HOSPITAL PORTAL™ net

Information Tools for HEALTHCARE

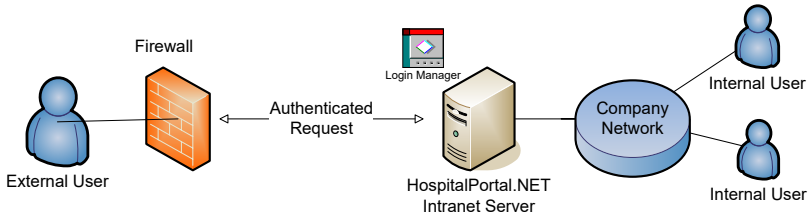
Product Data Sheet for HospitalPortal.net Login Manager™

The Login Manager is a secure mechanism that provides a means to access the internal intranet site running HospitalPortal.net from outside of the organization's firewall. The Login Manager prevents any content of the intranet portal from being accessed by anyone on the Internet without first being required to log in with a valid Intranet user name and password. The internal network users will not be affected by the Login Manager plug-in and will continue to be able to access anonymous content without being required to log in.

Some common scenarios for utilizing Login Manager include:

- Secure employee access to the intranet from home or from another internet location
- Secure access by Satellite offices to the company intranet from a location that is not on the same network
- Secure access by Board of Directors to Board of Directors information published on the intranet
- Secure access by a Partner or affiliated facility to view anonymous content.

SSL security can be applied to the Login Manager to further protect data transmissions. SSL can be utilized for all data transmissions or just the login page.



Technical Overview	The component is designed to allow for secure remote access to an internal portal by blocking incoming web traffic which originated from the Internet (outside of organization's firewall) or even from internal IP addresses or ranges for which you want to require login before exposing the anonymous information. The component uses an ISAPI filter to require authentication before presenting any information including the anonymous content of the site. Using IIS configuration, direct access to certain file types is first passed through a filter that confirms that the user attempting to access the content has already logged in, if the user is not logged in they will be immediately presented with the login screen and will not be able to access any content until successful authentication has occurred. The intranet server remains protected within the company's internal network. The external internet IP address is configured to be proxied and passed through the company's firewall(s) to the internal web server location containing the intranet. Therefore, the web server is protected from many outside threats while still allowing access to the intranet. Since the firewall is opened for port 80(HTTP Traffic) and/or port 443(HTTPS SSL Traffic) threats that come through these ports must still be protected with the proper antivirus, firewall and other tools to truly protect the site/server from attack. The component is configured by specifying an internal IP address or internal IP range denoting the traffic that is reaching the web server from the local network or trusted addresses. Any traffic that arrives at the web server from outside of these addresses must first authenticate before ANY content is displayed. Traffic from the internal network that reaches the web server will not be prompted for credentials and the anonymous view of the intranet will be provided.
Disclaimer	DISCLAIMER: Since the Login Manager is a user authorization and authentication mechanism that utilizes IIS ISAPI filters on the Intranet IIS web server, it will not block unauthorized traffic reaching the IIS server, but rather it filters and prevents unauthenticated and unauthorized external traffic reaching the Intranet site once the traffic reaches the designated Intranet IIS server that hosts the Intranet site. Therefore, it WILL NOT prevent or block potential Denial of Service or other potentially harmful hacking attempts reaching the IIS server. It is highly recommended an appropriate infrastructure, virus and malicious attack defense mechanisms and best practices per current industry standards are implemented by the client to prevent potentially malicious traffic reaching the IIS server when Login Manager is used.