Once you've installed a Daminion server, you may be wondering how to access it securely over the Internet.

Fortunately, there are various options available, depending on the level of security and accessibility you require:

- If only a limited number of employees need to access the server's content, and you don't need to share files with external partners, setting up a VPN connection is the safest way to go.
- On the other hand, if you want to share content with external partners or provide guest access, opening ports and setting up secure HTTPS access are the best options.

Note: Regardless of which connection method you choose, it's essential to configure user roles, tags restriction and content access control on both files and folders levels to ensure optimal security..

Let's take a look at both methods and their pros and cons.

VPN

Using a Virtual Private Network (VPN) is one way to protect your data when accessing a private network remotely. A VPN extends a private network across a public network, allowing users to send and receive data as if their devices were directly connected to the private network. The benefits of using a VPN include increased functionality, security, and management of the private network. It also provides access to resources that are inaccessible on the public network, making it a popular choice for remote workers.

Fortunately, almost all small office/home routers come equipped with a built-in VPN server, making it easy to set up a VPN connection. Additionally, you can set up a VPN server on the same computer where the Daminion server is located, providing an additional layer of security for your data.

Learn more about VPN.

Pros:

- Encrypts all traffic between the client and server, making it difficult for hackers to intercept data.
- Allows you to control access to the server by only allowing authorized users with VPN credentials.
- Allows you to configure the server to restrict access to the Internet and only grant access to the VPN connection.
- Generally, offers the highest level of security for accessing the Daminion server over the internet.

Cons:

- Requires additional setup and configuration, which may be challenging for some users.
- Slower connection speed due to the additional encryption and routing of traffic through the VPN server.
- Requires VPN configuration for each user.

Port forwarding

If you have a static IP address, you can redirect the necessary ports on your router to provide access to the Daminion server.

For web access, it's recommended to use a secure HTTPS connection, which you can set up by configuring SSL/TLS certificates. Additionally, to access the Daminion server's desktop interface, you only need to open the appropriate ports through port forwarding.

Pros:

- Easier to set up and configure than a VPN connection: the end users do not need to configure anything.
- Faster connection speeds since traffic is not being routed through a VPN server.
- Allows external partners or guests to access content on the Daminion server without requiring VPN credentials.
- The server can be accessed by the domain name corresponding to your company.

Cons:

- The costs of ensuring the security of the open server can be high.
- Potentially risky if not set up correctly since opening ports may expose the Daminion server to unauthorized access.
- HTTPS requires the purchase and installation of an SSL/TLS certificate.
- Offers lower security than a VPN connection since data is not encrypted end-to-end.

Ultimately, the choice between a VPN connection and port forwarding with HTTPS access will depend on your specific needs for security and accessibility. If you prioritize security over speed and ease of use, a VPN connection is the best choice. However, if you need to share content with external partners or guests and prioritize speed and convenience, port forwarding with HTTPS access may be the better option.

Firewall

To ensure secure access to the Daminion server, it’s important to configure the firewall on both the server itself and the router or other device that provides internet access. Before doing so, you should check with your Internet Service Provider (ISP) to determine which ports are blocked from their side.

For more information on configuring your firewall, please refer here.