



# Configuración avanzada



om:

<https://pandorafms.com/manual/!779/>

Permanent link:

[https://pandorafms.com/manual/!779/es/documentation/10\\_pandora\\_itsm/17\\_pandora\\_itsm\\_advanced](https://pandorafms.com/manual/!779/es/documentation/10_pandora_itsm/17_pandora_itsm_advanced)

2025/01/22 19:13



# Configuración avanzada

## Configuración

Al finalizar de modificar los valores de los *tokens* se debe pulsar el botón Actualizar (Update) a fin de guardar los cambios en la base de datos.

### Configuración general

Menú Configuración → Configuración → Configuración general (Setup → Setup → General setup).

- Language: Idioma global para el sistema (por defecto English), cada usuario puede tener definido un lenguaje y este prevalece sobre el valor definido acá.
- Sitename: Nombre del sitio (por defecto Pandora ITSM), visible en el título de todas las ventanas y en el campo asunto de todos los mensajes.
- Enable error log: Fichero con el registro de errores, ubicado por defecto en `/pandora_itsm.log`.
- Timezone for Pandora ITSM: Define el huso horario de la Consola web. Valor por defecto Europe/Madrid.
- List of IP addresses with access to API: Lista de direcciones IP con acceso a la API separadas por comas. Un asterisco (\*) significa "cualquiera" (no se recomienda), valor por defecto `127.0.0.1`.
- Default admin user: En Pandora ITSM siempre debe existir un *superadmin* activo. Esta opción permite especificar uno de estos super usuarios o, de manera predeterminada, en opción automática elegirá el primer *superadmin* activo para ejecutar labores periódicas del sistema PITSM.
- API password: Contraseña necesaria para hacer peticiones *vía API*.
- First day of the week: Primer día de la semana para calendarios y otros usos de la aplicación, lunes por defecto.
- URL update manager: Dirección del servidor de actualizaciones de Pandora ITSM.
- Login hash password: Se utiliza para generar una URL única que se utilizará para preautenticación.
- Enable HTTPS access: Configurar Pandora ITSM para usar HTTPS y cifrar así las comunicaciones.

Al activar el protocolo HTTPS y aumentar la seguridad en las capas de transporte será necesario añadir una verificación del certificado de OpenSSL. Para ello habrá que añadir la siguiente línea en el archivo `php.ini`:

```
openssl.cafile=/etc/ssl/certs/nombre_certificado.ca-bundle
```

- Access port: Configurar el número del puerto de acceso del servidor, valor por defecto 80.
- Public access to server: URL de acceso público al servidor, puede ser una dirección IP o una dirección URL. Se debe especificar HTTP o HTTPS y el sufijo `pandoraitsm`:

`https://mydomain.com/pandoraitsm` (en versiones anteriores el sufijo era `https://mydomain.com/integria`).

- CSV encoding type: Tipo de codificación por defecto de ficheros .csv (véase Separator data in CSV)
- Enable Update Manager checks: Habilita los avisos de actualizaciones disponibles de Pandora ITSM.
- Maximum direct download size (MB): Define el tamaño máximo de un archivo para descargar en la aplicación.
- Max. upload file size: Define el tamaño máximo de un archivo para subir a la aplicación. Si tiene un tamaño más bajo en el sistema (`php.ini`) este límite puede no respetarse.
- Max. Upload file size in CRM (MB) y Max. Upload file size in incidents (MB): Define el tamaño máximo de un archivo para subir a la aplicación en las secciones de *ticket* y CRM.
- Separator data in CSV: Separador de datos en ficheros CSV, valor por defecto la coma , .
- Temporary directory of pdfs: Directorio para almacenar ficheros temporales en informes tipo PDF.
- Hide version: Oculta la versión tanto en el pie de página como en la pantalla de inicio de sesión.
- Show modal last time logged: Muestra a cada usuario la fecha y hora de su último inicio de sesión (formulario modal).
- Welcome view: Define el tiempo (por defecto los últimos 21 días) a mostrar en la pantalla de bienvenida si el usuario tiene activada esta opción en su perfil.
- Chromium path: Ubicación de la dependencia para generación de informes, por defecto `/usr/bin/chromium-browser`.
- Send vacation request notifications to: Consultar [Gestión de proyectos](#).
- Active automatic timetrack stop: Utilizados para registrar el máximo de tiempo trabajado. Está activo por defecto y se detiene de manera automática al sumar y alcanzar el valor especificado en Stop timetrack after (ocho horas y media por defecto).

## Configuración visual

Menú Configuración → Configuración → Configuración visual (Setup → Setup → Visual setup).

Se pueden almacenar imágenes, iconos favoritos y logotipos personalizados en el directorio `../images/custom_logos` y `../images/favicon` respectivamente.

A partir de la versión OUM 103 se dispone del *token* Theme para la combinación de colores (temas) en la Consola web, tanto para la configuración general como a nivel de usuario. Default (Light) está establecido por defecto como tema global y a su vez de igual manera para los usuarios. A menos que se especifique lo contrario, los demás valores de configuración se refieren a ese tema en particular.

Para el caso del dark theme se han establecido *tokens* específicos.

- Favicon: Permite establecer un icono (generalmente de 16 por 16 píxeles) como favorito.
- Block size for pagination: Cantidad de elementos por página en listados. *Se recomienda utilizar valores bajos para evitar repercusiones en el rendimiento.*
- Global dashboard (welcome message): Permite colocar un *dashboard* como pantalla inicial de bienvenida (opcional).
- Font for ITSM: Tipo de fuente de letras por defecto, tanto para interfaz como para ficheros PDF.
- Tabs menu: Utilizado en objetos de inventario y boletos, permita ver las opciones como menú

desplegable, como pestaña o como ambas opciones.

- Global search limit: Número de elementos que aparecerán en los listados cuando se utiliza cualquier búsqueda.

Global search realiza una búsqueda de la(s) palabra(s) clave introducidas con los parámetros de búsqueda por defecto en las siguientes áreas:

- Manage tickets (los tickets cerrados no son mostrados).
- Project management.
- People.
- Contacts.
- Contracts.
- Companies.
- Invoices.
- Leads.
- Wiki (si no arroja resultado presenta enlace para crear artículo).

Se debe tener en cuenta que en los resultados de las búsquedas en cada área se limita a la cantidad de ítems establecida en Global search limit. Dicho valor límite no se muestra en el resultado de la búsqueda solicitada.

*Cada usuario, según sus derechos (ACL) podrá ver mayor o menor cantidad de áreas y resultados.*

## Configuración de política de contraseñas

Menú Configuración → Configuración → Configuración de política de contraseñas (Setup → Setup → Password policy setup).

Se debe asegurar que el *token* Enable password policy está habilitado, por contrario ninguno de los demás *token* funcionarán.

- Min. size password: Longitud mínima que debe tener la contraseña, por defecto cinco caracteres.
  - Password must have numbers: La contraseña debe contener *números*.
  - Password must have symbols: La contraseña debe contener *símbolos*.
  - Password expiration (days): Tiempo, en días, de caducidad de la contraseña, por defecto cero (nunca vence).
  - Force password change on first login: Forzar el cambio de contraseña en el primer inicio de sesión.
  - User blocked if login fails (minutes): Tiempo de bloqueo de usuario, en minutos (por defecto cinco), al haber fallado el inicio de sesión (tras los reintentos configurados en el siguiente campo).
  - Number of failed login attempts: Número de intentos de identificación fallidos.
- 
- A partir de la OUM 95 existe la opción (por defecto desactivada) de mostrar al usuario su último inicio de sesión (*token* **Show modal last time logged**).

- La política de contraseñas no se aplica a usuarios administradores.

## Configuración de incidencias

Menú Configuración → Configuración → Configuración de incidencias (Setup → Setup → Issue setup).

### Opciones visuales

- Show ticket owner y Show ticket creator: Mostrar el creador del *ticket* y mostrar el dueño del *ticket* en vistas de listado y búsqueda de *tickets*.
- Max. tickets by search: Número máximo de *tickets* por búsqueda, esto limitará los resultados en búsqueda de tickets para evitar impacto en el rendimiento. Se recomienda entre 200 y 500.
- Enable quick edit mode: Permite editar rápidamente algunos elementos del ticket (usuario propietario, criticidad, estado) sin entrar en el modo edición completo.
- Show user name instead of ID in the ticket search: Mostrar el nombre real de usuario en lugar del identificador en la búsqueda de *tickets*.
- Format date: Existen dos opciones de formato de fecha, largo yyyy/mm/dd h:m:s (opción por defecto) y aproximado (por ejemplo: 1 día, 2 horas).
- Completion date WU: Al marcar esta opción se mostrará el campo Fecha de realización en las *Workunits* (WU) de los *tickets*. Esa fecha puede ser diferente de la fecha de creación del *Workunit*.
- Sort work units by completion date: Ordenar WU por fecha de realización (en el listado de WU de un *ticket*).
- Most recent comments at the bottom: Cuando está habilitado, los comentarios más nuevos y el campo de entrada para agregar nuevos se mostrarán en la parte inferior de la vista del incidente.

### Comportamiento del ticket

- Disable ticket score: Deshabilitar valoración de las incidencias, por defecto inactivo.
- Allow IW to change creator y Allow IW to change owner: Los usuarios con ese bit de acceso podrán cambiar al creador y/o propietario del *ticket*.
- Editor adds a WU on ticket creation: Se añade una *Workunit* (WU) automáticamente al crear un *ticket*.
- Allow to change the ticket type: Si se desactiva no se podrá cambiar el tipo de *ticket* una vez creado.
- Allow to configure the date/time when creating it: Permitir definir la hora y fecha del *ticket* en el momento de su creación.
- Ignore user defined by the group for the owner: Permite ignorar el usuario predefinido por el grupo para el propietario.
- Ticket type required: Obliga a elegir un tipo de *ticket*, por defecto inactivo.
- Ignore creator user by default: Si se activa permite ignorar el usuario creador por defecto y se deberá especificar manualmente.
- Allow to change creator and owner: Permitir la modificación del usuario creador y el usuario propietario.
- Allow external users to modify their tickets: Permitir a usuarios externos (no agrupados) modificar sus *tickets*.

- Ignore group template for the issue creator: Ignorar plantilla de grupo al creador del incidente.
- Creator can see every user: El usuario creador podrá ver todos los usuarios, incluso de otros grupos (por defecto inactivo).
- Automatically assign ticket: En base a las reglas de asignación de los grupos, permite autoasignar *ticket*.
- Assign ticket to the first editing user: Si se marca, el usuario editor del *ticket* siempre se establecerá como el usuario que editó el *ticket* en primer lugar.
- Change to assigned status if owner adds a note in the ticket: Cambiar el estado asignado si el propietario añade una nota en el *ticket*.

## Opciones de unidades de trabajo (UT)

- Automatically close ticket: Número de días (45 por defecto) tras las cuales un *ticket* será cerrado de forma automática.
- Ticket WU default time: Valor por defecto utilizado al introducir una unidad de trabajo, en unidades de hora. Ejemplo: 0.25 serán 15 minutos.
- Sending email when managing WU: Envío de correo electrónico al administrar WU. A partir de la versión 103 OUM también se puede enviar un correo electrónico a un usuario si este es mencionado en la WU.
- Default internal work units: Las Unidades de trabajo se configuran como internas de manera predeterminada.
- New WU are always public: Activación de comentarios como siempre públicos.

## Flujos de trabajo

- Check closed tickets when running workflow rules: Esta opción sirve para que las reglas de *Workflow* procesen los *tickets* cerrados.
- Days to check closed tickets: Si está marcado el campo anterior, se tendrán en cuenta los *tickets* cerrados en los últimos 15 días (valor por defecto).

## Opciones de envío de correo electrónico

A excepción de los *tokens* 1, 2 y 15, todos los demás vienen activos por defecto.

1. Masking email addresses: Con esta opción activada, no se mostrarán las direcciones de correo que estén en el contenido del *ticket*.
2. Send all attachments for each issue update by email: Envío de todos los adjuntos asociados al *ticket* en cada actualización realizada por medio de *email*.
3. Send email for each created ticket: Enviar notificación de cada *ticket* que sea creado.
4. Send email for each closed ticket: Enviar *email* por cada cierre de incidencia.
5. Send email for each update of the issue status: Enviar notificación por cada cambio de estado del *ticket*. En caso de cambiar su estado a cerrado el envío de la notificación dependerá de la configuración del *token* anterior.
6. Send email for each update of the issue owner: Si el propietario de la incidencia es cambiado, se enviará *email*.

7. Send email for each update of the issue priority: Enviará notificación por cada cambio en la prioridad de trabajo en la incidencia.
8. Send email for each update of the issue group: Enviar *email* por cada actualización del grupo del *ticket*. Esta configuración puede ser general o bien específica por grupo. Para que sea específica por grupo es necesario configurarlo en la edición del propio grupo.
9. Send email for each update of the issue in other fields: Enviará notificación por cada modificación de cualquiera de los otros campos de la incidencia.
10. Send email for each created work unit: Enviar *email* por cada *Workunit* creada. A partir de la versión 103 OUM también se puede enviar un correo electrónico a un usuario si este es mencionado en la WU.
11. Send email for each added attachment: Enviar notificación por cada fichero adjunto añadido.
12. Group work units for each ticket and email: A fin de disminuir la cantidad de mensajes a enviar, este *token* (activo por defecto) agrupa varias notificaciones (ficheros adjuntados y/o WU agregadas en un período de 5 minutos) en una sola notificación.
13. Send email for each validated work order: Enviar *email* por cada validación de orden de trabajo.
14. Send additional emails when the comment is internal: En un *ticket* se pueden agregar direcciones de correo electrónico distintos incluso a los participantes y usuarios de PITSM. Para evitar que estos buzones sean notificados al agregar una WU en comentario interno, se debe deshabilitar esta opción.
15. Send email to workunit creator: Deshabilitado por defecto. Para evitar el comportamiento de bucle que se genera con las respuestas automatizadas por correo electrónico (vacaciones, fuera de horario de trabajo, etcétera) a los creadores de las unidades de trabajo.

## Personalización

### Status y Resolution

Se pueden modificar las etiquetas de los estados y las resoluciones de *tickets*. Es importante tener en cuenta que aunque cambie la etiqueta, la lógica asociada a los estados sigue siendo la misma, por lo que las reglas de SLA, Workflow, o colores de los *tickets* según su estado (nuevo/cerrado) permanecerán igual.

Los mensajes en sí mismos están configurados por defecto en idioma inglés, cambiar el idioma de la Consola web no traducirá estas cadenas de texto.

### Weekends are working days y Special day

Los días no laborables se usan para definir fiestas locales/nacionales, etcétera. No se tienen en cuenta en las SLA, y se visualizan de manera diferente en los calendarios. Con estos dos *token* se pueden definir los fines de semana (sábados y domingos) como laborables y se pueden agregar días festivos con el concepto de días especiales, ambos con fines al cálculo de las SLA.

### Default custom columns

Desde la versión 105 se podrán configurar las columnas por defecto a mostrar en el listado de incidencias. Por defecto los siguientes campos están seleccionados:

- ID.
- SLA.
- Descripción.
- Título / Tipo de incidencia.
- Grupo / Empresa.
- Estado / Resolución.
- Prioridad.
- Actualización de fecha / Fecha de inicio.
- Creador.
- Propietario.

Se podrán agregar a este listado más campos de sistema e incluso campos personalizados que estén marcados para ser mostrados en el listado de incidencias.

Si un campo personalizado es desmarcado para ser mostrado en el listado de incidencias (Show in the list of tickets) aparecerá como una columna vacía, sin título ni contenido. Siendo así, se deberá retirar manualmente dicho campo del listado de los seleccionados.

The screenshot shows a configuration form for a custom field. It includes the following elements:

- Field name:** A text input field containing "Version of product".
- Show in the list of tickets:** A toggle switch that is currently turned off.
- Global field:** A checkbox that is currently unchecked. A tooltip next to it states: "The field will be displayed in a specific column in the ticket list view."
- Type:** A dropdown menu currently set to "Combo".
- Required:** A toggle switch that is currently turned off.
- Combo value:** A text input field containing the values "1,1.1,1.2,1.2.1,2.0,2.1,2.2,2.3,2.3.1".

## Configuración del correo electrónico

Menú Configuración → Configuración → Configuración del correo electrónico (Setup → Setup → Email setup).

El envío de correos (*email*) se utiliza, por ejemplo, cuando se produce un cambio en un *ticket* o se incumple un SLA.

La recepción de correos solamente es necesaria si se utiliza la creación y gestión de *tickets* por *email*.

- Notification period: Periodo de notificación, tiempo mínimo en horas (24 por defecto) que debe pasar entre dos notificaciones de SLA.
- System email from address: Dirección de correos desde el sistema, será el remitente que se utilizará al enviar correos desde Pandora ITSM.

## Configuración de envío de correo

Los campos comunes, independientes del tipo cifrado (excepto cuando se utiliza OAuth 2.0 en el campo Encryption), son:

- SMTP Host: Ubicación de la oficina de correo. Si se deja en blanco, intentará usar un sistema de correo local postfix/sendmail (si se encuentra habilitado).
- SMTP Port: Número de puerto para enviar correo.
- SMTP user: Nombre de usuario.
- SMTP password: Contraseña de usuario.

Los campos para configuración interna de Pandora ITSM son:

- SMTP queue retries: Reintentos de envío de la cola de correo. Si es excedido este número, se marcará el *mail* en la cola como incorrecto.
- Max. pending emails: Número máximo de *emails* pendientes. Si es excedido este número, mostrará una advertencia en la zona de avisos del sistema para indicar que puede haber un problema en el envío de correos.
- Max. emails sent per execution: Máximo número de *mails* enviados por ejecución, se limita así el número máximo de correos en cada ejecución periódica del *script* de mantenimiento.

## Gmail (SMTP)

Gmail® solamente permite el envío de correos cifrados.

- Cifrado con STARTTLS:

## SMTP Parameters - Sending email server configuration

### Encryption

STARTTLS 

### SMTP Host

smtp.gmail.com

### SMTP Port

587

### SMTP user

your@mail

### SMTP password

..... 

### Test connection

Test 

### SMTP queue retries

10

### Max. pending emails

15

### Max. emails sent per execution

0

- Método de cifrado: STARTTLS.
- SMTP Host: smtp.gmail.com
- Puerto: 587 (también podría utilizarse el 25).

Para obtener una contraseña de aplicación de Google® (<https://myaccount.google.com/apppasswords>) se deberá crear una entrada de aplicación, automáticamente se generará una contraseña, copiar manualmente sin espacios al campo correspondiente.

## Google Account

### ← App passwords

App passwords help you sign in to your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.

[Learn more](#)

#### Your app passwords

App name

Created on 06:50



To create a new app-specific password, type a name for it below...

App name

Create

- Cifrado con SSL/TLS
- Método de cifrado: SSL/TLS
- SMTP Host: smtp.gmail.com
- Puerto: 465

### Outlook (SMTP)

MS Outlook® solamente permite el envío cifrado de correos con STARTTLS.



- Método de cifrado: STARTTLS.
- SMTP Host: smtp-mail.outlook.com .
- Puerto: 587 (también podría utilizarse el 25).
- Compatibilidad: Outlook.

MS Outlook® no permite utilizar usuarios de otros servicios de correo, solamente los suyos propios, por lo que es necesario especificar el mismo correo que se utiliza para la configuración SMTP.

### Office 365 (OAuth 2.0)

Desde enero de 2023 Microsoft® solamente permite el envío de correos mediante la autenticación de terceros con OAuth 2.0 .

- Método de cifrado: OAuth 2.0.
- User ID: Identificador de usuario.
- Client ID: identificador de aplicación registrada en Microsoft®.
- Tenant ID: Los valores permitidos son *tenant ID* para el identificador de inquilino o el nombre de dominio, *common* tanto para cuentas de Microsoft® como para cuentas profesionales o educativas, *organizations* solamente para cuentas profesionales o educativas y *consumers* solamente para cuentas de Microsoft®.
- Secret: *Token* privado del usuario.

### Otros (SMTP)

- Cifrado: None para envío sin cifrado o cifrado con SSL/TLS, SSLv2, SSLv3 o STARTTLS.
- Nombre: Nombre DNS o dirección IP del servidor de correo.
- Puerto: Puerto en el que esté escuchando el servidor de correo.
- Usuario: Usuario configurado en el servidor de correo.

- Contraseña: Contraseña configurada para el usuario indicado anteriormente.

## Configuración de recepción de correo

### Configuración de IMAP/POP

Es recomendable, en la medida de lo posible, no utilizar la cuenta de IMAP/POP de ningún usuario interno de Pandora ITSM, ya que esto puede provocar algún comportamiento extraño a la hora de la creación y actualización de los tickets en Pandora ITSM.

#### Gmail (IMAP/POP)

Gmail® solamente permite la recepción cifrada de mensajes de correo mediante SSL/TLS.

#### IMAP:

- POP/IMAP Host: `imap.gmail.com`.
- POP/IMAP Port: 993.
- POP/IMAP user: Buzón de correo electrónico del usuario.
- Select IMAP or POP: IMAP.
- Compatibility: Compatibilidad con Gmail.

#### POP:

- POP/IMAP Host: `pop.gmail.com`.
- POP/IMAP Port: 995 (POP).
- POP/IMAP user: Buzón de correo electrónico del usuario.
- Select IMAP or POP: POP.
- Compatibility: Compatibilidad con Gmail.

La opción Accept any certificate (aceptar todos los certificados) no es recomendable ya que no validará los certificados para el cifrado.

Para configurar la “[Gestión de colas de correo electrónico por grupos](#)” deberá agregar un filtro de dominio en el campo Email origin que coincida con lo establecido acá.

## Outlook (IMAP/POP)

MS Outlook® solamente permite la recepción cifrada con SSL/TLS.

### IMAP:

- POP/IMAP Host: `imap-mail.outlook.com`.
- POP/IMAP Port: 993.
- Select IMAP or POP: IMAP.
- Compatibility: Compatibilidad con Outlook.

### POP:

- POP/IMAP Host: `pop-mail.outlook.com`.
- POP/IMAP Port: 993 (IMAP)/995 (POP).
- Select IMAP or POP: POP/IMAP.
- Compatibility: Compatibilidad con Outlook.

La opción de aceptar todos los certificados no es recomendable de utilizar ya que no validaría los certificados para el cifrado.

Dentro de la configuración de MS Outlook® es necesario tener activada la opción Permitir que los dispositivos y aplicaciones usen la configuración POP.

Para configurar la “**Gestión de colas de correo electrónico por grupos**” deberá agregar un filtro de dominio en el campo Email origin.

## Office 365 (IMAP/POP)

Office 365 solamente permite la recepción cifrada con SSL/TLS.

### IMAP:

- Nombre: `outlook.office365.com` válido tanto para POP/IMAP.
- Puerto: 993 (IMAP)/995 (POP).
- Selección Protocolo: POP /IMAP.
- Compatibilidad: Office 365.

### POP:

- Nombre: `outlook.office365.com` válido tanto para POP/IMAP.
- Puerto: 993 (IMAP)/995 (POP).

- Selección Protocolo: POP /IMAP.
- Compatibilidad: Office 365.

La opción de aceptar todos los certificados no es recomendable utilizarla ya que no validará los certificados para el cifrado.

Para configurar la “**Gestión de colas de correo electrónico por grupos**” deberá agregar un filtro de dominio en el campo Email origin que coincida con lo establecido acá.

#### Otros (IMAP/POP)

- Cifrado: Se puede configurar el servidor POP/IMAP sin cifrado o cifrado con SSL/TLS, SSLv2, SSLv3 o STARTTLS.
- Nombre: Dirección IP o DNS del servidor POP/IMAP.
- Puerto: Número de puerto en el que esté escuchando el servidor POP/IMAP.
- Usuario: Usuario configurado en el servidor de correo.
- Contraseña: Contraseña configurada para el usuario indicado anteriormente.
- Protocolo: POP o IMAP.
- Compatibilidad: Otros.
- Aceptar todos los certificados: Marcado si se desea aceptar cualquier certificado, incluso los autofirmados.

#### Textos genéricos para correo

Los correos que envía Pandora ITSM son encolados hasta que el *script* de mantenimiento los envía, por defecto cada 5 minutos. Para ajustar este comportamiento existen una serie de parámetros especiales, así como un gestor de cola de envíos pendientes.

- Cabecera del correo electrónico: Se utilizará en cualquier correo automático de Pandora ITSM.
- Pie del correo electrónico: Se utilizará en cualquier correo automático de Pandora ITSM.

En ninguno de los dos elementos anteriores se permite el uso de macros.

#### Gestión de la cola de envío de correos

Este sistema permite ver los *mails* pendientes de envío y su estado. Además permite borrar de la cola actual y/o reenviar aquellos mensajes marcados como inválidos. Se pueden seleccionar para dicha operaciones los *mails* de manera individual marcando la casilla asociada a cada uno y luego pulsando Reenviar correos pendientes (Reactivate pending emails) o Borrar correos pendientes (Delete pending emails).

## Configuración de plantillas de correo electrónico

Menú Configuración → Configuración → Configuración de plantillas de correo electrónico (Setup → Setup → Email templates setup).

Permite editar las plantillas de correo que utilizará Pandora ITSM para componer *emails* así como las plantillas del asunto o *subject* del mensaje. Las plantillas de correo son genéricas y se utilizan para todos los grupos.

Para editar una plantilla se hace clic en su nombre o se pulsa el botón de editar correspondiente en la columna de acciones.

Las macros son variables que se sustituirán en el momento de componer el mensaje por un valor real concreto:

- `_author_`: Creador del *ticket*.
- `_creation_timestamp_`: Fecha y hora de la creación del *ticket*.
- `_fullname_`: Nombre completo del usuario que recibe el correo.
- `_group_`: Grupo asignado a dicho *ticket*.
- `_havecost_`: Para informes de la unidad de trabajo del proyecto exclusivamente.
- `_incident_id`: Identificador de *ticket*.
- `_incident_main_text_`: Texto descriptivo principal del *ticket*.
- `_incident_title_`: Título del *ticket*.
- `_owner_`: Usuario que controla el *ticket*.
- `_priority_`: Prioridad del *ticket*.
- `_projectname_`: Para informes del proyecto exclusivamente.
- `_resolution_`: Resolución del *ticket*.
- `_sitename_`: Nombre del sitio, tal y como se haya definido en la Configuración General.
- `_status_`: Estado del *ticket*.
- `_taskname_`: Para informes del proyecto exclusivamente.
- `_time_used_`: Tiempo total empleado en este *ticket*.
- `_update_timestamp_`: La última vez que se actualizó el *ticket*.
- `_url_`: URL del *ticket*.
- `_username_`: Nombre del usuario que recibe el correo (*login name*).
- `_wu_text_`: Texto de la unidad de trabajo.
- `_wu_user_`: Usuario que reporta una unidad de trabajo.
- Plantillas de campos personalizados: Esto permite que al crear un tipo de objeto, el nombre de los campos que se agregue pueda incluirlos como una macro, la cual mostrará el valor de dicho campo: “\_nombre del campo personalizado\_”.

## Gestión de la Visibilidad

Menú Configuración → Configuración → Gestión de la visibilidad (Setup → Setup → Visibility management).

Esta opción sirve para “ocultar” ciertas partes de Pandora ITSM a los grupos de usuarios. Se puede

configurar, para cada sección y grupo de usuarios, los siguientes niveles de visibilidad:

- Oculto: No se mostrará para aquellos usuarios que pertenezcan al grupo indicado.
- Completo: Los usuarios que pertenezcan al grupo indicado tendrán acceso completo a la sección.

Si una sección no tiene ninguna configuración de visibilidad, por defecto el acceso será Completo para todos los usuarios.

Cada sección está asociada a un perfil, siendo este el que se chequea junto con el grupo del usuario para saber si tiene visibilidad o no:

- Proyectos ⇒ PR.
- Tickets ⇒ IR.
- Inventarios ⇒ VR.
- BC ⇒ KR.
- File releases ⇒ KR.
- Agenda ⇒ AR.
- Personas ⇒ Cualquier perfil.
- Work Orders ⇒ WOR.
- Configuración ⇒ Cualquier perfil.

Si el usuario es administrador siempre tendrá acceso completo independientemente de la configuración de visibilidad de menú.

Si un usuario tiene perfiles en varios grupos que tienen distintos niveles de visibilidad en una sección, la visibilidad para ese usuario en esa sección será la menos restrictiva.

Si se crea un nivel de visibilidad para una sección seleccionando todos los grupos (grupo Todos), se eliminará cualquier otra configuración anteriormente registrada para esa sección, permaneciendo solamente la introducida.

## Inventario de Pandora FMS

Menú Configuración → Configuración → Inventario de Pandora FMS (Setup → Setup → Pandora FMS inventory).

Esta sección controla tanto las opciones de **inventario** como la gestión del inventario remoto (procesamiento de datos enviados por agentes de Pandora FMS a Pandora ITSM, sin necesidad de instalar Pandora FMS).

### Opciones de inventario

- Duplicate inventory name: Permite la opción de tener nombres de objetos de inventario con el mismo

nombre. Opción activada por defecto.

- CSV compatibility import: Si la opción está desactivada permite que se muestren los CSV como un informe mostrando los objetos de inventario seleccionados previamente por el usuario tal y como aparecen en la lista. Opción activada por defecto.

Procesado de datos de inventario desde agentes de Pandora FMS (Remote inventory):

- Default owner: Propietario por defecto para esos objetos.
- Associated company y Associated user: Compañías y usuarios con acceso a esos objetos.

## Configuración del método de autenticación

Menú Configuración → Configuración → Configuración del método de autenticación (Setup → Setup → Authentication configuration).

Los usuarios de tipo Super administrator (*superadmin*) son los únicos que siempre realizan una autenticación de manera local, a diferencia del resto de los usuarios quienes, si se configura, pueden autenticar de manera remota con LDAP® o Active Directory®.

Si el LDAP® o Active Directory® están configurados, Pandora ITSM consultará primero a estas plataformas si el usuario existe y si la contraseña es correcta.

Con el *token* Session timeout (secs) se configura el tiempo máximo de la sesión (por defecto nueve mil segundos).

### Active Directory

Se puede configurar si, en caso de fallar la autenticación remota, se pueda autenticar de manera local activando el *token* Fallback to local authentication.

Al activar la opción de crear usuarios de manera automática (Automatically create remote users) se puede configurar la opción de asignar nivel de usuario, perfil y grupo e incluso especificar una lista de usuarios restringidos (Automatically create blacklist). En la configuración avanzada de Active Directory® (Advanced Configuration AD) se podrán agregar nuevos permisos.

### LDAP

Al seleccionar LDAP® como autenticación remota se podrá elegir entre LDAPv1, LDAPv2 y LDAPv3 y, de manera opcional, cifrar las comunicaciones al activar el *token* Start TLS.

Este método de autenticación carece de la opción de autenticar de manera local en caso de

algún fallo (para usuarios que no sean *superadmin*).

## Autenticación en dos pasos

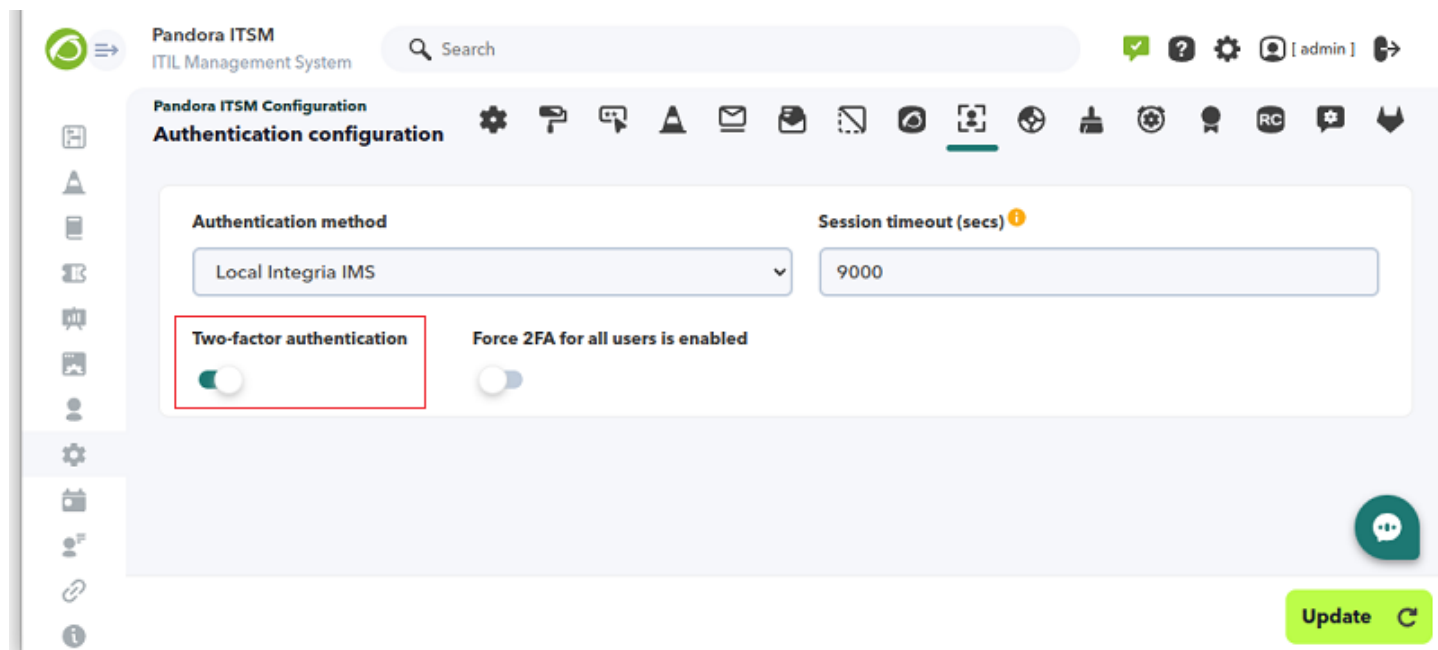
La autenticación en dos pasos (o doble autenticación) lleva años posicionándose como una de las mejores opciones para aumentar la seguridad de una cuenta de usuario. Pandora ITSM incorpora esta funcionalidad realizando una integración con la solución Google Authenticator®.

### Requisitos

Será necesario disponer de la aplicación generadora de códigos en un dispositivo móvil personal para cada usuario.

<https://support.google.com/accounts/answer/1066447>

Se debe tener derechos de *superadmin* para acceder a las opciones de configuración de PITSM, menú Setup → Setup → Authentication configuration → Two-factor authentication y habilitar esta funcionalidad.



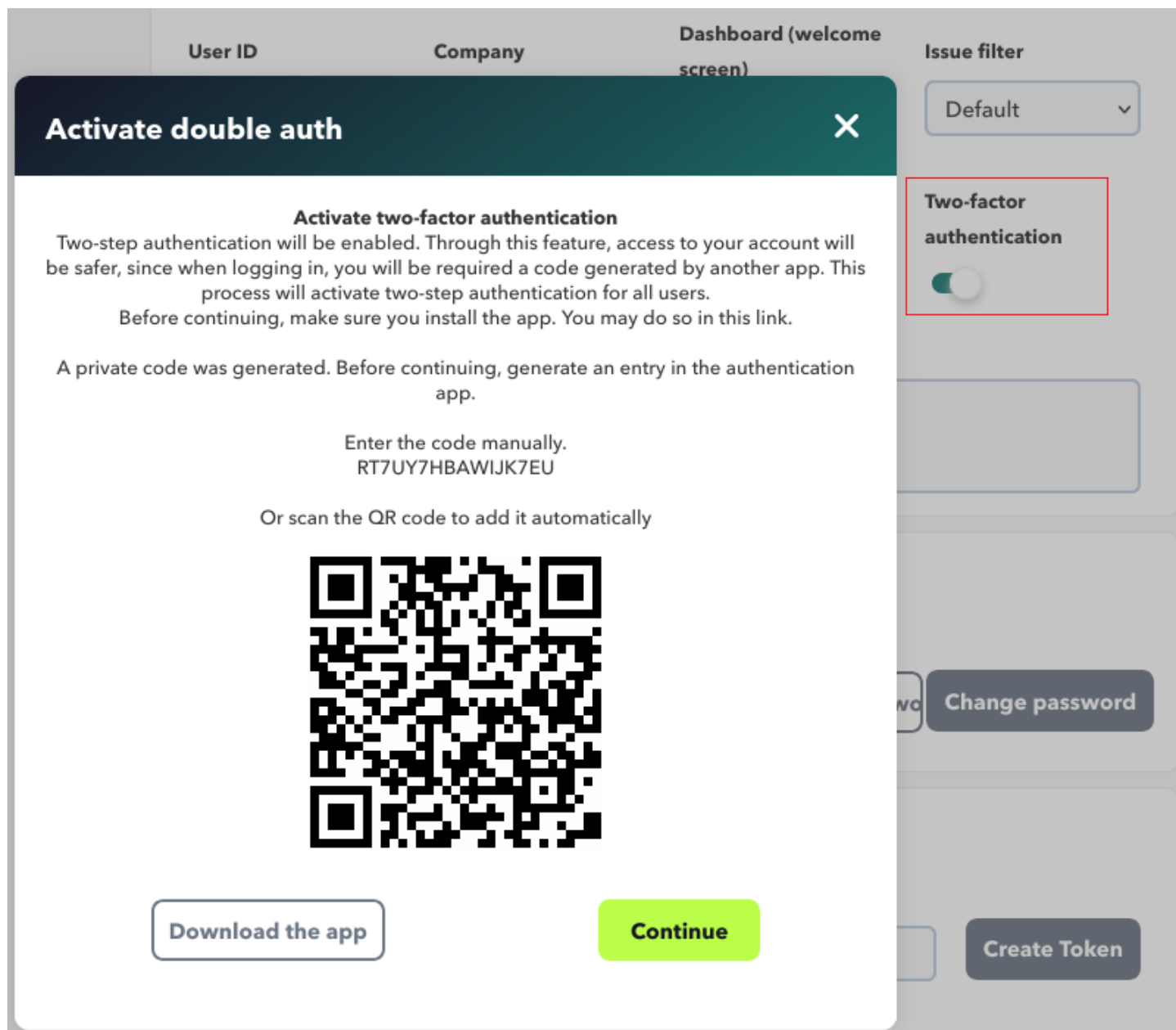
De esta manera cada usuario podrá activar la autenticación en dos pasos con la opción **Edit my user**. Se cuenta también con la opción Force 2FA for all users is enabled, por defecto desactivada, para indicar al resto de los usuarios, al inicio de cada sesión, de que activen la autenticación en dos pasos.

Es sumamente importante que el servidor PITSM tenga configurado exactamente la hora

y fecha.

## Proceso a seguir para cada usuario

Cuando cada usuario edite sus propio datos y active su Two-factor authentication, Pandora ITSM generará un clave de autenticación la cual mostrará también por medio de un código QR:



Por medio de la aplicación instalada podrá leer dicho código QR (o ingresar manualmente la clave) y el código resultante debe ser ingresado PITSM y hacer clic en el botón Validate code.

Luego que el usuario cierre sesión deberá volver a colocar sus credenciales y, si son validadas, se procederá introducir el código generado por el dispositivo personal, para ese momento específico, y finalizar así la doble autenticación.

En caso de que un usuario no *superadmin* necesitare un reinicio de su clave de doble

autenticación, deberá solicitarlo directamente con un *superadmin* quien utilizará la opción Reset double factor authentication code del usuario solicitante:

People / Users  
**Edit user**

— Security

Set a new password

.....

Generate password

Confirm new password

.....

We recommend the password to be at least 12 characters long, include a mix of uppercase and lowercase letters, contain numbers and special characters (e.g., !, @, #, \$), and avoid common words or easy-to-guess details like your name or birthday.

**Reset double factor authentication code**

Reset

Reset double factor authentication for this user

The next time this user logs in, they will be prompted to create a new code. This action does not kick his out of the system.

send email to user with username and password

**Activation**

Enabled ☒ Disabled ☐

**Ena**

Enabled ☒ Disabled ☐

En caso de que un *superadmin* necesite reiniciar su clave de autenticación en dos pasos deberá iniciar sesión con su nombre de usuario y contraseña y luego pulsar el botón Reset double factor authentication code. Un mensaje de correo electrónico le será enviado de inmediato, acompañado de un enlace y dispondrá de 15 minutos para hacer clic en dicho *link*.

El envío de correos **SMTP** debe estar activo y plenamente funcional para poder reiniciar la clave de doble autenticación de los *superadmin*.

## Configuración CRM

Menú Configuración → Configuración → Configuración CRM (Setup → Setup → CRM setup).

En esta sección se configuran los parámetros de **factura** tales como imagen para la cabecera, métodos de pago, o siglas del impuesto. También se puede ocultar el identificador fiscal (deshabilitado por defecto) y automatizar la numeración de facturas.

Se puede activar (o desactivar) la generación automática de ID de factura, y modificar su estructura:

En el campo Invoice ID pattern se guarda una cadena de texto que se utilizará como patrón para generar los identificadores, por defecto 21/[1000]. Este patrón contendrá una parte fija y una variable. La parte variable debe ser numérica y servirá como primer elemento a partir del cual calcular una secuencia. La parte variable irá entre corchetes. Lo demás será constante en todas las facturas.

La generación de identificadores de facturas se aplica únicamente en las facturas de tipo Enviado.

En la sección de configuración del CRM podrá también cambiar el nombre de los estados de los *leads* para personalizar su *pipeline*.

## Mantenimiento de datos antiguos

Menú Configuración → Configuración → Mantenimiento de datos antiguos (Setup → Setup → Old data maintenance).

Permite especificar al sistema cómo gestionar la información histórica. Si el valor indicado es cero 0 en un *token*, los datos relacionados siempre se mantendrán.

La opción Eliminar todos los datos eliminará TODOS los datos de la base de datos y también los ficheros adjuntos. Use esta opción para comenzar de nuevo.

El botón Restaurar a valor por defecto cambiará todos y cada uno de los *tokens* y guardará automáticamente. Se indican dichos valores por defecto y los detalles relevantes:

- Días para borrar eventos: 30.
- Días para borrar tickets cerrados: 0. También se borrarán los datos relacionados.
- Días para borrar Unidades de Trabajo: 0. Siempre y cuando pertenezcan a proyectos deshabilitados, se borrarán también las horas de trabajo más antiguas que los días indicados.
- Días para borrar partes de trabajo: 0.
- Días para borrar información de auditoría: 15.
- Días para borrar sesiones: 7.
- Días para borrar eventos de flujos de trabajo: 900.
- Días para borrar los ficheros adjuntos a los tickets: 0.
- Días para borrar datos de seguimiento de archivos: 30.
- Días para borrar copias de seguridad: 30.
- Días para borrar los emails no válidos: 30. Mensajes que no hayan podido ser enviados.
- Días para borrar informes: 365. Informes que hayan sido autogenerados de forma periódica.
- Días para borrar rooms de chat-bot archivados: 365.

## Gestión de proyectos

Menú Configuración → Configuración → Gestión de proyectos (Setup → Setup → Project management).

- Autocompletado de UT (días): Se especifica la cantidad de días (por defecto cero) en un ciclo de trabajo. Generalmente se utilizan períodos de tiempo tales como semanal, quincenal o mensual,

introduciendo la cantidad de días reales a trabajar. Esta característica autocompletará las UT hacia atrás desde el momento actual. Estas horas introducidas a los usuarios no se asignan a ninguna tarea en ningún proyecto, sino a las horas “Sin justificar”.

- Usuarios sin completado de UT: Esta es una lista específica de usuarios (separados por un espacio) sin autocompletado de UT.
- Horas de trabajo por día: Este número representa el número de horas (ocho por defecto) de un día de trabajo normal, a fin de calcular el autocompletado de UT.
- Tiempo por defecto para UT de un proyecto: cuatro horas, valor por defecto.
- Moneda: euro por defecto (eu).
- Deshabilitar adición de tickets y unidades de trabajo para tareas pendientes y verificadas: A fin de poder finalizar un proyecto verificado, se activa este *token* para cesar de agregar trabajo que ocasione retraso.
- Días totales de vacaciones: Número de días de vacaciones (veintidós por defecto) que será usado para los cálculos correspondientes en el apartado de informe de vacaciones.
- Enviar notificaciones de solicitud de vacaciones a: Permite establecer el usuario por defecto para la **aprobación de vacaciones**. Se debe verificar que se especifica un usuario válido (existente y habilitado).

## Pandora RC

Menú Configuración → Configuración → Pandora RC (Setup → Setup → Pandora RC).

Para activar el **sistema de gestión remota Pandora RC** (anteriormente conocida como *eHorus*).

## ChatBot

Menú Configuración → Configuración → ChatBot (Setup → Setup → ChatBot).

Para **activar ChatBot** y configurar el servidor y canales.

## GitLab

Menú Configuración → Configuración → GitLab (Setup → Setup → GitLab).

Para la integración con GitLab® se necesita de un *token* de acceso que pertenezca a un usuario de **GitLab** con permisos para visualizar los *tickets* de un proyecto determinado. Una vez haya sido configurado se podrá consultar por la Consola web de Pandora ITSM, solamente en modo de lectura, las incidencias registradas en un proyecto.

## Gestor de archivos

Menú Configuración → Gestor de archivos (Setup → Setup → File manager).

Permite subir nuevos ficheros al Sistema de distribución de ficheros integrado en Pandora ITSM. Dichos ficheros se ubican en el directorio `/attachment/downloads`.

Además permite la creación y borrado de directorios para una mejor organización.

También se pueden cambiar los iconos por defecto en el directorio `/images`. Para almacenar imágenes de logotipos se utiliza el directorio `/images/custom_logos`.

## Información de diagnóstico

Menú Configuración → Información de diagnóstico (Setup → Diagnostic info).

Se describen algunas características:

- Información del estado de Pandora ITSM: Con la versión y el directorio donde está instalada, entre otros valores.
- Configuración PHP: Con la versión instalada y el valor de importantes parámetros como el máximo de memoria dedicado y tamaño máximo de los ficheros a subir.
- Estadísticas de tamaño de la base de datos: Total de boletos, usuarios y sesiones registradas.
- Información sobre el estado de la base de datos: Versión y fecha del motor de base de datos.
- Información del sistema: Con información básica el hardware donde se ejecuta Pandora ITSM.
- Métricas de rendimiento de MySQL: Valores configurados, además se muestran los valores recomendados como medida de comparación.
- Fechas de logs de Pandora ITSM.
- Estado de la carpeta de adjuntos: Cantidad general de ficheros almacenados.
- Sistema de fechas: Fecha y hora de Pandora ITSM.

## Noticias globales

Menú Configuración → Noticias globales (Setup → News board).

Permite añadir pequeñas noticias del sistema, que serán visibles a todos los usuarios cuando entren. Útil para avisar de cambios en la plataforma o avisos sobre intervenciones, desconexión del servicio u otros.

Se puede enviar a grupos específicos y de manera opcional establecer una fecha de vencimiento tras lo cual se dejará de mostrar el mensaje en el tablero de anuncios.

## Gestor de bases de datos

Menú Configuración → Gestor de bases de datos (Setup → DB Manager).

Es una interfaz directa contra la base de datos del sistema, en SQL, a la cual solamente tienen acceso los *superadmin* y los **usuarios con perfil DM**.

Para uso exclusivo de usuarios expertos pues su mal uso de ella puede causar daños irreversibles en la herramienta y la eliminación de datos.

## Enlaces

Menú Configuración → Enlaces (Setup → Links).

Se podrán añadir y eliminar enlaces externos que se mostrarán en la sección Enlaces del menú principal y se abrirán en una pestaña nueva del navegador web. Para los enlaces internos se debe colocar los subdirectorios, tal como para la **Wiki**: `wiki/operation/wiki/wiki`.

## Eventos del sistema

Menú Configuración → Eventos del sistema (Setup → System events).

Histórico de los eventos sucedidos en el sistema, como el envío de informes programados, ejecución de tareas del cron, fallos del sistema, etcétera.

La información de actividad de usuarios se almacena en el *log* de **auditoría**.

## Log de auditoría

Menú Configuración → Log de auditoría (Setup → Audit log).

En este registro quedarán reflejadas las acciones de cada usuario en cada sección, todas en compendio de 51 acciones. Si alguien modifica un dato de un cliente, se sabrá cuándo y qué se cambió. Si alguien crea una factura, se sabrá cuándo y cuál factura, etcétera.

Permite buscar por una subcadena concreta y por período de fecha, además de poder exportar a un fichero CSV.

## Registro de errores

Menú Configuración → Registro de errores (Setup → Error log).

Visualiza el *log* de errores (si éste está activado), útil para identificar posibles errores de código del sistema. Por defecto lee del fichero `/var/www/html/integria/pandora_itsm.log` las últimas líneas y presenta un botón de borrado definitivo de datos.

## Traducir cadenas

Menú Configuración → Traducir cadenas (Setup → Translate strings).

Permite realizar traducción personalizada de cualquier texto que aparece en la interfaz de Pandora ITSM.

Se podrá seleccionar el idioma que desea modificar y un campo libre para buscar texto específico o se puede dejar vacío para visualizar todas las cadenas.

La búsqueda se realiza sobre el idioma inglés original, todas las traducciones se basan en este idioma. Al seleccionar este idioma en la lista se podrá ajustar y/o corregir cadenas.

## Copia de seguridad

Menú Configuración → Copia de seguridad (Setup → Backup).

La sección de *backup* permite a los usuarios de Pandora ITSM realizar copias de seguridad de los archivos adjuntos y de la base de datos, tanto de forma manual como de manera programada.

Backup list 

La primera consiste en una lista de *backups* existentes en la carpeta backup dentro del directorio de Pandora ITSM. Desde aquí puede borrar un *backup*, descargar o restaurar el sistema PITSM desde cualquier ítem de la lista.

Se debe tener especial cuidado al realizar esta acción ya que el *backup* sustituirá la

información de base de datos por la que tenía en ese *backup*, haciendo que la información añadida entre el *backup* y el sistema en su estado actual desaparezca.

## Backup programming

La segunda sección permite realizar programaciones para que, pasado un tiempo específico, se realice un *backup* del sistema Pandora ITSM. Para la creación de una programación de *backups* se debe incluir un nombre para la programación, un modo de *backup* (hay tres modos, solamente base de datos, solamente ficheros adjuntos o ambos) y una periodicidad de *backup* (por defecto semanal). Se puede agregar una dirección de correo electrónico al que llegarán las notificaciones si algo sale mal en este proceso. Además, en la misma sección se tiene disponible la lista de programaciones para su edición o borrado, según convenga.

## Backup manager

La tercera y última sección es la encargada de realizar los *backup* manuales en el momento actual, dando la posibilidad de crear un *backup* con el nombre y el modo deseado (y opcionalmente una dirección de correo para las notificaciones de error). Este respaldo de datos se creará en la carpeta backup dentro del directorio de Pandora ITSM y luego estará disponible en la lista de respaldos.

También cuenta con la posibilidad de subir respaldos previamente descargados, estos deben tener la misma estructura que genera la herramienta para mantener la consistencia y no estar previamente en base de datos.

# Actualización

- Menú Warp update → Update offline.
- Menú Warp update → Update online.
- Menú Warp update → Options.
- Menú Warp update → Warp journal.

Desde la versión 105 el **Warp update** forma parte de Pandora ITSM. Ayuda a los administradores de sistemas a actualizar Pandora ITSM automáticamente ya que se encarga de la tarea de encontrar nuevos módulos, *plugins* y funcionalidades (incluso herramientas de migración para futuras versiones) de manera automática.

## Licencia

Menú Warp update → Licencia (Warp update → License).

En esta sección se debe introducir la licencia de Pandora ITSM. Una vez introducida se pulsa el botón de Actualizar licencia (Update license) para que Pandora ITSM verifique si es válida.

## License

### License information

#### License key

PAND  
1TEG  
2XVX

ZRXOZMT  
SQPR3PFR  
UNW1LDH

**Licence mode** Perpetual

**Expires** December 31, 2034, 12:00 am

**Manager limit** 5

**Manager count** 2

Manage users

Request new license

Update license 

### Solicitar nueva licencia

Al pulsar el botón Request new license se abrirá un formulario donde se deberá introducir la clave de autorización (Auth key) proporcionada por el [departamento de soporte](#).

# License

License information

Activate license
X

Your **request key** is:

**#0000000000**

You can activate it manually **here** or automatically filling the form below:

Auth Key:

**Online validation**

Manage users
Request new license
Update license ↻

Se deberá pulsar el botón de validación en línea (Online validation) y finalmente actualizar la licencia en el botón Update license.

En el caso de que la Consola web esté aislada de internet, se podrá usar la opción fuera de línea copiando el enlace (texto here) el cual incluye la clave de solicitud (Request key).

## Generate key for PandoraTSM

Auth key

Request key

License key

Generate

Una vez en el navegador web con acceso a internet, introducir la clave de autorización (Auth key)

proporcionada por el [departamento de soporte](#), pulsar Generate y obtener una nueva licencia. Esta se debe copiar y regresar a la Consola web, borrar la licencia anterior, pegar la nueva licencia y pulsar el botón de actualizar licencia.

[Volver al índice de documentación de Pandora ITSM](#)