



Requisitos aplicaciones web

Contenido

Introducción	2
Base de datos.....	2
Servidores	3
Instalación monolítica	4
Instalación monolítica con servidor de base de datos independiente	5
Instalación independiente.....	6
Instalación a medida	7
Servidor DMZ (Opcional)	8
Subdominio de Internet.....	8
Certificado SSL.....	8
Cuenta de correo electrónico.....	9
Apertura de puertos	9

datos de contacto

A.T. MEDTRA, S.L.
Parque Científico y Tecnológico
Edificio 3000
C/ Isabel Torres 11 B
39011 Santander
Cantabria (España)
atmedtra@atmedtra.es
www.atmedtra.es
+34 942 23 51 41



Requisitos aplicaciones web

Introducción

En este documento se detallan los requisitos técnicos para desplegar las aplicaciones web de A.T. Medtra, S.L.: **Sehtra** Edición Web, **Integra Prevención** y **Portal de Prevención**.

Lea atentamente este documento y no dude en contactar con nosotros si tiene cualquier duda o su infraestructura no se adapta a los escenarios de despliegue aquí propuestos.

Cuando tenga listos todos los requisitos hardware y software, un técnico de AT Medtra se conectará con usted para instalar las aplicaciones web y el software adicional.

Base de datos

Las aplicaciones soportan varias bases de datos, se detallan a continuación:

- Microsoft SQL Server 14.0 o superior
- Oracle Server 18c o superior

Es muy importante que la conexión entre el servidor de base de datos y las aplicaciones sea rápida y tenga tiempos de respuesta y latencia reducida. Una latencia elevada afectará enormemente a la velocidad de las aplicaciones y la experiencia de usuario empeorará mucho. Sería ideal contar con tiempos de respuesta inferiores a 5 ms.

** La base de datos al igual que el resto de los componentes de las aplicaciones se despliegan en las instalaciones del cliente, por tanto, es este quien provee del servidor o servidores de bases de datos necesarios y asume su coste de adquisición y mantenimiento.*



Requisitos aplicaciones web

Servidores

Las aplicaciones web de A.T. Medtra, S.L. se despliegan en las instalaciones del cliente (On-Premise, nube privada), por tanto, es este quien provee del servidor o servidores web necesarios y asume su coste de adquisición y mantenimiento. Se soportan varios escenarios de despliegue, que se detallan a continuación:

- **Instalación monolítica:** Todos los componentes y aplicaciones, incluida la base de datos, se despliegan en el mismo servidor.
- **Instalación monolítica con servidor de base de datos independiente:** todas las aplicaciones de la Suite Medtra se despliegan en el mismo servidor, el servidor de base de datos es independiente en este caso.
- **Instalación independiente:** En este caso, el servidor de aplicaciones web es independiente al de aplicaciones (las aplicaciones de escritorio de la Suite Medtra se despliegan en un servidor y las aplicaciones web en otro distinto).
- **Instalación a medida:** Si ninguno de los anteriores escenarios se adapta a las necesidades de tu servicio de prevención, podemos analizar tu situación y buscar otras alternativas.



Requisitos aplicaciones web

Instalación monolítica

Este es un escenario habitual para servicios de prevención pequeños, o para desplegar máquinas de pruebas (también cuando se dispone de pocos recursos o máquinas). Es la instalación más minimalista posible. En este escenario existe un único servidor que aloja todos los componentes necesarios para el uso de la Suite Medtra: Las aplicaciones de escritorio para Microsoft Windows (**Medtra, Sehtra, Ergotra, Citaciones**), como las aplicaciones web. Es el despliegue más sencillo de realizar y económico, pero no es demasiado flexible y no será muy escalable.

Requisitos mínimos:

- Uno de los siguientes sistemas operativos de 32 o 64 bits.
 - o Windows Server 2016.
- 10GB de memoria RAM.
- CPU de 4 núcleos.
- Cliente nativo para base de datos (SQL Server u Oracle).
- Internet Information Services 7.0 (o superior).
- URL Rewrite (módulo de Internet Information Services).
- Un navegador web (utilizado por el usuario final para acceder a la aplicación).
 - o Google Chrome u otro navegador basado en Blink.
 - o Mozilla Firefox u otro navegador basado en Gecko.
 - o Safari u otro navegador basado en WebKit.

Requisitos recomendados:

- Uno de los siguientes sistemas operativos de 64 bits.
 - o Windows Server 2019 o superior.
- 16GB de memoria RAM.
- CPU de 4 núcleos o superior.
- Cliente nativo para base de datos (SQL Server u Oracle).
- Internet Information Services 10.0 (o superior).
- URL Rewrite (módulo de Internet Information Services).
- Un navegador web (utilizado por el usuario final para acceder a la aplicación).
 - o Google Chrome.
 - o Mozilla Firefox.
 - o Microsoft Edge.



Requisitos aplicaciones web

Instalación monolítica con servidor de base de datos independiente

Este es el escenario más común en servicios de prevención pequeños. En este escenario existe un único servidor que aloja tanto las aplicaciones de escritorio para Microsoft Windows (**Medtra, Sehtra, Ergotra, Citaciones**), como las aplicaciones web. La base de datos se despliega en otro servidor independiente. Es un despliegue sencillo de realizar y de mantener, pero para algunos clientes puede no ser lo suficientemente flexible.

Requisitos mínimos:

- Uno de los siguientes sistemas operativos de 32 o 64 bits.
 - o Windows Server 2016.
 - o Windows 10.
- 8GB de memoria RAM.
- CPU de 4 núcleos.
- Cliente nativo para base de datos (SQL Server u Oracle).
- Internet Information Services 7.0 (o superior).
- URL Rewrite (módulo de Internet Information Services).
- Un navegador web (utilizado por el usuario final para acceder a la aplicación).
 - o Google Chrome u otro navegador basado en Blink.
 - o Mozilla Firefox u otro navegador basado en Gecko.
 - o Safari u otro navegador basado en WebKit.

Requisitos recomendados:

- Uno de los siguientes sistemas operativos de 64 bits.
 - o Windows Server 2019 o superior.
 - o Windows 10 o superior.
- 12GB de memoria RAM.
- CPU de 4 núcleos o superior.
- Cliente nativo para base de datos (SQL Server u Oracle).
- Internet Information Services 10.0 (o superior).
- URL Rewrite (módulo de Internet Information Services).
- Un navegador web (utilizado por el usuario final para acceder a la aplicación).
 - o Google Chrome.
 - o Mozilla Firefox.
 - o Microsoft Edge.



Requisitos aplicaciones web

Instalación independiente

Este es el escenario más flexible y que más posibilidades ofrece a los administradores. Además, permitirá gestionar de una manera más eficiente los recursos. Es el escenario recomendado para servicios de prevención medianos o grandes. En este escenario existe un servidor de aplicaciones que aloja las aplicaciones de escritorio (**MEDTRA** y **SEHTRA**, **Ergotra**, **Citaciones**), un servidor web que aloja únicamente las aplicaciones web (Edición web de **SEHTRA**, **Integra Prevención** y **Portal de Prevención**) y el servidor de base de datos. Este servidor web puede estar compartido con otras aplicaciones web corporativas también (si los recursos lo permiten).

Requisitos mínimos:

- Uno de los siguientes sistemas operativos de 32 o 64 bits.
 - o Windows Server 2016.
 - o Windows 10.
- 8GB de memoria RAM.
- CPU de 4 núcleos.
- Cliente nativo para base de datos (SQL Server u Oracle).
- Internet Information Services 7.0 (o superior).
- URL Rewrite (módulo de Internet Information Services).
- El servidor web debe pertenecer al mismo dominio de Windows que el servidor de aplicaciones.
- Una cuenta de dominio para ejecutar el servicio que utiliza la aplicación y poder acceder a ficheros en unidades de red.
- Un navegador web (utilizado por el usuario final para acceder a la aplicación).
 - o Google Chrome u otro navegador basado en Blink.
 - o Mozilla Firefox u otro navegador basado en Gecko.
 - o Safari u otro navegador basado en WebKit.

Requisitos recomendados:

- Uno de los siguientes sistemas operativos de 64 bits.
 - o Windows Server 2019 o superior.
 - o Windows 10 o superior.
- 12GB de memoria RAM.
- CPU de 4 núcleos o superior.
- Cliente nativo para base de datos (SQL Server u Oracle).
- Internet Information Services 10.0 (o superior).



Requisitos aplicaciones web

- URL Rewrite (módulo de Internet Information Services).
- El servidor web debe pertenecer al mismo dominio de Windows que el servidor de aplicaciones.
- Una cuenta de dominio para ejecutar el servicio que utiliza la aplicación y poder acceder a ficheros en unidades de red.
- Un navegador web (utilizado por el usuario final para acceder a la aplicación).
 - o Google Chrome u otro navegador basado en Blink.
 - o Mozilla Firefox u otro navegador basado en Gecko.

Instalación a medida

Si ninguno de los escenarios detallados anteriormente se ajusta a tu servicio de prevención, podemos buscar alternativas y valorar realizar un despliegue diferente. En este caso, contacta con nosotros y analizaremos la situación.



Requisitos aplicaciones web

Servidor DMZ (Opcional)

Este escenario es complementario de los dos escenarios descritos anteriormente. Si el cliente dispone de servidores web en DMZ para aumentar la seguridad, dicho servidor funciona como proxy inverso: recibe las peticiones de los clientes y las redirige al servidor web interno.

Es decir, en este servidor no se instala el código ejecutable de las aplicaciones web y no es necesario (ni recomendable) que esté en el dominio de Windows, pues no necesita acceso a los recursos del servidor de aplicaciones.

Requisitos mínimos:

- Requisitos mínimos del escenario descrito anteriormente.
- Módulo de IIS [Application Request Routing](#).

Requisitos recomendados:

- Requisitos recomendados del escenario descrito anteriormente.
- Módulo de IIS [Application Request Routing](#).

Subdominio de Internet

Si los usuarios de las aplicaciones web van a acceder a ellas desde fuera de la red corporativa (lo más habitual), se debe configurar un subdominio para acceder a las aplicaciones. Por ejemplo:

- <https://portal.atmedtra.es>
- <https://integra.atmedtra.es>
- <https://sehtraweb.atmedtra.es>

Para esta configuración puede que necesite contactar con su Proveedor de Internet. Asegúrese de confirmar que su router soporta [NAT loopback](#) para que los usuarios puedan acceder a las aplicaciones web a través del subdominio público también desde la red corporativa. De otra forma, tendrá que configurar a resolución de nombres de forma diferente en la red interna.

Certificado SSL

Las aplicaciones web de AT Medtra SL gestionan datos personales definidos por la LOPD como de máximo nivel. Por tanto, se configuran de forma que sólo se puedan acceder por protocolo https.

El cliente asume el coste de solicitar un certificado SSL a una [autoridad de certificación \(CA\)](#) de confianza, así como de los costes de su renovación. El



Requisitos aplicaciones web

cliente se encargará también de su instalación en el servidor web, tanto la primera vez como las sucesivas renovaciones.

El certificado SSL se instala en el servidor web que recibirá las peticiones del cliente. Si no hay servidor web en DMZ, es el servidor web interno. Si hay DMZ, es el servidor web en DMZ. La conexión DMZ-servidor interno también debe darse cifrada, pero en este caso se puede instalar un certificado emitido por la CA del dominio Windows, si existe.

Asegúrese de que el certificado está emitido para el mismo subdominio que ha configurado en el paso anterior. Si utilizamos los ejemplos anteriores, podría ser "portal.atmedtra.es", "integra.atmedtra.es" o "sehtraweb.atmedtra.es". Tenga en cuenta que puede que ya disponga de un [certificado comodín](#) (que protege varios subdominios), por ejemplo "*.atmedtra.es". En ese caso, no sería necesario adquirir uno nuevo.

Cuenta de correo electrónico

Las aplicaciones web de AT Medtra SL envían correos electrónicos a sus usuarios (por ejemplo, el correo de restablecimiento de contraseña). Para ello, se debe configurar una cuenta de correo electrónico genérico (por ejemplo, prevencion@atmedtra.es) que permita estos envíos.

Consulte con su Servicio de Prevención si ya está utilizando una cuenta genérica, para evitar crear una nueva. Para configurar esta cuenta en las aplicaciones web, es necesario conocer:

- El servidor de correo saliente y su puerto.
- El usuario y contraseña (si se requiere autenticación).
- Si el servidor utiliza protocolo TLS/SSL.

Apertura de puertos

Para que los distintos servidores se comuniquen entre sí y para que el servidor web reciba las peticiones del cliente desde el exterior, es necesario abrir puertos en el router o firewall. Es posible que también sea necesario configurar reglas NAT (o [traducción de direcciones de red](#)) en función de su arquitectura de red.

- El servidor web que recibe las peticiones del cliente (ya sea el servidor web interno o el servidor DMZ) debe ser accesible a través del puerto 443 (https).
- Si hay DMZ, debe permitirse la comunicación https entre el servidor DMZ y el servidor web interno.



AT MEDTRA



**Integra
Prevención**



**Portal De
Prevención**



Sehtra

Requisitos aplicaciones web

- El servidor web interno donde se instala la aplicación web debe poder comunicarse con el servidor de correo electrónico, según se describe en el punto anterior. Los puertos concretos pueden variar en cada caso.