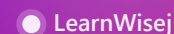


Configuración, seguridad y despliegue

Configuración y secretos · Seguridad y preparación para el despliegue



Configuración y secretos

Qué archivos de configuración revisar antes de publicar, cómo distinguir depuración de producción y cómo gestionar de forma segura las claves de licencia y los secretos.



Objetivo de la lección

Aprende qué archivos de configuración revisar antes de publicar, cómo distinguir depuración, staging y producción, y cómo gestionar de forma segura las claves de licencia, las cadenas de conexión y otros secretos.

1. Archivos de configuración que debes revisar

En un proyecto Wisej.NET, la configuración puede estar en varios sitios. No necesitas memorizar cada ajuste avanzado, pero sí debes saber dónde mirar antes del despliegue.

Área	Qué comprobar	Por qué importa
<code>Program.cs</code> / inicio	Qué ventana o página se inicia, la lógica de inicio específica de cada entorno y la configuración de los servicios.	La aplicación desplegada debe abrir el punto de entrada correcto.
<code>Web.config</code> / configuración de hosting	Indicador de depuración, handlers, ajustes del servidor, reglas de reescritura, comportamiento ante errores.	El hosting en IIS depende en gran medida de una configuración correcta.
<code>Default.json</code> / JSON de la aplicación	Endpoint de Wisej.NET, tema, URL, ajustes de ventana o página, referencias a recursos estáticos.	Unas URL o unos temas incorrectos pueden hacer que una aplicación desplegada falle o se vea rota.
Temas y archivos estáticos	Carpeta de temas, CSS, imágenes, iconos, archivos JavaScript.	Los recursos deben incluirse en el paquete de despliegue.
Configuración del registro	Destino del registro, nivel de registro, detalles de error protegidos.	Producción necesita poder diagnosticar sin exponer detalles internos.

2. Depuración frente a staging frente a producción

Los ajustes de depuración ayudan durante el desarrollo, pero los de producción deben ser más seguros y estar más controlados. Antes de publicar, revisa el entorno y asegúrate de que no se ha dejado activado por accidente el comportamiento de depuración.

- **Depuración:** errores detallados, pruebas en local, diagnóstico más sencillo; no es seguro para usuarios públicos.
- **Staging:** un área de pruebas similar a producción que se usa antes de publicar.
- **Producción:** mensajes de error seguros, secretos protegidos, configuración estable, registro activado.



Regla de publicación segura

Los usuarios deben ver un mensaje útil; los desarrolladores deben ver los detalles técnicos en registros seguros del servidor. Nunca muestres trazas de pila, rutas de archivos, claves de licencia ni cadenas de conexión en la interfaz.

3. Gestión de secretos y claves de licencia

Los valores sensibles no deben escribirse directamente en el código de la interfaz, en los eventos de los botones, en capturas de pantalla ni en el control de versiones: claves de licencia, cadenas de conexión a bases de datos, claves de API, contraseñas SMTP y credenciales de despliegue.

Práctica insegura	Práctica más segura
Escribir una clave de licencia directamente en una página o en el evento de un botón.	Usar una configuración segura o variables de entorno.
Confirmar cadenas de conexión en Git.	Mantener los secretos fuera del control de versiones; usar los secretos del despliegue.
Mostrar a los usuarios los detalles sin procesar de las excepciones.	Registrar los detalles en el servidor y mostrar un mensaje seguro.
Compartir credenciales de producción en capturas de pantalla.	Ocultar los secretos o evitar mostrarlos en los materiales de formación.



Ya estás listo para la siguiente lectura

Sabes localizar los archivos de configuración clave, separar la depuración de la producción y mantener seguros los secretos. A continuación: autenticación y autorización, registro y una lista de comprobación de despliegue.

Seguridad y preparación para el despliegue

Autenticación frente a autorización a nivel junior, registro seguro, destinos de despliegue y una lista de comprobación obligatoria antes de publicar.



Objetivo de la lección

Entiende la diferencia entre autenticación y autorización a nivel junior, registra de forma segura y construye una lista de comprobación de despliegue para IIS, Kestrel o hosting en la nube.

1. Autenticación y autorización

La **autenticación** responde a *¿quién es el usuario?* La **autorización** responde a *¿qué puede hacer este usuario?* El Módulo 9 lo presenta como un concepto de diseño antes de una implementación completa de identidad.

- **Autenticación:** inicio de sesión, proveedor de identidad, identidad de la sesión, nombre de usuario, claims de rol.
- **Autorización:** comprobaciones de rol, acceso a páginas, acceso a comandos, botones ocultos o deshabilitados.
- **Ejemplo:** un Support Agent puede gestionar tickets; un Admin puede editar los ajustes de despliegue.
- Nunca confíes *solo* en ocultar un botón: la lógica del servidor también debe proteger la acción.

```
bool canReviewDeployment =
    currentUser.Role == "Admin" || currentUser.Role == "Team Lead";

btnReviewPackage.Enabled = canReviewDeployment;
lblPermission.Text = canReviewDeployment
    ? "Deployment review available."
    : "Review is restricted.";
```

2. Lista de comprobación de registro y diagnóstico

El registro debe dejar constancia de lo que ha ocurrido sin exponer secretos. Un buen registro de diagnóstico es breve, legible y útil cuando algo sale mal.

- Registra el inicio y el final de los flujos importantes.
- Registra los fallos de validación y los fallos de la revisión del despliegue.
- Registra las excepciones en el servidor con el detalle suficiente para un desarrollador.
- No registres contraseñas, claves de licencia ni datos privados de los usuarios.
- Añade marcas de tiempo para que el orden de los eventos quede claro.

3. Destinos de despliegue

Destino	Comprobaciones a nivel junior
IIS	Publica la carpeta de la aplicación, revisa <code>Web.config</code> , comprueba el hosting bundle si es necesario, confirma el grupo de aplicaciones y prueba la URL.
Kestrel / autohospedaje	Confirma las variables de entorno, los puertos, el proxy inverso, HTTPS y los archivos de configuración JSON.
Nube	Confirma los ajustes de la aplicación, los secretos, los archivos estáticos, el registro y la configuración de ranuras de despliegue / staging.

4. Lista de comprobación obligatoria antes de publicar

- `Web.config` revisado y modo de depuración configurado correctamente.
- Clave de licencia de Wisej.NET gestionada de forma segura.
- Ventana predeterminada o de inicio, tema y URL comprobados.
- Temas y recursos estáticos incluidos.
- Destino del registro configurado.
- Plan de autenticación y autorización revisado.
- Los archivos sensibles no se pueden descargar públicamente.
- Compilación release probada en local antes del despliegue.
- Requisitos del destino de despliegue comprobados.



Ya estás listo para el laboratorio

A continuación: mira el recorrido guiado de la revisión del despliegue, supera la evaluación de conocimientos y después construye una pantalla de lista de comprobación de publicación: comprobaciones obligatorias y opcionales, notas de despliegue, un registro de diagnóstico y un mensaje de estado del paquete que cambia cuando se completan las comprobaciones obligatorias.