura (SSL).** Indica si se quiere realizar la conexión SOAP con servidor encriptando la información. El puerto por defecto del servidor para la conexión segura es el 9016.
- **Usuario.** Usuario de acceso al servidor por Web Service.
- **Contraseña.** Password de acceso al servidor por Web Service.

Importante: Se recomienda no modificar la configuración indicada por defecto.

CAPITULO 4. CONFIGURACIÓN DEL SERVIDOR.

4.1 Introducción

Una de las funciones del **EDICOM AS2 Viewer** es la configuración del servidor AS2. Se puede acceder a la configuración del **EAS** desde la barra de herramientas del **EDICOM AS2 Viewer**:

- opción del menú principal **Archivo**: opción **Configuración Servidor**.
- Barra de herramientas, botón **Configuración Servidor**.

De esta forma se accede al panel de configuración del servidor, dividido en cinco secciones.

- **General**. Permite la configuración del Servidor.
- **Protocolos transporte**. Permite la configuración de los distintos protocolos que pueden ser utilizados por el servidor. HTTP, HTTP/S, SMTP y SSL.
- **Dominios y Usuarios**. Permite la gestión de los Dominios y Usuarios del Servidor.
- **Certificados**. Permite la gestión de los Certificados Electrónicos alojados en el servidor. Estos certificados se utilizan para las opciones de seguridad implementadas en el envío de documentos.
- **Alarmas**. Permite la gestión de alarmas y avisos automáticos que el servidor puede enviar a una cuenta email de notificación.

Se pueden distinguir claramente cinco secciones en la configuración del servidor: **General**, **Protocolos**, **Dominios/Usuarios**, **Certificados** y **Alarmas**. que pueden seleccionarse en el menú de la izquierda.

4.2 Configuración General

En la pantalla de configuración *General* se puede acceder a las siguientes secciones:

General

- 1 Protocolos transporte
- 2 Dominios/Usuarios
- 3 Certificados X509
- 4 Alarmas

Directorios

Directorio de datos: C:\EAS\CONFIG\

Directorio local: C:\EAS\CONFIG\

Datos Servidor

Nombre/IP Externa: 192.168.0.51

IP Interna: 192.168.0.51

Nombre dominio SMTP: 192.168.0.51

Servidor DNS: 192.168.0.51

Acceso Web Services

Usuario: EAS Contraseña: XXXX

Puerto: 9015 Puerto Seguro: 9016

4.2.1 DIRECTORIOS

Importante: Los datos de Directorio de datos y Directorio local no deben ser modificados. Reflejan el directorio donde se aloja la Base de datos.

- **Directorio de datos.** Indica el directorio donde se almacenarán los mensajes enviados/recibidos por el servidor.
- **Directorio local.** Indica el directorio donde se almacenarán los ficheros de configuración del servidor.

4.2.2 DATOS SERVIDOR

- **Nombre/IP Externa.** Dirección IP externa del servidor (IP Pública). Si la IP pública tiene un nombre asignado en un servidor DNS se puede indicar el nombre. Si no se dispone de una IP pública en este campo se indicará la IP Privada del servidor dentro de la red local a la que está conectado.
- **IP Interna.** Si el servidor pertenece a una subred interna se indicará en este campo la IP privada del servidor. Si solo tiene una IP asignada (publica o privada) la IP interna y externa serán la misma.

- **Nombre dominio SMTP.** Este campo es necesario solo si se van a intercambiar mensajes por AS1. Se debe indicar un dominio válido en cualquier servidor de nombres (DNS). Además ese nombre debe estar registrado en el DNS como un servidor de correo. Si solo se quiere realizar una prueba de conexión entre dos interlocutores de un servidor se puede indicar en este campo la IP privada del servidor. No se puede intercambiar mensajes AS1 con otros servidores AS1 si no se tiene un nombre de dominio SMTP registrado, ya que la dirección de e-mail necesaria para identificar a un interlocutor AS1 de manera única se forma a partir del identificador del usuario propio y del nombre de dominio SMTP al que pertenece. Por ejemplo, si se introduce en este campo el texto "miDominio.com", la dirección de e-mail de un usuario propio cuyo identificador es "usuario1" sería: usuario1@miDominio.com.
- **Servidor DNS.** Se debe indicar la IP de un servidor de nombres (DNS).

4.2.3 ACCESO WEB SERVICES

Esta sección establece la configuración del servicio Web Service. El servicio Web Service permite que el **EDICOM AS2 Viewer** puede interactuar con el servidor. También se utiliza para integrar el EAS con el sistema de gestión interno de la empresa con la herramienta **EDICOM AS2 Batch**. Para configurar el Web Service se deben indicar los siguientes parámetros:

Datos de usuario para conectar con el Web Service:

- **Usuario.** Usuario para acceder al Web Service. Valor por defecto: "EAS"
- **Contraseña.** Contraseña del usuario para acceder al Web Service. Valor por defecto: "3A5" Por motivos de seguridad, se recomienda cambiar este password una vez se realice el primer acceso al servidor. No hay que olvidar actualizar también el nuevo password en la configuración del **Edicom AS2 Viewer**, para más información pulse aquí

Puertos del Web Service:

- **Puerto.** Indica el puerto de escucha del Web Service. Valor por defecto: 9015
- **Puerto Seguro.** Indica el puerto de escucha seguro (SSL) del Web Service. Valor por defecto: 9016

4.3 Configuración Protocolos transporte

En la pantalla de configuración *Protocolos de transporte* se diferencian las siguientes secciones:

0 General

1 Protocolos transporte

2 Dominios/Usuarios

3 Certificados X509

4 Alarmas

HTTP (AS2)

Puerto Externo Puerto Interno Activar log HTTP ☒

Desactivar protocolo HTTP ☐

HTTP/S (AS2)

Puerto Externo Puerto Interno Activar log HTTPS ☒


Desactivar protocolo HTTPS ☐

SMTP (AS1)

Puerto Interno Activar log SMTP ☒

Desactivar protocolo SMTP ☐

SSL

Certificado 

4.3.1 HTTP (AS2)

- **Puerto externo.** Puerto por el que se reciben las conexiones HTTP.
- **Puerto interno.** Puerto interno por el que reciben las conexiones. Para más información pulse aquí
- **Activar log HTTP.** Si se activa esta opción, se almacenan todos los eventos que ocurren en una conexión HTTP.
- **Desactivar protocolo HTTP.** Si se activa esta opción, se anula el protocolo HTTP.

4.3.2 HTTPS (AS2)

- **Puerto.** Puerto por el que se reciben las conexiones HTTPS.
- **Puerto interno.** Puerto interno por el que reciben las conexiones. Para más información pulse aquí
- **Activar log HTTPS.** Si se activa esta opción, se almacenan todos los eventos que ocurren en una conexión HTTPS.
- **Desactivar protocolo HTTPS.** Si se activa esta opción, se anula el protocolo HTTPS.

4.3.3 SMTP (AS1)

- **Puerto.** Puerto por el que se reciben las conexiones SMTP.
- **Activar log SMTP.** Si se activa esta opción, se almacenan todos los eventos que ocurren en una conexión SMTP.
- **Desactivar protocolo SMTP.** Si se activa esta opción, se anula el protocolo SMTP.

4.3.4 SSL

- **Certificado:** Certificado necesario para establecer un canal de comunicación seguro mediante el protocolo de seguridad SSL. No se pueden establecer conexiones HTTPS sino se dispone de un certificado SSL. Para dar de alta un certificado en la aplicación, ver el apartado Certificados.

Importante: Si se tiene instalado un firewall en la red en la que está el servidor, se deberá habilitar el tráfico en los puertos que se hayan indicado en los puntos anteriores.

Explicación del campo “Puerto interno”:

Existen empresas que por ejemplo para un servidor por ejemplo de correo, utilizan una IP y puerto público diferentes de la IP privada y puerto interno donde se está ejecutando el servidor. Esto se consigue modificando la configuración del cortafuegos o firewall para que redirija las peticiones externas a la IP y puerto correspondientes mediante un mapeo de direcciones IP y puertos.

Con esta opción el servidor de AS2, puede ser configurado para tener un puerto público diferente del puerto interno.

Importante: Para el correcto funcionamiento del puerto interno, tiene que estar correctamente configurado el cortafuegos o firewall de su empresa, para realizar el mapeo de puertos correspondiente.

4.4 Configuración de Dominios/Usuarios

La configuración de dominios y Usuarios permite crear dominios independientes y sus usuarios, tanto propios como externos. Cada domino esta estructurado entre

- **Usuarios Propios.** El interlocutor o interlocutores propios del dominio. Se entiende por usuario propio, por ejemplo, la empresa que va enviar y recibir mensajes utilizando el servidor.
- **Usuarios Externos.** El interlocutor o interlocutores externos del dominio. Se entiende por usuario externo, por ejemplo, aquellas empresas de las que se espera recibir o a las que se desea enviar mensajes utilizando el Servidor.

En la pantalla de configuración *Dominio/Usuarios* se disponen de las siguientes acciones



disponibles en el menú contextual. (Botón derecho del ratón).

Añadir. Permite añadir un nuevo elemento a la estructura de Dominios y Usuarios. según el nodo seleccionado en ese momento se trata de:

- Añadir un nuevo dominio.
- Añadir un nuevo usuario propio, teniendo seleccionado el nodo Propios de un determinado dominio
- Añadir un nuevo usuario externo, teniendo seleccionado el nodo Externos de un determinado dominio.

Eliminar. Permite eliminar el elemento seleccionado en ese momento.

Propiedades. Permite acceder a las propiedades del usuario seleccionado.

4.4.1 CREACIÓN DE DOMINIOS

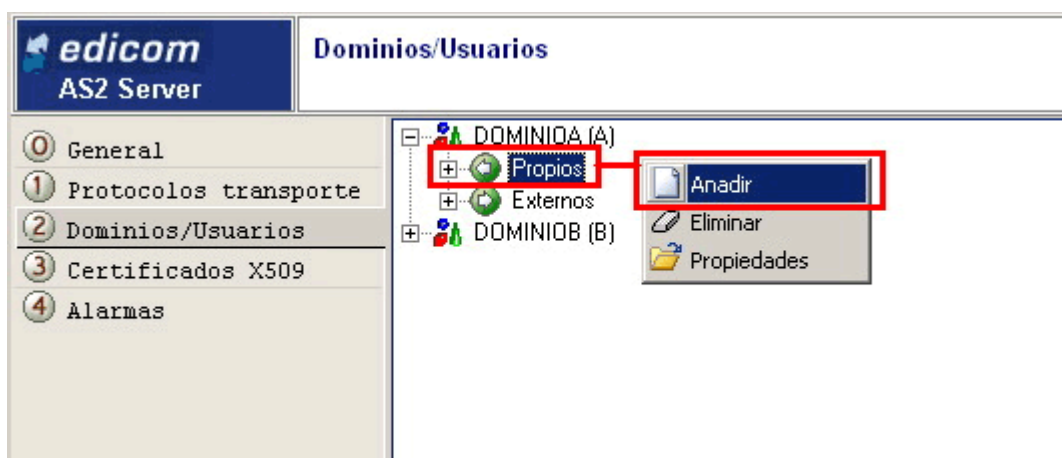
Para la creación de dominios se debe situar el puntero del ratón sobre un dominio ya existente, mostrar el menú contextual con el botón derecho del ratón y desde:

- Menú contextual: Opción **Añadir**.

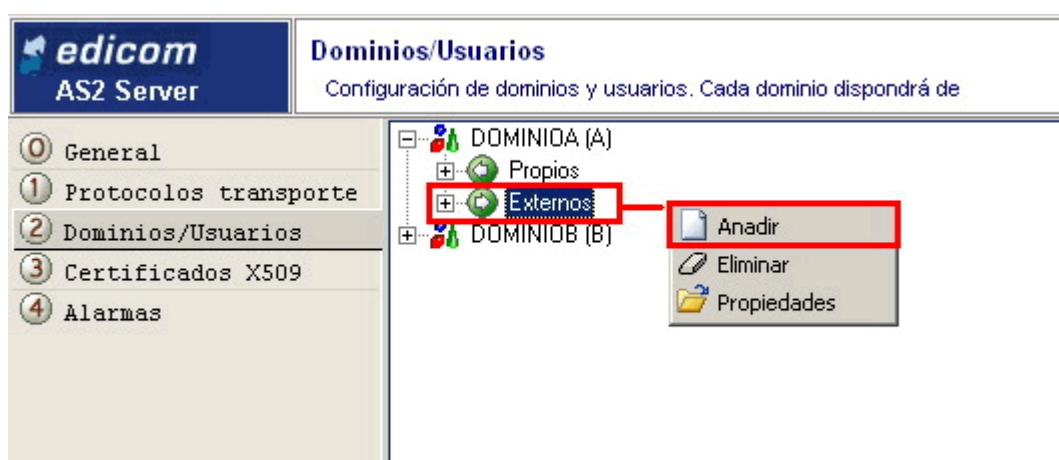
Si no hay ningún dominio ya creado, la opción **Añadir** muestra siempre la pantalla de creación de un nuevo dominio.

4.4.2 CREACIÓN DE USUARIOS

Para la creación de usuarios se debe primero seleccionar el subnodo adecuado del dominio para crear un interlocutor Propio o un interlocutor Externo. El grupo de interlocutores seleccionado dicta si se crea un nuevo usuario Propio o Externo.



Nota: para añadir un usuario propio, partir del nodo Propios



Nota: para añadir un usuario Externo, partir del nodo Externos.

4.4.3 UNA VEZ SELECCIONADO EL NODO CORRECTO, DESDE:

- Menú contextual. Opción **Añadir**.

Aparece así el panel de configuración de un nuevo usuario, Ya sea Propio o Externo. Existen diferencias entre la configuración de un usuario propio y uno externo que se explican a continuación.

4.4.4 CONFIGURACIÓN DE USUARIOS PROPIOS

Al crear un usuario propio o acceder a sus propiedades se visualiza la siguiente pantalla de configuración.

edicom AS2 server v2 Usuario **USER_EASTEST_01**

Datos generales

Descripción: USER_EASTEST_01

Certificado SMIME(1): certUser1 (1E35F8D12DC4EF7)

Datos de autenticación

Usuario local: USER_EASTEST_01 Contraseña local: [oculto]

Conexiones de entrada

Activar HTTP: ☒ Activar HTTPS: ☒ Activar SMTP: ☒

Usuario en test: ☐

Integración EBI

Activar EBI: ☒ URL Broker: https://aspebi.sedeb2b.com:9020/services/EBIBroker

Usuario: usuario Contraseña: [oculto]

Dominio: PRODUCCION Aplicación: APP

Referencia: REFERENCIA1234 Destino: DESTINO

Esquema: EDI_INVOIC Patrón: Content,*.ORDER.*,EDI_C

Duplicados: Ignorar duplicados

Otras propiedades

Nº de días en el histórico: 7

Tiempo máximo de espera del MDN: 1 Días

Nº de intentos de envío (inmediatos): 3

Nº de envíos posteriores: 3

Intervalo entre cada envío posterior: 1 Días

Alarmas

Destinatarios: alert@domain.com

Asunto: USER_EASTEST_01: Problemas en el mensaje

☐ Desactivar TODAS las alarmas relacionadas con este usuario

La pantalla de configuración contiene las siguientes secciones:

Datos generales:

- **Descripción.** Permite indicar el nombre del usuario propio.
- **Certificado SMIME (1).** Permite indicar el certificado del interlocutor propio. Se utiliza para firmar los mensajes que envía el usuario propio. También se utilizar para descifrar los mensajes encriptados que recibe el usuario propio. Antes de poder asignarle el certificado es necesario darlo de alta en el servidor. En la selección solo aparecen aquellos certificados que incluyen una clave privada. Para más información consultar la sección [gestión de certificados](#).

Datos de autenticación:

- **Usuario local.** Identificador del usuario para acceder a sus mensajes. Es utilizado por la herramienta Edicom AS2 Batch para acceder a sus mensajes a través de Web Service.
- **Contraseña local.** Contraseña del usuario que permite acceder sus mensajes mediante Web Service.

Importante: Es muy importante asignar un password al usuario propio para evitar que otras personas puedan acceder mediante el Edicom AS2 Batch a nuestros mensajes.

Conexiones de entrada.

- **Usuario en test.** Si se activa esta opción se indica al **Edicom AS2 Batch** que no procese los mensajes recibidos por este interlocutor. De esta forma se evita que lleguen al sistema de gestión interno de la empresa mensajes de prueba enviados por algún interlocutor externo. Una vez terminadas las pruebas, se pueden borrar los mensajes de pruebas que no se deseen y desactivar esta opción para que el resto de mensajes recibidos pasen al sistema interno.
- También se pueden indicar los protocolos por los que se quiere recibir conexiones. Para poder recibir mensajes por un protocolo se deben activar su protocolo. Si un interlocutor externo envía mensajes por un protocolo de transporte no permitido, los mensajes no serán procesados y pasarán a la carpeta de Sistema.
 - **Activar HTTP.** Permite activar el protocolo HTTP.
 - **Activar HTTPS.** Permite activar el protocolo HTTPS.
 - **Activar SMTP.** Permite activar el protocolo SMTP.

A continuación como configurar cada uno de estos tres protocolos.

Conexión por HTTP/HTTPS

Cuando se quiera intercambiar mensajes con otros interlocutores, se solicitará la URL de conexión de los usuarios propios. Todos los usuarios propios del EAS tienen la misma URL de conexión, que es la siguiente:

```
HTTP: http://IP_DEL_SERVIDOR:PUERTO_HTTP
HTTPS: https://IP_DEL_SERVIDOR:PUERTO_HTTPS
```

Por ejemplo si el servidor tiene la IP externa 212.147.48.10, el puerto HTTP es el 9013, y el puerto HTTPS es el 9014, la URL de los usuarios propios sería:

```
HTTP: http:// 212.147.48.10:9013
HTTPS: https:// 212.147.48.10:9014
```

Conexión con SMTP (AS1)

En el caso de SMTP (AS1) se solicitará a los interlocutores una dirección de e-mail. La dirección de mail es diferente para cada usuario propio ya que se construye a partir del identificador del usuario propio y del dominio SMTP asignado al servidor EAS:

```
identificador_usuario@dominio_SMTP
```

Por ejemplo si el nombre de dominio SMTP es "EAS.com", el usuario propio del servidor cuyo identificador es "USUARIO1", se identificará con la dirección de mail "USUARIO1@EAS.com".

Nota: Se pueden consultar todos estos datos del servidor en la pantalla de configuración general del servidor y en la pantalla de protocolos de transporte.

Integración EBI

- **Activar EBI.** Permite activar la integración con EBI desde EAS. Se debe seleccionar la URL del servicio EBIBroker a través del cual se publicará.
- **Usuario.** Permite indicar el usuario de acceso al servicio EBIBroker.
- **Contraseña.** Permite indicar la contraseña de acceso al servicio EBIBroker.
- **Dominio.** Permite indicar el dominio EBI en que se publicarán los mensajes.
- **Aplicación.** Permite indicar la aplicación EBI para la publicación.
- **Referencia.** Permite indicar la Referencia del documento/s publicados.
- **Destino.** Permite indicar el Destino EBI de publicación
- **Esquema.** Permite indicar el esquema por defecto de publicación de documentos.
- **Patrón.** Permite indicar una o varias expresiones regulares que en caso de ser localizadas en el Contenido, Asunto o Nombre de archivo, forzarán la publicación en un esquema de documento u otro. La sintaxis para completar este campo debe ser:

```
<buscar en>,ExpReg1,Esquema1,ExpReg2,Esquema2
```

- El primer elemento de la lista define dónde se debe buscar la expresión regular, Las opciones son:
 - "content ". Buscar el patrón en el contenido del fichero.
 - "subject ". Buscar el patrón en el subject del fichero.
 - "filename". Buscar el patrón en el nombre de fichero.
- El resto de elementos corresponden por parejas a la expresión regular y el esquema de documento correspondiente en caso de ser encontrada.

Por ejemplo:

```
content,.*ORDER.*,EDI_ORDERS,.*INVRPT.*,EDI_INVRPT
```

Si se encuentra *.ORDER.* en el "contenido" se publicará como un pedido (EDI_ORDERS). Si se encuentra *.INVRPT.* se publicará como reporte de facturas (EDI_INVRPT). En caso que no se cumpla ninguna de las condiciones, se aplicará el valor del campo "Esquema".

- **Duplicados.** Permite indicar el comportamiento del EBI frente a publicaciones duplicadas.
 - **Ignorar duplicados.** Se generará una nueva Publicación.
 - **Aceptar duplicados.** No se generará una nueva publicación, ni sus suscripciones correspondientes, y se devolverá el identificador de la publicación que tiene el mismo HASH.

- **Generar un Error.** Generará un código de error.

Nota: Se entiende por duplicados dos documentos con el mismo HASH dentro del mismo dominio y aplicación.

Otras propiedades:

- **Nº de días en el histórico.** Indica el número de días que permanecerá el mensaje en el Histórico de Mensajes, una vez sobrepasado este número de días el mensaje será eliminado del servidor.
- **Nº de reintentos de envío (inmediato).** Indica el número de intentos de envío de un mensaje tras el primer intento de envío. Esta opción permite resolver problemas momentáneos en las redes de comunicación. Si se excede el límite de reintentos el mensaje pasará a situación igual a Rechazado (RCH) si no se ha configurado un posterior reenvío.
- **Reenvíos.** Permite indicar al servidor que una vez terminado el número de reintentos inmediatos sin éxito, intente establecer la conexión pasado un intervalo de tiempo. Se tienen que configurar dos parámetros:
 - **Ejecutar.** Indica el número de intentos de reenvío.
 - **Reenvios cada.** Indica el intervalo de ejecución del reenvío. (Se puede indicar días, horas o minutos)

Por ejemplo, si se configura un reintento cada dos horas, un mensaje que no se ha podido enviar a las 15:00 horas en el primer intento, se volverá a intentar a las 17:00, y sino se consigue, a las 19:00 horas.

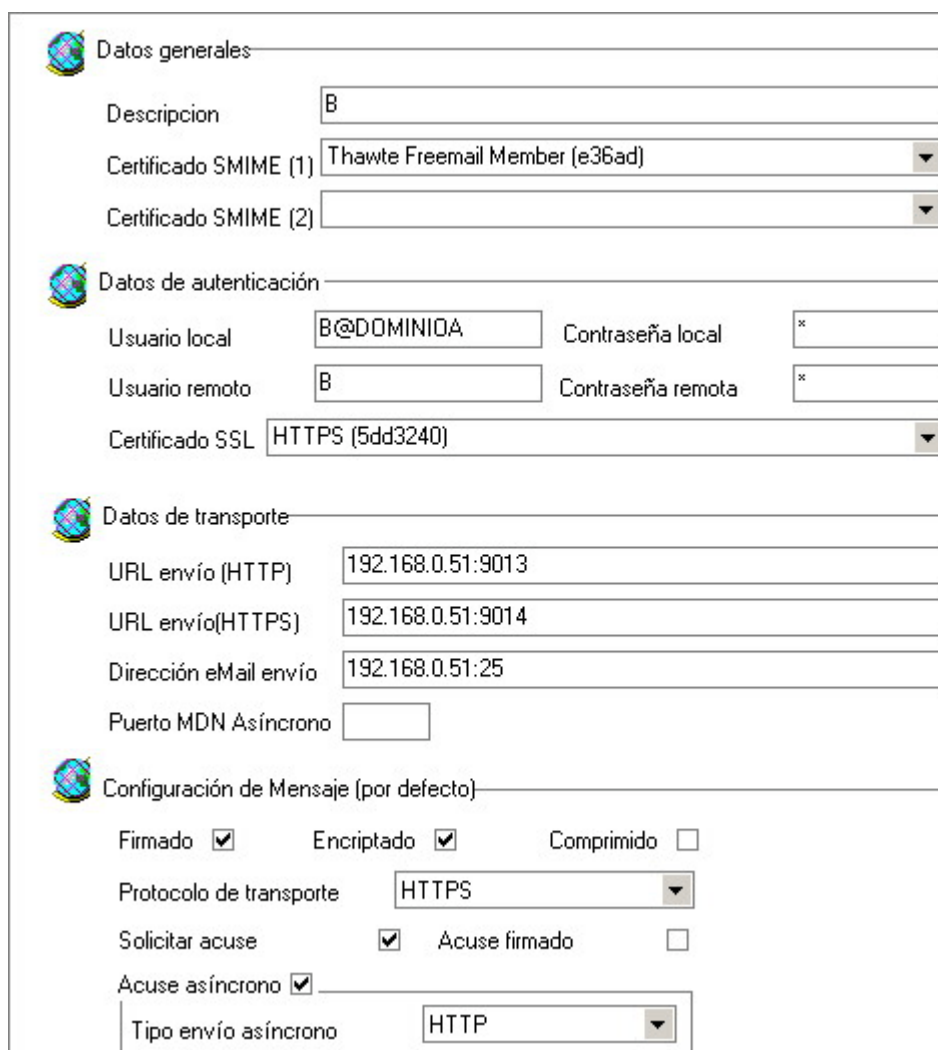
- **Tiempo máximo de espera del MDN.** Indica el número de días/horas máximo de espera de un acuse de recibo. Si no se recibe ningún acuse durante este intervalo de espera, el mensaje pasará a la situación de "Rechazado" (RCH).

Alarmas

- **Destinatarios.** Indica los destinatarios de alarma enviada. Para indicar varios destinatarios, se deben separar con punto y coma.
- **Asunto.** Indica el asunto que se enviará con la alarma enviada.
- **Desactivar todas las alarmas relacionadas con este usuario.** Si se activa no se enviarán las alarmas al destinatario.

4.4.5 CONFIGURACIÓN DE USUARIOS EXTERNOS

Al crear un usuario externo o acceder a sus propiedades se visualiza la siguiente pantalla de configuración.



Datos generales

Descripción: B

Certificado SMIME (1): Thawte Freemail Member (e36ad)

Certificado SMIME (2):

Datos de autenticación

Usuario local: B@DOMINIOA Contraseña local: *

Usuario remoto: B Contraseña remota: *

Certificado SSL: HTTPS (5dd3240)

Datos de transporte

URL envío (HTTP): 192.168.0.51:9013

URL envío(HTTPS): 192.168.0.51:9014

Dirección eMail envío: 192.168.0.51:25

Puerto MDN Asíncrono:

Configuración de Mensaje (por defecto)

Firmado ☒ Encriptado ☒ Comprimido ☐

Protocolo de transporte: HTTPS

Solicitar acuse ☒ Acuse firmado ☐

Acuse asíncrono ☒

Tipo envío asíncrono: HTTP

La pantalla de configuración de usuarios externos se divide en las siguientes secciones.

Datos generales:

- **Descripción.** Permite indicar el Nombre del usuario externo del dominio.
- **Certificado SMIME(1).** Permite indicar el certificado necesario si se selecciona en Configuración de mensaje la opción de enviar mensajes cifrados. La selección se realiza de la lista de certificados cargados previamente desde la pantalla para la gestión de certificados. También se utiliza este certificado para verificar los mensajes firmados que recibimos del interlocutor externo
- **Certificado SMIME(2).** Permite indicar el certificado adicional utilizado para verificar el mensaje firmado si falla con el Certificado SMIME (1).

Datos de autenticación:

- **Usuario local.** Si se requiere autenticación básica en nuestro servidor, un interlocutor externo deberá indicar en su conexión este usuario.
- **Contraseña local.** Contraseña del usuario local para autenticación básica.

- **Usuario remoto.** Cuando el servidor del interlocutor externo requiere autenticación básica, para conectarse al servidor, se debe realizar utilizando este usuario.
- **Contraseña remota.** Contraseña del usuario remoto para autenticación básica.
- **Certificado SSL.** Certificado del servidor remoto para garantizar la seguridad del canal de comunicación. Este certificado solo es necesario si se va a establecer una conexión por HTTPS con el modo autenticación por servidor.

Nota: Los datos viajan cifrados aunque no sea utilizado el modo de autenticación por servidor.

Datos de transporte:

- **URL envío (HTTP).** Se debe indicar la URL y el puerto donde espera la conexión HTTP el servidor remoto. Ejemplo: 192.168.0.79:9013
- **URL envío (HTTPS).** Se debe indicar la URL y el puerto donde espera la conexión HTTPS el servidor remoto. Ejemplo: 192.168.0.79:9014
- **Dirección e-mail de envío.** Este parámetro solo es necesario indicarlo si realizamos intercambios por AS1. Debemos introducir la dirección e-mail del interlocutor externo.
- **Puerto MDN Asíncrono.** Permite indicar el puerto por que se quiere recibir el mdn (Acuse) asíncrono que envía el destinatario. Si no se indica ningún valor se utiliza el puerto por defecto asociado al protocolo indicado en los datos de transporte del mdn.

Configuración del Mensaje (por defecto)

El **EAS** permite indicar una configuración por defecto para los mensajes que se enviarán a un interlocutor externo. La configuración de un mensaje tiene los siguientes parámetros:

- **Firmado.** Se deberá disponer de un certificado con clave privada para el interlocutor propio.
- **Encriptado.** Se deberá disponer del certificado con clave pública del interlocutor externo.
- **Comprimido.** Realiza una compresión del contenido del mensaje.
- **Protocolo de transporte.** Indica el protocolo de transporte usado para enviar el mensaje (HTTP, HTTPS o SMTP).

Configuración del acuse de recibo:

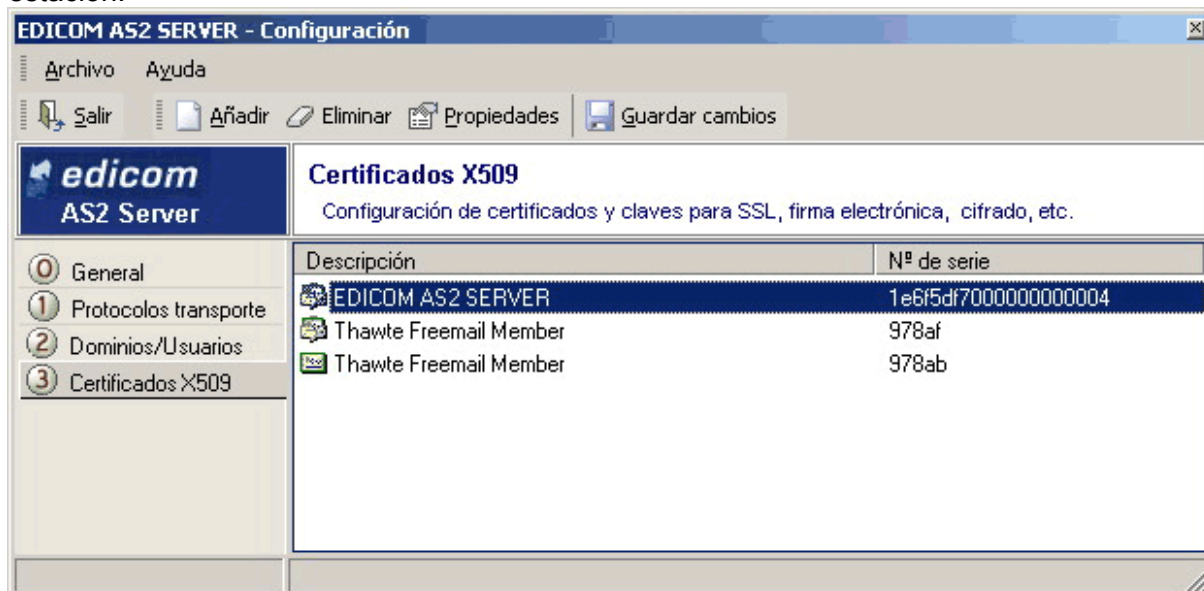
- **Solicitar acuse.** Solicita el envío de acuse una vez recibido el mensaje en el servidor remoto.
- **Acuse firmado.** Solicita que el acuse enviado por el servidor remoto esté firmado.
- **Acuse asíncrono.** Si se desea recibir el acuse de forma asíncrona, se debe marcar esta opción. Si no se activa esta opción, el acuse se recibirá de forma síncrona.

- **Tipo de envío asíncrono.** Indica el tipo de transporte (HTTP, HTTPS o SMTP) para el envío del acuse de recibo del mensaje en el caso de que se solicite un acuse asíncrono.

Nota: Si se usa el protocolo SMTP (AS1) el acuse de recibo siempre es asíncrono y utilizando el protocolo SMTP.

4.5 Certificados X509

En la pantalla de configuración Certificados se listan los certificados que hay cargados en la estación.



Se listan tanto los certificados propios, con clave privada, para la firma de mensajes salientes y los certificados externos, enviados por los interlocutores, para confirmar la validez de sus mensajes entrantes en el servidor.

Las opciones del menú contextual de este panel de control son

Añadir. Permite añadir un nuevo certificado
Eliminar. Permite eliminar el certificado seleccionado.
Propiedades. Permite acceder a las propiedades del certificado seleccionado.
Generar auto-certificado. Permite generar un certificado generado por el propio EAS, para testeos. Estos certificados no están reconocidos por ninguna autoridad de Certificación.

4.5.1 GESTIÓN DE CERTIFICADOS

Añadir un certificado

Para dar de alta de un nuevo certificado se debe pulsar el botón derecho del ratón sobre la lista de certificados y desde:

- Menú contextual: opción **Añadir**.

A continuación se muestra un formulario para importar certificados que permite buscar en el directorio local el archivo del certificado a importar. El campo **Contraseña** solo se deberá indicar para importar el certificado en caso de que se trate un certificado con clave privada para un usuario propio (con el que se firmarán los mensajes salientes). Los certificados con clave privada tienen un icono diferente de los que solo tienen clave pública.

Para ver las propiedades de un certificado se debe seleccionar del listado y desde: Menú contextual: opción **Propiedades**.

- o haciendo doble clic sobre el certificado.

Se accede así a la ventana de propiedades del certificado. La Información del certificado cargado se indica automáticamente:

- **Descripción.** Indica la descripción del certificado.
- **Nº de serie.** Indica el Nº de serie del certificado.
- **Emisor.** Indica la autoridad de certificación emisora del certificado.
- **Usuario.** Indica la información del usuario autorizado del certificado. A quien se a emitido.
- **Periodo de validez.** Indica el periodo de vigencia del certificado.
- **Tengo confianza en este certificado.** Indica al servidor que los mensajes firmados con este certificado son de confianza. Se activa por defecto. Si no se confía en un certificado debe eliminarse del servidor.

EDICOM AS2 SERVER - Propiedades de certificado

edicom AS2 Server | **Certificado Thawte Freemail Member**

Datos del certificado

Descripción: Thawte Freemail Member

Nº de serie: 978af

Emisor: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte, OU=Certificate Services, CN=Personal Freemail RSA 2000.8.30

Usuario: CN=Thawte Freemail Member/Email=edicomsm1@edicom.es

Periodo de validez: 10/03/2003 12:07:00 - 09/03/2004 12:07:00

Tengo confianza en este certificado ☒

Exportar certificado **Aceptar**

Eliminar un certificado

Para eliminar un certificado, seleccionar el certificado a eliminar del listado y desde : Menú contextual: Opción **Eliminar**.

Visualizar las propiedades

Para visualizar de nuevo las propiedades de un certificado o acceder a la opción Exportar certificado, se puede seleccionar del listado y desde:

- Menú contextual: Opción **Propiedades**
- O doble clic sobre el certificado seleccionado.

Se accede así de nuevo a las propiedades del certificado.

4.5.2 EXPORTAR UN CERTIFICADO

Los interlocutores externos necesitan la clave pública de los interlocutores propios para poder encriptar sus mensajes. Una vez importado el certificado del usuario propio, podemos exportar su clave pública siguiendo este proceso:

1. Se realiza doble clic sobre el certificado a exportar.

2. Se visualiza la pantalla de propiedades del certificado. En la parte inferior de la pantalla está el botón **Exportar Certificado** que permite la exportación del certificado en cuestión.
3. Seleccionar el nombre y ubicación del fichero con la clave pública.

Si por alguna razón se necesita el fichero del certificado de un interlocutor externo, también se puede exportar de la misma forma.

4.5.3 GENERAR UN AUTOCERTIFICADO

El EAS permite generar certificados autofirmados (self-signed). Un certificado autofirmado no está validado por ninguna entidad certificadora (Certifying Authority: CA) por lo que puede ser que los interlocutores no confíen en él. Sin embargo puede ser útil para realizar pruebas sin asumir el coste de comprar un certificado a una entidad certificadora.

Los certificados que genera el EAS incluyen todos una clave privada válida para cifrar/firmar mensajes y para asegurar conexiones SSL con otros servidores. Se puede usar el mismo certificado para el servidor y para un usuario propio.

Si posteriormente se decide adquirir un certificado de una entidad certificadora es conveniente asegurarse que el certificado es válido para las funciones antes comentadas. Si los interlocutores externos confiaran en nuestro certificado autogenerado, no sería necesario comprar un nuevo certificado a una entidad certificadora.

Para generar un certificado se deben completar una serie de pasos: Se realiza clic con el botón derecho del ratón.

1. Se selecciona la opción Generar autocertificado tal y como indica la imagen. Una vez pulsado, se visualizarán una serie de pantallas donde se procederá a indicar los datos solicitados (Descripción del certificado, Provincia, Ciudad, Localidad, Empresa y e-mail).

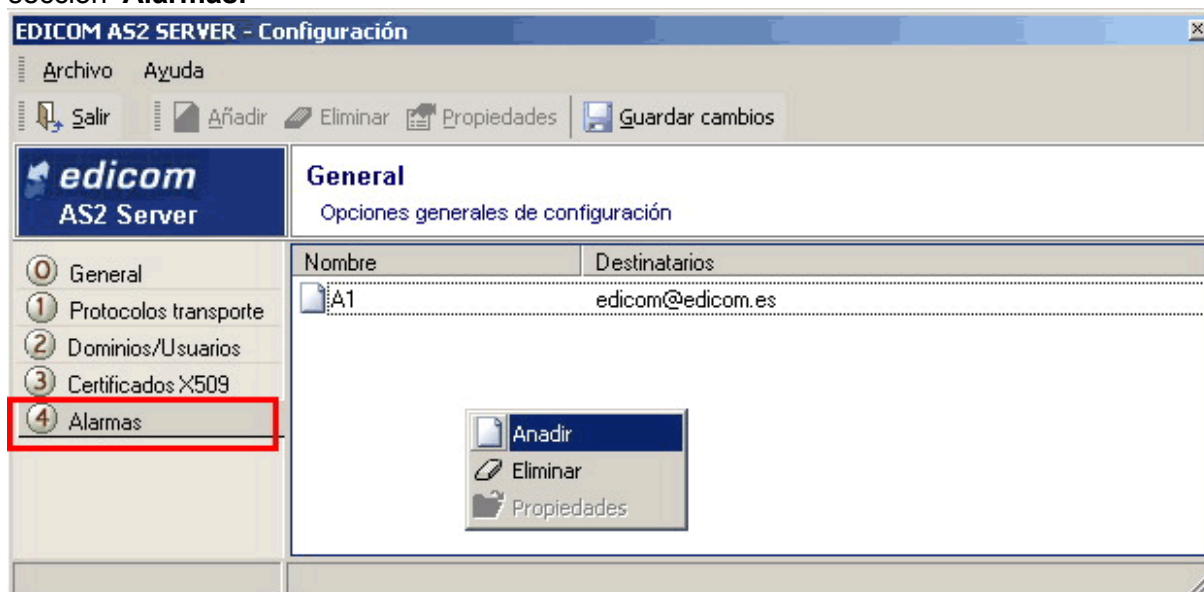
Importante: Cualquier certificado generado de esta forma se gestionará bajo su responsabilidad. Edicom no se hace responsable del uso que se le dé a los certificados autogenerados con el EAS.

4.6 Alarmas

4.6.1 INTRODUCCIÓN

Importante: Para el correcto funcionamiento de las alarmas se debe indicar en la pantalla de "Configuración-General" del EDICOM AS2 Server un servidor DNS.

El **EDICOM AS2 Server** dispone de una gestión de alarmas que permite enviar por email un mensaje a los administradores del EAS cuando se detecta algún problema en el servidor (fallo al inicializar un servicio, problemas al enviar/recibir un mensaje, no recepción de un MDN etc). Se puede acceder a la gestión de alarmas del **EDICOM AS2 Server** desde la sección **Alarmas**.



El menú contextual de la pantalla tiene las siguientes opciones:

Añadir. Permite añadir una alarma y configurar su parametrización inicial.

Eliminar. Permite eliminar la alarma seleccionada.

Propiedades. Permite modificar la parametrización de la alarma seleccionada.

4.6.2 GESTIÓN DE ALARMAS

Añadir alarmas

Para añadir una nueva alarma, desde:

- Menú contextual: opción **Añadir**.

A continuación se muestra la pantalla de *datos de la alarma*.

Los campos que se deben rellenar son los siguientes: **Destinatarios**. Permite indicar el o los destinatario del mensaje. Si se quiere indicar varios destinatarios se deben separar sus direcciones de e-mail con punto y coma.

- **Asunto**. Permite indicar el texto inicial del asunto del correo recibido. Los correos emitidos por esta alarma comenzarán siempre por este Asunto.
- **Notificar alarmas del tipo**. Permite indicar la contingencia o contingencias que harán saltar la alarma configurada. **Comunicaciones, Mensajes, Sistema y Control**. Para más información ver Contingencias

Eliminar alarmas

Para eliminar una alarma basta seleccionarla y desde: Menú contextual: Opción **Eliminar**.

Editar propiedades

Una vez creada una alarma pueden editarse sus propiedades, Seleccionándola y desde:

- Menú contextual: Opción **Propiedades**
- o doble clic sobre la alarma.

A continuación se volverá a mostrar la pantalla de propiedades de la alarma.

4.6.3 CONTINGENCIAS

El **EAS** informa de las siguientes contingencias: Alarmas notificando problemas en la inicialización de los servicios.

Este tipo de alarmas indican cualquier tipo de problema, al inicializarse cualquier servicio del **EDICOM AS2 Server**. Indica que no se podrán recibir/enviar problemas por ese servicio. Ejemplo:

```
EAS: Problemas en la inicialización del servidor

El servicio HTTP no se ha podido inicializar
El servicio HTTPS no se ha podido inicializar
El servicio SMTP no se ha podido inicializar
```

Alarmas notificando problemas en un mensaje saliente

Este tipo de alarma indica cualquier tipo de problema ocurrido ante el envío de un mensaje. En el mail siempre se indica el identificador del mensaje (0040323171133702) que presenta el problema por si se quiere revisar mediante el Edicom AS2 Viewer. Ejemplo:

```
EAS: Problemas en el mensaje saliente 0040323171133702
PARSER(23/03/2004 17:58:43) : El certificado recibido no coincide con el configurado
par el usuario <ZZedicom> en el dominio <edicom_test>.
PARSER(23/03/2004 17:58:43) : El MIC del MDN no coincide con el del MENSAJE
CONTROL(23/03/2004 17:58:43) : Mensaje rechazado.
PARSER(23/03/2004 17:58:43) : Negative MDN received: Error: Decryption-Failed
```


Alarmas notificando problemas en un mensaje entrante

Este tipo de alarma indica cualquier tipo de problema ocurrido ante la recepción de un mensaje. En el mail siempre se indica el identificador del mensaje que presenta el problema (I040323175843077) por si se quiere revisar mediante el **EDICOM AS2 Viewer**. Ejemplo:

```
EAS: Problemas en el mensaje entrante I040323175843077
PARSER(23/03/2004 17:58:43) : Error: Decryption-Failed ---> 197: Could not locate a
suitable decryption certificate
EAS: Problemas en el mensaje entrante I040914130146817
Origen del mensaje : Proveedor1
Destino del mensaje :5400110999990
PARSER(08/09/2004 17:55:08) : Unauthorized sender user: Proveedor1
```

En este último caso la alarma indica que hemos recibido un mensaje de un interlocutor externo que no está dado de alta en nuestro servidor AS2.

Mensajes recibidos para un interlocutor propio por un protocolo no permitido

En los mensajes entrantes, si el usuario tiene restringido un protocolo de transporte y recibe mensajes por este protocolo, se enviará una alarma como la siguiente:

```
EAS: Problemas en el mensaje entrante I040325105005421
PARSER(25/03/2004 10:50:05) : Se ha recibido un mensaje para el usuario <ZZedicom>
por un protocolo no permitido. Protocolo= HTTP
```

Se puede consultar el mensaje recibido en la carpeta Sistema del servidor. En la alarma siempre se informa del identificador del mensaje que presenta el problema (I04032510500542).

Control del certificado asociado al mensaje.

Esta alarma se ejecuta cuando el certificado asociado al mensaje no corresponde con el que tiene cargado el interlocutor.

```
EAS_LOCAL: Problemas en el mensaje entrante I050422155911747
Origen del mensaje : 0001
Destino del mensaje :0002

PARSER(22/04/2005 15:59:11) : Numero de serie del certificado
recibido: 021E2F2A
PARSER(22/04/2005 15:59:11) : Emisor del certificado recibido:
C=ES, S=Valencia, L=Paterna, O=EDICOM, CN=Edicom EAS Server,
E=edicom@eas.sedeb2b.com
PARSER(22/04/2005 15:59:11) : Error: Authentication-Failed --->
El servidor ha recibido un mensaje del usuario <0001> que ha
sido firmado con un certificado diferente al que tiene
configurado
```

Control de validación de usuario

Esta alarma se ejecuta cuando el usuario que ha enviado el mensaje, no es un usuario válido. Ejemplo de alarma:

```
EAS_LOCAL: Problemas en el mensaje saliente 0050425152114778
Origen del mensaje : 0001
Destino del mensaje :0002

CONTROL(25/04/2005 15:22:20) : Mensaje rechazado.
PARSER(25/04/2005 15:22:20) : El destinatario ha rechazado
nuestro mensaje. Causa: Error: Authentication-Failed
```

Control del certificado del servidor remoto para el establecimiento de una conexión SSL

Cuando se realiza la conexión SSL con un servidor de AS2 desde nuestro servidor se realiza una autenticación, para validar que el certificado cargado en el interlocutor externo con el que se va a iniciar la transacción, coincide con el certificado del servidor de AS2 remoto. Si coincide se realizará la transacción, y en caso de no coincidir se generará una alarma como la siguiente:

```
EAS_LOCAL: Problemas en el mensaje saliente 0050413114924363
Origen del mensaje : 0001
Destino del mensaje :0002

TRANSPORT(14/04/2005 12:12:38) : El certificado del servidor
remoto no coincide con el configurado.
TRANSPORT(14/04/2005 12:12:38) : Emisor del certificado
remoto:
/C=ES/ST=Valencia/L=Paterna/O=EDICOM/CN=Edicom_Interop_2005/Email=edicom_as2_interop_2005@edicom.es
TRANSPORT(14/04/2005 12:12:38) : Emisor del certificado
configurado: O=Cyclone One, CN=Terry Harding
TRANSPORT(14/04/2005 12:12:38) : Descripción del certificado
remoto:
/C=ES/ST=Valencia/L=Paterna/O=EDICOM/CN=Edicom_Interop_2005/Email=edicom_as2_interop_2005@edicom.es
TRANSPORT(14/04/2005 12:12:38) : Descripción del certificado
configurado: O=Cyclone One, CN=Terry Harding
TRANSPORT(14/04/2005 12:12:42) : El servidor remoto no ha
devuelto un código error. Posiblemente no se ha llegado a
conectar
TRANSPORT(14/04/2005 12:12:44) : Excepción en método
TAS2HttpClient.SendFile - Url=https://192.168.0.97:9214
TRANSPORT(14/04/2005 12:12:44) : InfoError=Error connecting with
SSL.
CONTROL(14/04/2005 12:12:44) : Mensaje rechazado
```



CAPITULO 5. EDICOM AS2 BATCH

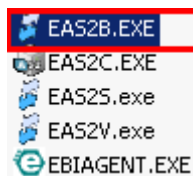
5.1 Introducción

Explicación de los comandos en modo batch para:

- Envío y recepción de mensajes.
- Creación, Edición o Eliminación de usuarios.
- Importación y eliminación de certificados.

Importante: EDICOM dispone de una herramienta para planificar el lanzamiento de los procesos Batch a determinadas horas. Si considera que esta herramienta puede ser útil para usted, póngase en contacto con nuestro departamento comercial.

5.2 Comandos Básicos envío y recepción.



El **Edicom AS2 Batch (EAS2B.exe)** es una herramienta que permite configurar y lanzar los procesos necesarios para el envío/recepción de mensajes desde el sistema interno de gestión. Para invocar el comando batch se dispone de una serie de comandos y parámetros que se explican en este apartado:

5.2.1 SINTAXIS

```
EAS2B -s <EAS2Server> -u <User> -pass <Pass>
      [-p <Port>] [-sec] [-safeTerminated <0|1>] [-timeout <Timeout>] [-help]
      -send -mo <MascOrig> -to <DirTo> [-tp <TanspProt>]
          [-url <URL>]
          [-MsgSign] [-MsgEnc] [-MsgComp] [-Msg0]
          [-Mdn] [-MdnSign] [-MdnA <AsyncProt> <AsyncPort>] [-Mdn0]
          [-sub <Subject>]
          [-contentEDI <content>] [-DEL | -REN]
      -receive -dd <DirDest> [-DirExt | -PrefExt] [-OriFile] [-noConfirm ]
      -manageFile -file <DataFile>
```

5.2.2 PARÁMETROS BÁSICOS

- **-s <EAS2Server>** es el nombre o dirección IP del servidor EAS.
- **-u <User>** y **-pass <Pass>** son el usuario y password para acceder al servidor EAS.
- **-p <Port>** indica el puerto remoto al que debe conectarse el Batch (9015 por defecto)
- **-sec** establece una conexión segura (HTTPS) con el servidor. Indica que se cifre la información que se intercambia entre el **EAS2B** y el servidor (opción no disponible en esta versión del producto).

- **-safeTerminated** indica que si la aplicación que ha lanzado el **EAS2B** se finaliza debe abortarse también el proceso **EAS2B**. Por defecto esta activado (1) para desactivarlo indicar 0.
- **-timeout.** indica el tiempo máximo de funcionamiento del EAS2B en minutos. Por defecto su valor son 30 minutos. Si lo indicamos 0 la duración es ilimitada.
- **-help** muestra las opciones del programa por pantalla.

5.2.3 ENVIAR MENSAJES: -SEND

```
-send -mo <MascOrig> -to <DirTo> [-tp <TanspProt>]
      [-url <URL>]
      [-MsgSign] [-MsgEnc] [-MsgComp] [-Msg0]
      [-Mdn] [-MdnSign] [-MdnA <AsyncProt> <AsyncPort>] [-Mdn0]
      [-sub <Subject>]
      [-contentEDI <content>] [-DEL | -REN]
```

-send utiliza el servidor AS2 para enviar los mensajes indicados mediante los parámetros:

- **-mo <MascOrig>** es la mascara origen de los ficheros a enviar. Ej: *.edi
- **-to <DirTo>** es la dirección AS1/AS2 del destinatario del mensaje. Ej: Zzedicom
- **-tp <TanspProt>** indica el protocolo de envío: HTTP, HTTPS, SMTP, FTP.
- **-url <URL>** indica la URL a la que debe enviarse el mensaje. El protocolo de envío se especifica con el parámetro **-tp <TanspProt>** por lo que la <url> no debe incluir el prefijo http:// o https://

Nota. Para conectar, utilizar el usuario propio asociado a los mensajes

Cuando se envía un mensaje, se usa la configuración de mensajes y acuses de recibo que tiene establecida el interlocutor destino. Además, si se quiere añadir alguna característica no contemplada en la configuración por defecto, se pueden utilizar estos parámetros:

Parámetros de seguridad del mensaje (MSG)

- **-MsgSign.** Permite indicar que el mensaje debe enviarse firmado.
- **-MsgEnc.** Permite indicar que el mensaje debe enviarse encriptado.
- **-MsgComp.** Permite indicar que el mensaje debe enviarse comprimido.

Parámetros del acuse de recibo (MDN)

- **-Mdn.** Permite indicar que se solicita un acuse de recibo para cada mensaje enviado.
- **-MdnSign.** Permite indicar que se espera que el acuse vaya firmado.
- **-MdnA <AsyncProt> <AsyncPort>.** Permite indicar si el acuse es asíncrono, el protocolo y el puerto por el que se va a recibir.

- **<AsyncProt>**. Permite indicar el protocolo de recepción de la notificación asíncrona, hay dos posibles valores: HTTP o HTTPS. Ej: -MdnA HTTPS
- **<AsyncPort>**. Permite indicar el puerto por que se quiere recibir el acuse de recibo asíncrono. El puerto por defecto es el puerto externo que se indica en la pestaña de protocolos.

Anular configuración por defecto

Los parámetros anteriormente indicados permiten **añadir** características a la configuración por defecto. Si se quiere que la configuración por defecto **no se aplique**, se debe indicar mediante los siguientes parámetros:

- **-Msg0**. Indica que no se quiere hacer uso de la configuración por defecto del mensaje para el usuario externo.
- **-Mdn0**. Indica que no se quiere hacer uso de la configuración por defecto del acuse de recibo para el usuario externo.

Una vez indicado que no se quiere usar la configuración por defecto, se puede indicar con los parámetros antes indicados la configuración del mensaje a enviar (-MsgSign, -MdnSign, etc)

Parámetros de gestión de ficheros y directorios al enviar

Por último, comentar dos parámetros que afectan a la gestión de ficheros/directorios: [-sub <Subject>]

[-contentEDI <content>] [-DEL | -REN]

- **-sub <Subject>**. Permite indicar el asunto del mensaje
- **-contentEDI <content>** Permite especificar un content-type específico para el mensaje EDI intercambiado.
- **-REN**. Fuerza a que se renombre el fichero una vez enviado. Se le concatena el identificador de mensaje a la extensión del fichero original. Esto permite detectar que el fichero se ha enviado y además relacionarlo con el identificador de mensaje que se le ha asignado en el servidor.
- **-DEL**. Borra el fichero original al enviarse al Servidor.

5.2.4 RECIBIR MENSAJES: -RECEIVE

```
-receive -dd <DirDest> [-DirExt | -PrefExt] [-OriFile] [-noConfirm ]
```

-Receive descarga los mensajes recibidos en el servidor a un directorio local. Los mensajes ya están en el servidor AS2, simplemente se mueven a una ubicación para que el sistema de gestión interno pueda trabajar con ellos. Para ello se utilizan los parámetros:

- **-dd <DirDest>**. Permite indica el directorio destino donde se guardarán los ficheros.
- **-DirExt**. Permite crea un subdirectorio para cada usuario externo.

- **-PrefExt.** Permite añadir como prefijo al nombre del fichero el usuario externo. Esta opción es incompatible con la opción **-DirExt**. Se debe elegir entre una de las dos.
- **-OriFile.** Permite guardar el fichero recibido con su nombre original.
- **-noConfirm.** Recibe los mensajes sin cambiar su estado a tratados

Nota. Para conectar, utilizar el usuario propio asociado a los mensajes

5.2.5 PROCESO DE FICHEROS: -MANAGEFILE

-ManageFile permite indicar un fichero con registros a procesar, con funciones para la gestión de Usuarios y Certificados.

```
-manageFile -file <DataFile>
```

- **-file <DataFile>.** Permite indicar el nombre del fichero con registros a procesar. Se pueden indicar varios registros con funciones diferentes por fichero.

Nota. Para conectar, utilizar el usuario propio asociado a los mensajes

5.2.6 EJEMPLOS:

A. Enviar mensajes <-send>:

```
EAS2B -s 192.168.0.52 -u ZZUserOwn -pass 9999999999999999 -send
-mo C:\AS2\TEST_DATA\*. * -to DDedicom -tp HTTP -MsgSign -MsgEnc
-MsgComp -Mdn -MdnSign -MdnA HTTPS 9932
```

B. Recibir mensajes <-receive>:

```
EAS2B -s 192.168.0.52 -u ZZUserOwn -pass 9999999999999999
-receive -dd C:\AS2\TEST_DATA\Receive\ -DirExt
```

C. Gestionar usuarios/certificados <-manageFile>

```
EAS2B -s 192.168.0.52 -u DDWebServiceUser -pass 8888888888888888
-manageFile -file C:\AS2\TEST_DATA\Receive\UsersData.txt
```

5.3 Funciones de usuarios

Para la ejecución de las funciones, se debe indicar el registro en un fichero, el EAS2B, se encarga de la ejecución de la función indicada en cada registro contenido en el fichero. Se pueden indicar varios registros con funciones diferentes por fichero.

Ejemplo:

```
EAS2B -s 192.168.0.52 -u DDWebServiceUser -pass 8888888888888888
-manageFile -file C:\AS2\TEST_DATA\Receive\UsersData.txt
```

Donde los parámetros indican lo siguiente: **-s**. Indica la IP del servidor

- **-p**. Indica el puerto del servidor.
- **-u**. Indica el código/nombre del administrador (EAS).
- **-pass**. Indica la contraseña del administrador.
- **-manageFile**. Especifica la ruta del fichero a ejecutar.

Los datos de usuario (**-u**) y contraseña (**-pass**) son los que se indican para acceder al **EDICOM AS2 Viewer**.

5.3.1 CREAR, EDITAR O MODIFICAR USUARIOS

Explicación de los comandos en modo batch para realizar la creación, edición o eliminación de usuarios.

Importante: Para cualquier duda sobre el significado de los parámetros utilizados en las funciones consulte los apartados: Dominios/Usuarios y Certificados X509

Los comandos disponibles son los siguientes:

A. Alta usuario propio

Estructura del registro:

```
function~domain~own~user~description~certificate~passCertificate~userAuth
entication~passAuthentication~testMode~allowHTTP~allowHTTPS~allowSMTP~dia
sHistorico~numRetrysInm~numResend~resendInterval~horasWaitingAsyncMDN~ala
rmasOff
```

Ejemplo:

```
1~test~1~prueba~TestImportacion~C:\EAS\CERTS\Cert.PFX~pwdCert~us
uario~pwdUsuario~1~1~~1~22~5~4~120~600~0
```

B. Alta usuario externo

Estructura del registro:

```
function~domain~own~user~description~certificate~certaux~userauthenticati
on~passauthentication~userRemote~passRemote~certRemote~urlRemote~urlsRemo
te~emailRemote~transportProtocol~encrypt~sign~compress~requestMDN~mdnSign
~mdnAsinc~mdnTransport~mdnAsyncPort
```

Ejemplo:

```
1~test~0~prueba_ext~Usuario externo de
prueba~C:\EAS\CERTS\COVAST.CER~C:\EAS\CERTS\EDS.CER~ext_auth~pas
s_ext~userremote_ext~pw_remote_ex~C:\EAS\CERTS\CECID.CER~url.rem
ote~ssl.url.remote~email@remote~http~1~0~1~1~1~0~https~9999
```

C. Borrado de usuario

Estructura del registro:


```
function~domain~own~user
```

Ejemplo:

```
2~test~1~prueba
```

Modificación de datos de un usuario.

Ediwin AS2 Batch no puede modificar los parámetros de un usuario ya creado. Para modificar un usuario desde Ediwin AS2 Batch, se debe primero realizar el **borrado** del usuario y a continuación darlo de nuevo de **alta** con los nuevos datos de configuración.

5.3.2 PARÁMETROS ESPECÍFICOS DE LOS COMANDOS DE USUARIO

- **function.** Indica el comando a ejecutar. 1: Alta de usuario, 2: Baja de usuario.
- **domain.** Indica el nombre del dominio.
- **own.** Indica si se trata de un usuario propio o externo: 0: Falso, 1: Cierto
- **user.** Indica el nombre del usuario
- **description.** Indica la descripción del usuario

5.3.3 PARÁMETROS ESPECÍFICOS DE LOS COMANDOS DE USUARIO PROPIO

Parámetros de configuración del certificado

- **certificate.** Indica la ruta al fichero del certificado con clave privada. Se debe indicar la ruta completa al certificado, y el nombre del fichero.
- **passCertificate.** Indica la contraseña del certificado con clave privada.

Parámetros de datos de autenticación

- **userAuthentication.** Indica el código de usuario.
- **passAuthentication.** Indica la contraseña del usuario.

Parámetros de conexiones de entrada

- **testMode.** Indica si el usuario se crea en un entorno de test. 0: Falso (No en modo test) 1: Cierto (En modo test).
- **allowHTTP.** Indica si permite conexiones de entrada HTTP. 0: Desactivado 1: Activado
- **allowHTTPS.** Indica si permite conexiones de entrada HTTPS. 0: Desactivado 1: Activado
- **allowSMTP.** Indica si permite conexiones de entrada SMTP. 0: Desactivado, 1: Activado

Parámetros de configuración de mensajes

- **diasHistorico.** Indica los días que se almacenan los mensajes en el histórico.
- **numRetrysInm.** Indica el número de reintentos de envío inmediato.
- **numResend.** Indica el número máximo de reenvíos.
- **resendInterval.** Indica el intervalo de tiempo en minutos entre cada reenvío.
- **horasWaitingAsyncMDN.** Indica el número de horas de espera del acuse del intercambio.
- **alarmasOff.** Indica si se activan las alarmas para el nuevo usuario. 0: Desactivado
1: Activado

5.3.4 PARÁMETROS ESPECÍFICOS DE LOS COMANDOS DE USUARIO EXTERNO

Parámetros datos generales:

- **certificate.** Indica la ruta al fichero del certificado. Se debe indicar la ruta completa al certificado, y el nombre del fichero.
- **certaux.** Indica la ruta al fichero del certificado auxiliar. Se debe indicar la ruta completa al certificado, y el nombre del fichero.

Parámetros de configuración de datos de autenticación

- **userauthentication.** Indica el código/nombre del usuario local.
- **passauthentication.** Indica la contraseña del usuario local.
- **userRemote.** Indica el código/nombre del usuario remoto.
- **passRemote.** Indica la contraseña del usuario remoto.
- **certRemote.** Indica la ruta al fichero del certificado para el usuario remoto. Sólo para conexiones HTTPS. Se debe indicar la ruta completa al certificado, y el nombre del fichero.

Parámetros de configuración de datos transporte

- **urlRemote.** Indica la URL para el protocolo HTTP.
- **urlsRemote.** Indica la URL para el protocolo HTTPS.
- **emailRemote.** Indica la cuenta de correo para el protocolo SMTP.

Nota: Para los parámetros *UrlRemote*, *urlsRemote* o *emailRemote* no es necesario indicar delante "Http://" o "Https://".

Parámetros de configuración del mensaje

- **transportProtocol**. Indica el protocolo de transporte del mensaje. Sólo se pueden indicar los siguientes valores: HTTP, HTTPS, SMTP
- **encrypt**. Indica si el intercambio se envía encriptado. 0: Desactivado, 1: Activado
- **sign**. Indica si el intercambio se envía cifrado. 0: Desactivado, 1: Activado
- **compress**. Indica si el intercambio se envía comprimido. 0: Desactivado, 1: Activado
- **requestMDN**. Indica si se solicita el envío de acuse de recibo. 0: Desactivado, 1: Activado
- **mdnSign**. Indica si el acuse debe ir firmado. 0: Desactivado 1: Activado
- **mdnAsinc**. Indica si el acuse se debe enviar en una conexión asíncrona. 0: Desactivado 1: Activado
- **mdnTransport**. Indica el protocolo de transporte del acuse. Sólo se pueden indicar los siguientes valores: HTTP, HTTPS.
- **mdnAsyncPort**. Permite indicar el puerto por que se quiere recibir el mdn (Acuse) asíncrono que envía el destinatario. Si no se indica ningún valor se utiliza el puerto por defecto asociado al protocolo indicado en mdnTransport

Nota: El puerto por defecto es el puerto externo que se indica en la pestaña de protocolos.

5.4 Funciones de certificados.

Explicación de los comandos en modo batch para realizar la importación y eliminación de certificados.

Importante: Para cualquier duda sobre el significado de los parámetros utilizados en las funciones consulte el capítulo de [Configuración del Servidor](#)

5.4.1 A. IMPORTACIÓN DE UN CERTIFICADO

Estructura del registro:

```
function~certificate~passCertificate
```

Ejemplo:

```
3~C:\EAS\CERTS\GIGANTE.PFX~12345
```

5.4.2 B. ELIMINACIÓN DE UN CERTIFICADO

Estructura del registro:

```
function~NumSerieCert
```

Ejemplo:

4~5f55219

5.4.3 EXPLICACIÓN DE LOS PARÁMETROS DE LOS COMANDOS:

- **function.** Indica el comando a ejecutar. 3: Importar certificado, 4: Eliminar certificado.
- **certificate.** Indica la ruta al fichero del certificado. Se debe indicar la ruta completa al certificado, y el nombre del fichero.
- **passCertificate.** Indica la contraseña del certificado. Sólo es necesario si el certificado tiene clave privada.
- **numSerieCert.** Indica el número de serie del certificado que se debe eliminar.

5.5 Comentarios adicionales

Se deben tener en cuenta los siguientes puntos. Los campos de los registros vienen separados por ~, si en algún momento hay que indicar dentro de un campo ese carácter, debe escribirse &ESCAPE; Ejemplo: para una descripción de usuario: Usuario&ESCAPE;avanzado, sería la descripción de usuario "**Usuario~avanzado**". Si no se indica una ruta al certificado asociado a un usuario, la aplicación escribe un *warning* pero permite importar el usuario, solo que no se le asigna ningún certificado al nuevo usuario.

- La aplicación indica si el *warning* corresponde con un problema al importar el certificado propio, el certificado de un usuario externo (Principal o auxiliar) o certificado para la conexión SSL del usuario remoto. El *warning* también indica la razón del error: no se ha encontrado el fichero o no se ha especificado la ruta del certificado.
- Si al crear un usuario, se indica una ruta a un certificado que ya está importado (es decir mismo número de serie y emisor), el certificado no se importa nuevamente y se asigna al usuario el certificado ya importado.

CAPITULO 6. ENVÍO Y RECEPCIÓN DE MENSAJES

6.1 introducción

El envío/recepción de mensajes se puede llevar a cabo de dos formas:

- De forma **interactiva** desde la aplicación **EDICOM AS2 Viewer**. A través de las opciones del menú de esta aplicación.
- De modo **desasistido o batch** utilizando el **EDICOM AS2 Batch**.

6.2 Envío de mensajes de modo interactivo.

Para realizar el envío de mensajes desde la aplicación **EDICOM AS2 Viewer** se procede de la siguiente manera:

- **Paso 1-** Se pulsa la opción del menú **Crear**.
- **Paso 2-** A continuación se abrirá un cuadro de dialogo desde donde se seleccionará el fichero a enviar al interlocutor.
- **Paso 3-** Una vez seleccionado se visualizará la siguiente pantalla:

EDICOM AS2 SERVER - Propiedades: 0040212191411264_EDICOM@192.168.0.79

edicom AS2 Server

Propiedades
Disponemos de propiedades de control, del mensaje EDI, del mensaje AS1/AS2 y del Acuse MDN. Adicionalmente se puede visualizar el contenido de cada uno de los ficheros mencionados.

Propiedades de control

Situación:

Sentido:

Identificador:

Fecha de creación:

Fecha de transmisión:

Fecha de transmisión MDN:

Mensaje

Origen:

Destino:

Asunto:

Firmado ☐ Encriptado ☐ Comprimido ☐

Protocolo de transporte:

Url:

Fichero EDI

Nombre:

Tipo:

Acuse MDN

Solicitar acuse ☐ Firmado ☐

Acuse asíncrono ☐

Tipo envío asíncrono:

Tipo MIC:

Fichero EDI | Mensaje AS1/AS2 | Acuse MDN

UNA:~?~UNB+UNQA:1+ZZedicom:ZZ+TESTER2:ZZ+961007:2013+000000003+AAA:AA+1A+1++123456789+1~UNH+000050001+ORDERS:000:948:UN+23X232323232EC+1:C'BGM+105:161:136:PURCHASE ORDER+1A+9+NA'DTM+11:071096:2'PAJ+2:44:11:107:11:5'ALI+UK+8+21+22+111MD+8+3+123-ABC:35'LIN+1+18+1:CV:110:108+1+67+'LIN+2+18+1:CV:110:108+1+67+'LIN+3+18+1:CV:110:108+1+67+'LIN+4+18+1:CV:110:108+1+67+'LIN+5+18+1:CV:110:108+1+67+'LIN+6+18+1:CV:110:108+1+67+'LIN+7+18+1:CV:110:108+1+67+'LIN+8+18+1:CV:110:108+1+67+'LIN+9+18+1:CV:110:108+1+67+'LIN+10+18+1:CV:110:108+1+67+'LIN+11+18+1:CV:110:108+1+67+'LIN+12+18+1:CV:110:108+1+67+'LIN+13+18+1:CV:110:108+1+67+'LIN+14+18+1:CV:110:108+1+67+'LIN+15+18+1:CV:110:108+1+67+'LIN+16+18+1:CV:110:108+1+67+'LIN+17+18+1:CV:110:108+1+67+'LIN+18+18+1:CV:110:108+1+67+'LIN+19+18+1:CV:110:108+1+67+'LIN+20+18+1:CV:110:108+1+67+'LIN+21+18+1:CV:110:108+1+67+'LIN+22+18+1:CV:110:108+1+67+'LIN+23+18+1:CV:110:108+1+67+'LIN+24+18+1:CV:110:108+1+67+'LIN+25+18+1:CV:110:108+1+67+'PIA+2+123-EFG:CV:190:104'MEA+AAJ+CHN:7:8:JHJHGJG+THG:2323.90:1122:767756+RR'QTY+164:4243234242:232'ALI+JA+8+20'UNS+S'MQA+109:23321:UK:6:2'UNT+38+000050001'UNZ+1+000000003'














- **Paso 4.-** Se indica en el campo **Destino**, el interlocutor al que va destinado el mensaje.
 - Si para el interlocutor al que se le envía el mensaje, se han configurado las opciones de configuración por defecto del mensaje, estas opciones se activarán de forma automática. Para más información sobre configuración de un mensaje por defecto ver [Configuración del Mensaje \(por defecto\)](#)
 - Si no se han configurado estos parámetros, se deberán indicar de forma manual el resto de campos, según los requisitos que haya establecido el interlocutor externo.
- **Paso 5.-** Cuando se haya terminado de indicar los parámetros, se pulsará el botón Aceptar para proceder a su envío.

6.2.1 REENVÍO DE MENSAJES

Para cada interlocutor propio se puede configurar las opciones de reenvío de mensajes de forma automática. Para más información pulse aquí.

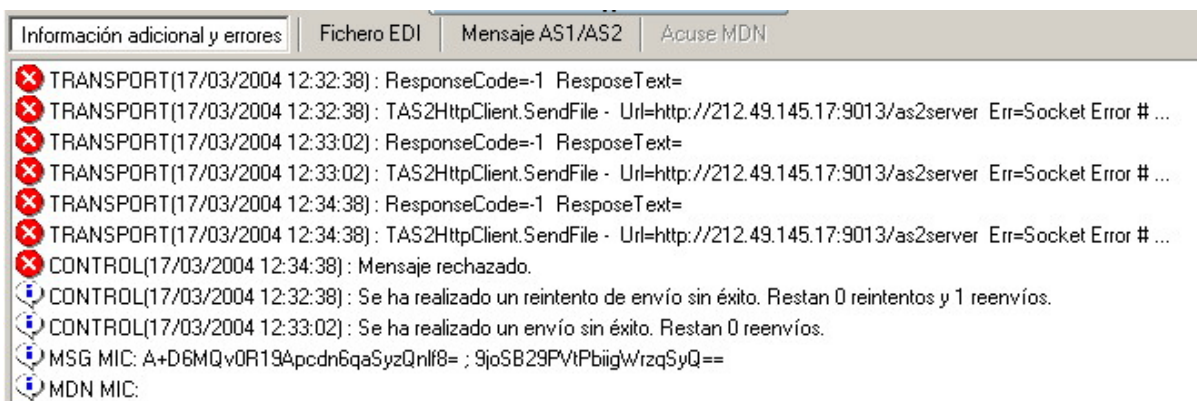
Si las opciones de reenvío de mensajes para el interlocutor propio seleccionado están configuradas, se puede dar la siguiente situación:

- **Paso 1.-** El mensaje no se ha podido enviar en primera instancia, con lo que se realizan varios reintentos de envío de forma inmediata, según la configuración establecida. Si tras estos reintentos inmediatos no se ha podido enviar el mensaje, se quedará en situación Depositado (DEP).

Fichero de control	Situación	Fecha	Id. Externo	Protocolo			
 0040317123203309	 DEP	17/03/2004 12:32:03	ZZedicom	HTTP			 A/S
 0040317121924989	 RCH	17/03/2004 12:19:24	ZZedicom	HTTP			 SYNC
 0040213154102358	 RCH	13/02/2004 15:41:26	ZZedicom	HTTP			 SYNC

- **Paso 2.-** Se realizarán tantos reenvíos como tenga configurado el interlocutor, pasando a situación Rechazado (RCH) en caso de sobrepasar este número. El mensaje pasará a situación Enviado (ENV) si es enviado con éxito durante alguno de los reenvíos.

En la imagen siguiente se puede visualizar un log de conexión, donde el mensaje no se ha podido enviar en una primera conexión, pero se realizan reenvíos de forma automática hasta que finalmente el mensaje es rechazado.



Nota: Para saber como obtener información adicional de un mensaje, como por ejemplo los logs de conexiones, [Información adicional y errores](#)

6.3 Recepción de mensajes de modo interactivo.

La recepción desde el **EDICOM AS2 Viewer** es un proceso automático que actualizará los mensajes listados en el panel de control cada vez que se envíe o reciba un mensaje o acuse de recibo. El usuario no tiene que realizar ninguna acción para recibir los mensajes pero puede refrescar la información cuando lo desee.

6.4 Envío de mensajes desde línea de comandos

Para realizar el envío de mensajes desde la línea de comandos se procede de la siguiente manera:

- **Paso 1.-** Configurar correctamente el servidor de AS2 y el usuario externo receptor del mensaje.
- **Paso 2.-** Ejecutar por ejemplo un proceso Batch como el siguiente:

```
EAS2B -s 192.168.0.52 -u Zzedicom -pass 9999999999999999
      -send -mo C:\AS2_DATA\*. * -to Zzedicom -tp HTTP -MsgSign
      -MsgEnc -MsgComp -Mdn -MdnSign -MdnA HTTPS
```

- **Paso 3.-** Al finalizar el proceso, los mensajes estarán en situación Enviado **ENV** en el servidor de AS2, y pasarán al estado Recuperado **RCP** cuando se reciba el acuse de recibo correspondiente.

6.5 Recepción de mensajes desde línea de comandos

Para realizar la recepción de mensajes desde la línea de comandos se procede de la siguiente manera:

- **Paso 1.-** Crear por ejemplo un proceso como el siguiente:

```
EAS2B -s 192.168.0.52 -u Zzedicom -pass 9999999999999999
      -receive -dd C:\AS2_DATA\RECEIVED\ -DirExt
```

- **Paso 2.-** Al finalizar el proceso, los mensajes en situación Recibido REC sin errores pasarán a situación Tratado (TRA), Además el mensaje tratado pasará a la carpeta Histórico de mensajes. Los mensajes ya estaban en el servidor AS2, simplemente se mueven a una ubicación para que el sistema de gestión interno pueda trabajar con ellos y se cambia su estado para que quede reflejado en el servidor.

CAPITULO 7. INFORMACIÓN ADICIONAL DE UN MENSAJE

7.1 Introducción

Para obtener más información sobre un mensaje en concreto, basta con realizar doble clic sobre el mensaje seleccionado para ver sus propiedades:

The screenshot shows the 'Propiedades' window of the EDICOM AS2 SERVER. The window title is 'EDICOM AS2 SERVER - Propiedades: 0040211174716766_EDICOM_TEST@192.168.0.79 (Sol lectura)'. The window is divided into several sections:

- Propiedades de control:**
 - Situación: Recibido
 - Sentido: ENTRADA
 - Identificador: 0040211174716766_EDICOM_TEST@192.16
 - Fecha de creación: 11/02/2004 17:47:27
 - Fecha de transmisión: 11/02/2004 17:47:27
 - Fecha de transmisión MDN:
- Mensaje:**
 - Origen: Test
 - Destino: Edicom
 - Asunto: EDI message sent by EDICOM ASi SERVER
 - Firmado: ☒ Encriptado: ☒ Comprimido: ☒
 - Protocolo de transporte: HTTP
 - Url:
- Fichero EDI:**
 - Nombre: D2_edifact_edicom.edi
 - Tipo: EDI
- Acuse MDN:**
 - Solicitar acuse: ☒ Firmado: ☒
 - Acuse asíncrono: ☐
 - Tipo envío asíncrono:
 - Tipo MIC: SHA1

At the bottom, there are tabs for 'Información adicional y errores', 'Fichero EDI', 'Mensaje AS1/AS2', and 'Acuse MDN'. The 'Información adicional y errores' tab is active, showing a MIC value: 'nDbkr7W3WajQ6q6zoYydAhtg0hY='. A 'Salir' button is located at the bottom right.

Dentro de la pantalla se distinguen los siguientes apartados:

7.2 Propiedades de control

- **Situación.** Indica la situación del mensaje. Esta puede ser: Enviado, Recuperado, Rechazado, Recibido. Para más información sobre la situación de un mensaje pulse aquí.
- **Sentido.** Indica el sentido del mensaje (entrada/salida).
- **Identificador.** Indica el identificador del mensaje en el servidor
- **Fecha de creación.** Indica la fecha de creación del mensaje.
- **Fecha de transmisión.** Indica la fecha de envío del mensaje.
- **Fecha de transmisión de MDN.** Indica la fecha de envío/recepción del acuse de recibo.

7.2.1 FICHERO EDI

- **Nombre.** Indica el nombre original del fichero EDI que hemos enviado/recibido
- **Tipo.** Indica el tipo de formato del fichero EDI (XML, X12, Edifact).

7.2.2 MENSAJE

- **Origen.** Indica el interlocutor origen del mensaje.
- **Destino.** Indica el interlocutor destino del mensaje.
- **Asunto.** Indica el asunto del mensaje.
- **Firmado.** Indica si el mensaje está firmado.
- **Encriptado.** Indica si el mensaje está cifrado.
- **Comprimido.** Indica si el mensaje esta comprimido.
- **Protocolo de transporte.** Indica el protocolo de envío del mensaje (HTTP, HTTPS, SMTP).
- **URL.** Indica el servidor remoto de origen/destino del mensaje.

7.2.3 ACUSE MDN

- **Solicitar acuse.** Indica si se quiere solicitar acuse de recibo.
- **Firmado.** Indica si se quiere solicitar un acuse de recibo firmado.
- **Acuse asíncrono.** Indica si se quiere recibir el acuse de forma asíncrona.
- **Tipo de envío asíncrono.** Indica el tipo de transporte (HTTP, HTTPS, SMTP) para el envío del acuse.
- **Tipo de MIC.** Indica el algoritmo utilizado para generar el MIC del acuse.

7.2.4 INFORMACIÓN ADICIONAL Y ERRORES

Muestra información y logs referente al envío/recepción del mensaje. En esta ficha se puede visualizar si ha ocurrido algún tipo de error durante el transporte, envío o recepción del mensaje. También indica el historial de intentos de envío del mensaje, si ha sido reprocesado manualmente etc.

7.2.5 FICHERO EDI

Muestra el contenido del mensaje en el formato (XML, X12, Edifact) en el que ha sido enviado/recibido. Si el fichero es muy grande solo se visualiza una parte.

7.2.6 MENSAJE AS1/AS2

Muestra el mensaje en formato AS2/AS1 asociado al fichero a enviar.

7.2.7 Acuse MDN

Muestra el acuse de recibo del mensaje enviado/recibido.

CAPITULO 8. ANEXO: LOGS DE EDICOM AS2 SERVER

8.1 Introducción



En el directorio *LOGS* del directorio de instalación del EAS, se crean los logs del servidor.

- *EAS2S.LOG*. Es el log más importante del servidor. En él se reflejan todos los errores acaecidos durante su funcionamiento. Es el fichero que hay que monitorizar con más atención. También refleja cada vez que se ejecuta el paso a histórico de documentos.
- *EAS2A.LOG*. Este fichero es log del servicio windows que monitoriza al servidor **EAS**. Refleja las paradas e inicios del servidor. Cada vez que se para el servidor automáticamente, el servicio escribe en este log cuándo vuelve a iniciar el servidor. Si se para el servidor manualmente también se refleja. Es útil para revisar rápidamente las paradas y reinicios del servidor.
- *EAS2B.LOG*. Refleja las conexiones que realiza el **EDICOM AS2 Batch**.
- *EAS2_NEGOTIATION.LOG*. En este fichero se reflejan todas las comunicaciones HTTP/HTTPS que realiza el servidor **EAS**. No es necesario revisarlo a menos que se quiera comprobar un error concreto en la recepción o envío de un mensaje o saber si el servidor ha intercambiado mensajes en algún momento.
- *EAS2_ALARMS.LOG*. Refleja todas las alarmas que envía por mail el servidor **EAS** con el fin de que evitar que alguna se pierda por problemas con el correo. Cuando falla el envío de alguna alarma normalmente se refleja el error en el *EAS2S.LOG* con una excepción en el método `sendAlarm`. Si se quiere saber si alguna alarma falló, se puede recurrir a este log.
- *EAS2V.LOG*. este fichero es el log del **EDICOM AS2 Viewer**. Si se observa algún comportamiento anómalo en el Viewer o no se puede conectar, se puede comprobar si ha habido algún error en el cliente SOAP revisando este fichero.

CAPITULO 9. ANEXO: GUÍA RÁPIDA DE PUESTA EN MARCHA EAS.

Importante: Con el fin de poder empezar a intercambiar mensajes AS2 con el **EAS** fácilmente se ha definido una guía rápida de puesta en marcha. **Resaltar que esta configuración es la mínima que se debe realizar**, una vez se haya conseguido intercambiar mensajes con éxito se debe revisar todo el manual y ajustar la configuración del servidor a las necesidades del proyecto.

Si quiere realizar envíos entre usuarios de nuestro servidor (por ejemplo para probar el producto sin recurrir a otras empresas) es necesario crear además del dominio y los usuarios creados en la tabla anterior, otro dominio y otros usuarios que correspondan con los usuarios externos. Vamos a intercambiar mensajes entre usuarios de dos dominios diferentes.

Paso 1.- Configuración general de la aplicación.	
Acceder a la Configuración.	Para configurar el EAS se debe acceder a la pantalla de configuración desde EDICOM AS2 Viewer .
General	En la pantalla <i>General</i> indicar los siguientes datos: <ul style="list-style-type: none"> • Direcciones IP interna y externa. • Dirección IP del DNS.
Certificados	En la pantalla <i>Certificados</i> realizar la carga de los certificados del usuario propio y de los interlocutores externos. Realizar también la carga de un certificado para SSL. Si no se dispone de estos certificados, utilizar la herramienta de auto-generación de certificados que ofrece el servidor.
Protocolos Transporte	En la pantalla <i>Protocolos Transporte</i> indicar el certificado para conexiones SSL.
Dominios/Usuario	En la pantalla <i>Dominios/Usuario</i> crear el dominio.
Paso 2.- Configuración de dominio/usuario principal.	
Dominios	En la pantalla <i>Dominios/Usuario</i> crear el dominio.
Interlocutores	<ol style="list-style-type: none"> 1. Crear el interlocutor propio. <ol style="list-style-type: none"> 1. Indicar el nombre del interlocutor propio. (A) 2. Indicar el certificado en caso de enviar mensajes firmados. 2. Crear el interlocutor externo. <ol style="list-style-type: none"> 1. Indicar el nombre del interlocutor externo. (B) 2. Indicar el certificado en caso de enviar mensajes cifrados. 3. Indicar los datos de transporte (la dirección IP y el puerto del servidor) del interlocutor externo. 4. Indicar la configuración del mensaje por defecto.
Paso 3. Pruebas de envío entre dominios del mismo servidor.	
Dominios	En la pantalla <i>Dominios/Usuario</i> crear otro dominio de Prueba.
Interlocutores	<p>En este dominio de prueba crear un interlocutor propio cuyo identificador sea el interlocutor externo (B) que hemos definido en el punto 2. Su certificado también será el que se haya asignado en el punto 2 al interlocutor externo.</p> <p>También se debe crear un interlocutor externo cuyo identificador será el mismo que el del interlocutor propio (A) definido en el punto 2. Su certificado será el certificado asignado en el punto 2 al interlocutor propio.</p> <p>Los datos de transporte de este interlocutor externo serán: <IP del servidor:puerto_del_servicio> Ejemplo: si la IP publica del servidor es 212.48.147.10, y el servicio HTTP está configurado en el puerto 9013, la URL de este interlocutor sería http://212.48.147.10:9013</p> <p>Para poder realizar pruebas internas, se deben asignar los mismos datos de transporte al interlocutor externo del punto 2, ya que ambos interlocutores estarán en el mismo servidor.</p>

CAPITULO 10. ANEXO: ESTRUCTURA BASE DE DATOS EAS.

10.1 Introducción.

Las primeras versiones de **Edicom AS2 Server** almacenaban la información de configuración y los propios mensajes en una estructura de directorios y ficheros locales. Esto se ha sustituido por almacenamiento en base de datos. Este anexo lista las tablas y registros de las bases de datos. Haciendo referencia si es necesario a las diferencias mas notables entre EASv1 (Sobre ficheros) y EASv2 (Sobre BBDD).

10.2 Tablas EAS

Nombre	Descripción
EasCONFIG	Carga los datos de configuración básicos de servicio. Antes en EAS.DAT
EasDomains	Para almacenar dominios. Antes en EAS.DAT
EasAlarms	Para almacenar las alarmas. Antes en EAS.DAT
EasUsersOwn	Para almacenar usuarios propios. Antes en EAS_OWN.DBF
EasUsersExt	Para almacenar usuarios externos. Antes en EAS_EXT.DBF
EasCerts	Para almacenar certificados X509. Antes en EAS_CERT.DBF
EasMensajes	Para almacenar la información de los mensajes enviados/recibidos. Se guarda en BLOBS: El MSGAS2, el MDN, el MSGEDI, los ERRORES e INFORMACIONES.
EasLogs	Para almacenar los logs asociados a los mensajes.

10.2.1 EASCONFIG

Carga los datos de configuración básicos de servicio

ID	(ftInteger,0)	
DataDirectory	(ftString,255)	Obsoleto
LocalDirectory	(ftString,255) /	Dir local
LogSession	(ftboolean,0)	Log de movimiento de mensajes. Almacenar en DBF
TrazaDebug	(ftboolean,0)	Activa trazas al log de errores.
SERVERNAME	(ftString,255)	
SERVERIP	(ftString,255)	
DOMSMTP	(ftString,255)	
DNSSERVER	(ftString,255)	
SerialNumber	(ftString,255)	'EAS-V1-'+FormatDateTime('yymmdd (Now) + '-' +FormatFloat('000000 (Random(99999)) '); Creamos un nº de registro la primera vez.

LicenceNumber	(ftInteger,0)	Nº máximo de users OWNS: 0= UNREGISTERED 1000000=Ilimitados.
PASSKEYSOAP	(ftString,255)	Será el mismo FLicenceNumber encriptado. Lo pondremos en la sección SOAP como PASSKEY
USERSOAP	(ftString,255)	
PASSSOAP	(ftString,255)	
PORTSOAP	(ftInteger,0)	9015
PORTSOAPS	(ftInteger,0)	9016
URLHTTP	(ftString,255)	AS2SERVER
PortHTTP	(ftInteger,0)	4080
PortInterHTTP	(ftInteger,0)	4080
LogDebugHTTP	(ftboolean,0)	Log de movimiento de mensajes. Almacenar en DBF
DesactivarHTTP	(ftboolean,0)	Indica si debe haber un proceso escuchando para el protocolo HTTP
URLHTTPS	(ftString,255)	AS2SERVER
PortHTTPS	(ftInteger,0)	5443
PortInterHTTPS	(ftInteger,0)	5443
LogDebugHTTPS	(ftBoolean,0)	Log de movimiento de mensajes. Almacenar en DBF
DesactivarHTTPS	(ftBoolean,0)	Indica si debe haber un proceso escuchando para el protocolo HTTPS
CertHTTPS	(ftString,255)	
PortSMTP	(ftInteger,0)	25
LogDebugSMTP	(ftBoolean,0)	Log de movimiento de mensajes. Almacenar en DBF
DesactivarSMTP	(ftBoolean,0)	Indica si debe haber un proceso escuchando para el protocolo HTTP
ProxyServer	(ftString,255)	Atención: en la configuración antigua este parámetro está como 'ProxyServe' en lugar de 'ProxyServer'
ProxyPort	(ftInteger,0)	8080
ProxyUser	(ftString,255)	
ProxyPassword	(ftString,255)	
ProxyType	(ftString,255)	
MaxHoras	(ftInteger,0)	Por defecto no habilitado -1
MaxMem	(ftInteger,0)	
MinIntentando	(ftInteger,0)	1
MaxThreadsEnvio	(ftInteger,0)	16

AlarmServer	(ftString,255)	
AlarmFrom	(ftString,255)	
AlarmUser	(ftString,255)	
AlarmPW	(ftString,255)	
BoundPortMin	(ftInteger,0)	
BoundPortMax	(ftInteger,0)	
updated	(ftDateTime,0,FALSE)	Para marcarlo tras cada cambio realizado en la configuración.

10.2.2 EASDOMAINS

Almacenamiento de dominios

EASDOMAIN	(ftString,255)	
DELETED	(ftInteger,0)	
DescDom	(ftString,255)	
PassDom	(ftString,255)	
DirDom	(ftString,255)	Obsoleto
updated	(ftDateTime,0,FALSE)	Par marcarlo tras cada cambio realizado en la configuración.

10.2.3 EASALARMS

Almacenamiento de Alarmas

EASDOMAIN	(ftString,255)	
USEROWN	(ftString,255)	
NAME	(ftString,255)	
DELETED	(ftInteger,0)	
Subject	(ftString,255)	
Receivers	(ftString,255)	
Codes	(ftString,255)	(taComunicaciones,taMensaje,taSistema,taControl,taVarias); Su código es su ordinal, empezando por 0
updated	(ftDateTime,0,FALSE)	Par marcarlo tras cada cambio realizado en la configuración.

10.2.4 EASUSERSExt

Almacenamiento de usuarios Externos

AS2 Propios y externos		
EASDOMAIN	(ftString, 35)	
EASUSER	((ftString, 128)	
DELETED	(ftInteger, 0)	
DESCRIPTION	(ftString, 255)	
CERT	(ftString, 255)	
CERT2	(ftString, 255)	
ISSUER	(ftString, tamaño)	
ISSUER2	(ftString, tamaño)	
USERAUTHEN	(ftString, 70)	
PASSAUTHEN	(ftString, 50)	
AS2 Externos		
URLREMOTE	(ftString, 255)	URL completa. HTTP:\<server>:<puerto>\recurso
URLREMAUX	(ftString, 255)	
URLSREMOTE	(ftString, 255)	URL completa. HTTP:\<server>:<puerto>\recurso ó HTTPS:\<server>:<puertoS>\recurso DBFAux.FieldDefs.Add('PORTREMOTE (ftInteger, 0)
URLSREMAUX	(ftString, 255)	
EMLREMOTE	(ftString, 255)	
EMLREMAUX	(ftString, 255)	
EMLSREMOTE	(ftString, 255)	
EMLSREMAUX	(ftString, 255)	
FTPREMOTE	(ftString, 255)	
FTPREMAUX	(ftString, 255)	
FTPSREMOTE	(ftString, 255)	
FTPSREMAUX	(ftString, 255)	
USERREMOTE	(ftString, 255)	
PASSREMOTE	(ftString, 50)	
CERTREMOTE	(ftString, 255)	
IGNMIC	(ftBoolean, 0)	
DATOSAUX	(ftString, 255)	
DATOS DE CONTACTO 16/06/2009		

NAMECONT	(ftString, 255)
EMAILCONT	(ftString, 255)
LANGUAGECONT	(ftString, 2)
<i>AS2 Externos MSG DEFAULT</i>	
M_TRANPROT	(ftString, 10)
M_ENCRYPT	(ftBoolean, 0)
M_SIGN	(ftBoolean, 0)
M_COMPRESS	(ftBoolean, 0)
M_REQMDN	(ftBoolean, 0)
M_MDNSIGN	(ftBoolean, 0)
M_MDNASYNC	(ftBoolean, 0)
M_MDNASYNT	(ftString, 10)
M_MDNPORT	(ftString, 10)
updated	(ftDateTime, 0, FALS Par marcarlo tras cada cambio realizado en la configuración. E)

10.2.5 EASUsersOwn

Almacenamiento de usuarios propios

<i>AS2 Propios y externos</i>		
EASDOMAIN	(ftString, 35)	
EASUSER	(ftString, 128)	
DELETED	(ftInteger, 0)	
DESCRIPTION	(ftString, 255)	
CERT	(ftString, 255)	
CERT2	(ftString, 255)	
ISSUER	(ftString, tamaño)	
ISSUER2	(ftString, tamaño)	
USERAUTHEN	(ftString, 255)	
PASSAUTHEN	(ftString, 50)	
<i>PROPIOS</i>		

DELHISTDAY	(ftInteger, 0)	
RETRYSEND	(ftInteger, 0)	
MDNWAITHOURS	(ftInteger, 0)	
RESENDNUM	(ftInteger, 0)	
RESENDMINS	(ftInteger, 0)	
ALLOWHTTP	(ftBoolean, 0)	
ALLOWHTTPS	(ftBoolean, 0)	
ALLOWSMTP	(ftBoolean, 0)	
ALLOWSMTPS	(ftBoolean, 0)	
ALLOWFTP	(ftBoolean, 0)	
ALLOWFTPS	(ftBoolean, 0)	
AUTH_HTTP	(ftString, 30)	NONE, BASIC, CLIENT, SERVER, CLIENT/SERVER
AUTH_HTTPS	(ftString, 30)	NONE, BASIC, CLIENT, SERVER, CLIENT/SERVER
AUTH_SMTP	(ftString, 30)	NONE, BASIC, CLIENT, SERVER, CLIENT/SERVER
AUTH_SMTPS	(ftString, 30)	NONE, BASIC, CLIENT, SERVER, CLIENT/SERVER
AUTH_FTP	(ftString, 30)	NONE, BASIC, CLIENT, SERVER, CLIENT/SERVER
AUTH_FTPS	(ftString, 30)	NONE, BASIC, CLIENT, SERVER, CLIENT/SERVER
TEST	(ftBoolean, 0)	
ALARMASOFF	(ftBoolean, 0)	
Updated	(ftDateTime,0,FALSE)	Par marcarlo tras cada cambio realizado en la configuración.

10.2.6 EASCERTS

Almacenamiento de certificados.

<i>AS2 Propios y externos</i>		
EASDOMAIN	(ftString, 35)	
NUMSERIE	(ftString, 255)	
DELETED	(ftInteger, 0)	
DESCRIPCIO	(ftString, 255)	
VALDESDE	(ftDateTime,0)	
VALHASTA	(ftDateTime,0)	
SUBJECT	(ftString,tamanyo)	

ISSUER	(ftString,tamanyo)	
ISKEY	(ftboolean,0)	
TRUSTED	(ftboolean,0)	
PASSWRD	(ftString,50)	
FCERT	(ftBlob,0)	
FCPRI	(ftBlob,0)	
FP12	(ftBlob,0)	
Updated	(ftDateTime,0,FALSE)	Para marcarlo tras cada cambio realizado en la configuración.

10.2.7 EASMESSAGES

Almacenamiento de la información de los mensajes enviados/recibidos

Control		
EASDOMAIN	(ftString, 35)	
ID	(ftString, 32)	yymmddhhnnssxxx_rrrrr
USEROWN	(ftString,255)	
USEREXT	(ftString,255)	
Situation	(ftString, 10)	Estado del fichero de control: REC,TRA,DEP,RCH,ENV,RCP
State	(ftInteger, 0)	
MessageID	(ftString, 255)	
Direction	(ftString, 10)	
CreationTime	(ftDateTime, 0)	
TransTime	(ftDateTime, 0)	
TransMDNTime	(ftDateTime, 0)	
TEST	(ftBoolean, 0)	
BLOBS		
EDIData	(ftBlob, 0)	
AS2Data	(ftBlob, 0)	
MDNData	(ftBlob, 0)	
InformData	(ftBlob, 0)	
ErrorsData	(ftBlob, 0)	

Fichero EDI		
EDIFilename	(ftString, 255)	
EDIType	(ftString, 32)	Tres posibilidades: 'EDI 'X12 'XML'
<i>Fichero AS2/AS1</i>		
TransportProtocol	(ftString, 32)	HTTP HTTPS SMTP (FTP FILR AS2 ó AS1 ó ¿AS3?)
MsgFrom	(ftString, 255)	
MsgTo	(ftString, 255)	
Subject	(ftString, 255)	
Encrypt	(ftInteger, 0)	
Sign	(ftInteger, 0)	
Compress	(ftInteger, 0)	
MIC	(ftString, 255)	
<i>Fichero MDN</i>		
RequestMDN	(ftInteger, 0)	
MDNSign	(ftInteger, 0)	
MDNAsync	(ftInteger, 0)	
MDNAsyncTo	(ftString, 255)	En salida: HTTP, HTTPS o SMTP En entrada: URL o e-mail donde se debe enviar el MDN.
MDNAsyncPort	(ftString, 255)	Puerto por el que queremos recibir los MDNs asincronos, si vacio toma el puerto en que esta lanzado el protocolo por el que pedimos el MDN
MDNMICAig	(ftString, 32)	
MDNMIC	(ftString, 255)	
MDNTRANSPROT	(ftString, 32)	
MDNTO	(ftString, 255)	
<i>Extra</i>		
URL	(ftString, 125)	
<i>Reintentos y Reenvios</i>		
NextSendTime	(ftDateTime, 0)	
RetrysNum	(ftInteger, 0)	

RetrysPen	(ftInteger, 0)	
ResendNum	(ftInteger, 0)	
ResendPen	(ftInteger, 0)	
ResendMins	(ftInteger, 0)	
updated	(ftDateTime,0,FALSE)	Par marcarlo tras cada cambio realizado en la configuración.

10.2.8 EASLogs

Almacenamiento de logs asociados a los mensajes

Control		
EASDOMAIN	(ftString, 35)	
LogID	(ftString, 255)	EQUIVALE AL NOMBRE DEL LOG
LogType	(ftString, 255)	
LogDate	(ftDateTime, 0)	
LogMsg	(ftString, 255)	
LogData	(ftBlob, 0)	
IdMessage	(ftString, 32, FALSE)	

10.2.9 EASLocks

IDOBJECT	(ftString, 35)	
IDLOCK	(ftString, 255)	
TIMELOCK	(ftDateTime, 0)	
TIMEOUT	(ftDateTime, 0)	
SOURCELOCK	(ftString, 255)	
DESCRIPTION	(ftString, 255, FALSE)	