



# AppGate Access on Demand

Access-on-Demand is a new feature built into the AppGate Security Server from Cryptzone. This new webservice enables organizations to share internal web-based content on SharePoint or a web server with external users easily and securely, making collaboration much simpler and quicker without compromising network security.

## Overview

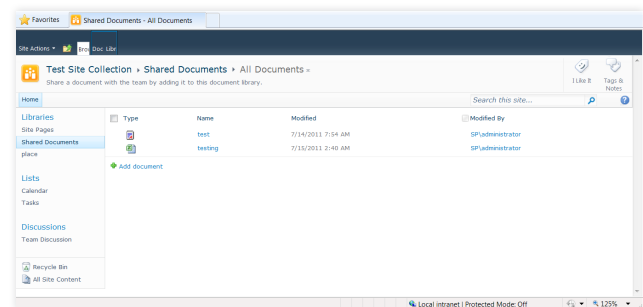
Enabling organizations to collaborate and share information stored on SharePoint and other internal web servers

Companies increasingly need to cooperate and collaborate with external parties. A major challenge they face is how to share information, in particular internal web based content. Many organizations use tools such as Microsoft SharePoint for internal collaboration but these cannot easily be externalized. External collaboration frequently requires duplication of effort as files and folders have to be copied onto external facing servers, or emailed. Even when the problems of accessing internal servers are resolved through the use of proxies or VPN's there remains the issue of internal URL's like `http://myintranet/mydoc.doc` not being recognized when emailed outside the organization.

Access-on-Demand, a new feature in the AppGate Security Server system from Cryptzone, resolves these issues. Access-on-Demand is a webservice that makes it easy for organizations to share internal web based content with external partners and suppliers, whilst also ensuring that other network resources remain secure and protected.

## Externalising information

The AppGate Security Server is an access control solution that enables internal and external users to access protected network resources securely. The AppGate system is usually positioned between the protected resource (services and content on the company network) and the users (who may be working remotely via the Internet). User authentication, authorization and access control is handled by the AppGate system. (For more information about the system please see the "AppGate Security Server" datasheet.)



## Key features and benefits

- **Collaborate without the need for duplicating information:** The Access-On-Demand service enables organizations to use the same URL internally and externally, so that co-workers and partners can share links and information from both sides of the firewall.
- **Automatic feature:** Access-on-Demand is built-in as standard on the AppGate Security Server v10.1.0 or later. There is no need to purchase an additional module.
- **External users seamlessly directed to internal content:** For any predefined Host URL (which is likely to contain many different /path/content combinations such as `http://myintranet/mydoc.doc`)

the new Access-on-Demand feature will be invoked. All matching URL's will always be resolved by the AppGate system and the user log in process initiated. The solution can resolve both `http://` and `https://` URL's.

- **Server access:** Once authenticated, the user connection may be terminated on the AppGate server (proxied) or passed through to the internal server directly depending on your requirements.
- **Single Sign On:** Single Sign-on is available through the Windows Credential Manager. Once authenticated to the AppGate system the user will not be required to re-enter login credentials to access other content that they are authorized to use.

Usually, the user will have prior knowledge of the existence of the AppGate system in order to initiate the secure connection, log in and finally navigate to the required service or content. With the new Access-on-Demand web service, the user requires no prior knowledge of the existence of the AppGate system.

Once a user account has been set up for them, the user just needs the internal URL of the information they want to access on the network, and their login details.

When the user clicks on the URL, the system will present the AppGate login dialogue(s), which the user needs to complete. Internal URL's are resolved automatically and the user is automatically directed to the appropriate service or content. As always, AppGate blocks access to any other online resource that the user is not authorized to use, thus ensuring that corporate assets remain protected from unauthorized access.

AppGate Access-on-Demand Technical Requirements	
<b>AppGate version:</b>	Access-on-Demand requires AppGate Security Server version 10.1.0 or later.
<b>Client:</b>	The solution requires the AppGate Java Web Start (JWS) client so any configurations such as Access Rules must be set to allow the use of this client type.  Users' machine(s) need to have Java installed ( <a href="http://www.java.com/en/download/index.jsp">http://www.java.com/en/download/index.jsp</a> )
<b>Network configuration:</b>	The AppGate Security Server must be located/configured with the users (Internet/outside) on one interface and the protected resources (network/inside) on another interface.
<b>URL resolution:</b>	The URL of the protected resource that is to be shared with external users must be resolvable to a machine on the inside of the network (the actual web server).  The URL of the protected resource must be designated such that it can be published on the outside (so NOT <a href="http://intranet">http://intranet</a> )  The outside DNS entry for the protected resource being shared should point to a unique IP address on the outside interface on the AppGate Security Server for the new Access-on-Demand web service that initiates login.
<b>AppGate Security Server configuration:</b>	If an <a href="https://">https://</a> URL is used then an appropriate root SSL/https certificate must be installed on the AppGate Security Server.  The AppGate Security Server will need to keep its existing IP address and name for users who are not using the Access-on-Demand feature.  If the SSL interface is being used for SSL VPN type access, this cannot be combined with the Access-on-Demand web service, so another IP address may be required.  The AppGate security server and the SharePoint/web server must share a common credential store (AD).

Cryptzone solutions mitigate information security risks identified in four key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

The AppGate solution from Cryptzone enables organizations to provide controlled access for all authorized users regardless of their location whilst also ensuring network resources are protected against internal and external threats. This award-winning technology combines an application layer firewall with device security and granular access control system in one easy to use, cost effective system.

Cryptzone Group AB  
Drakegatan 7,  
SE-412 50 Gothenburg,  
Sweden  
Tel: +46 (0)31 773 86 00

United Kingdom  
Tel: +44 (0)370 013 1600

United States  
Tel: +1.949.279.6177

[info@cryptzone.com](mailto:info@cryptzone.com)  
[www.cryptzone.com](http://www.cryptzone.com)