MAS 90®
internet.access Module

White Paper

Sage Software, Inc.

Table of Contents

Introduction to internet.access

The launch of internet.access heralds one of the most significant events in MAS 90 history—the availability of e-commerce business transactions for MAS 90 customers. This product is significant not only because it provides new functionality to help our customers stay competitive, but because it represents the beginnings of a new era for accounting software.

This release of internet.access represents Sage's initial phase in taking MAS 90 technology onto the Internet. The application has been designed so that more functionality can easily be plugged in later in the form of "applets"—little mini-modules of functionality that are controlled by the overall internet.access system, similar to the way MAS 90's Library Master module controls the other accounting applications today.

Due to the nature of the target audience best served by the MAS 90 product line, the IT modules will initially focus directly on allowing MAS 90 user companies to do business with their clients over the Internet. IT addresses the middle ground of allowing clients of a MAS 90 user company to perform account inquiry and order entry functions in a secure, Web-based environment.

The internet.access module takes Internet accessibility to the next level, allowing MAS 90 end-users to interact with MAS 90 data over the Internet, and enabling their customers to do the same.

Overview

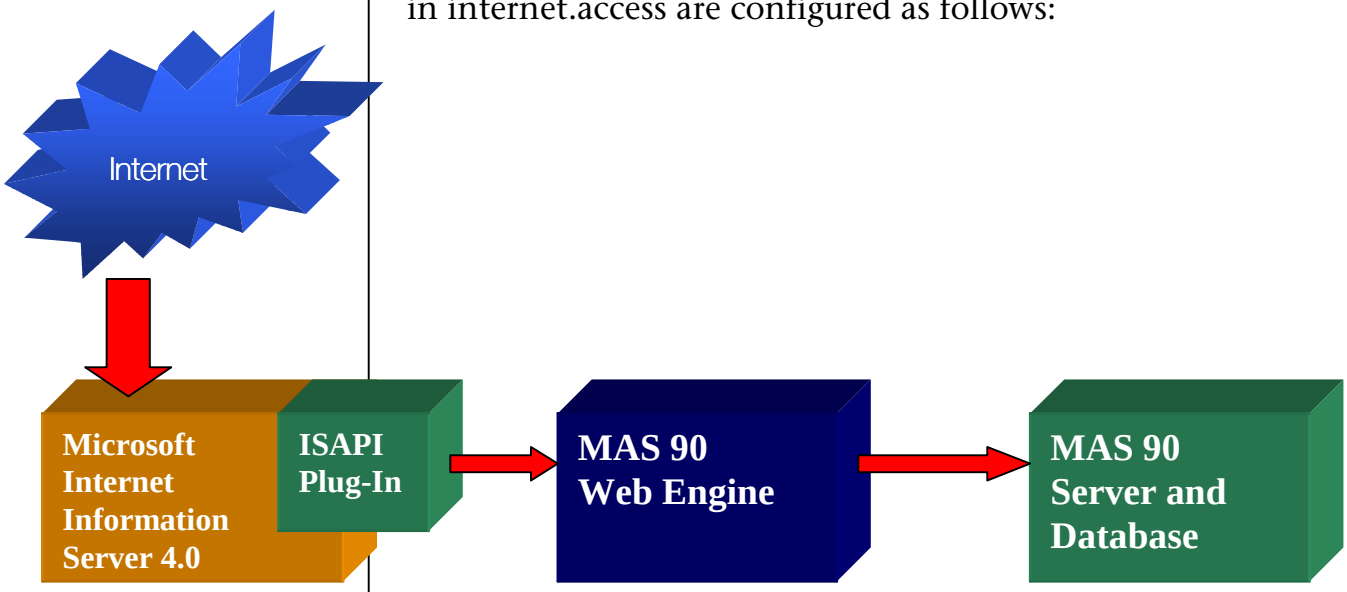
internet.access capabilities currently consist of a core internet.access system module, a customer inquiry applet (internet.inquiry) which allows for account and order inquiry capabilities, some account self-maintenance and a shopping cart applet (internet.order) which facilitates order entry.

Future internet.access enhancements will include additional functionality in the form of new applets, such as business to consume, field sales and vendor purchasing.

internet.access is currently compatible with MAS 90 for Windows® on the Microsoft® Windows NT® platform, and with MAS 90 Client/Server operating in the Windows NT and UNIX environments. The only Web server supported at this time is Microsoft Internet Information Server 4.0 (IIS).

internet.access Technology

The internet.access module is made up of a number of different technologies. Rather than build a unique, proprietary Internet application, internet.access takes advantage of existing technologies, allowing for maximum integration with an existing user's configuration. The three different servers that are utilized in internet.access are configured as follows:



The internet.access module will install components to each of these "servers." For optimal performance, each server should be hosted on its own machine. However, users may choose to install the MAS 90 Web Engine and the MAS 90 server on the same box. From both a security and performance standpoint, it is strongly recommended that Internet Information Server be installed on its own machine. Each of the servers is described in more detail below.

Internet Information Server (IIS)

This Web server is accessible from the Internet. Users access this server through a URL reserved for the MAS 90 end-user company. Many users will already have a Web site configured. If they are using IIS, they do not need to purchase any additional hardware or software. If they are using another Web server, such as Apache® or Netscape®, they will need to configure a second server that is running IIS, or migrate their existing content to IIS.

internet.access installs an ISAPI plug-in to IIS. ISAPI is the interface used to integrate custom applications with IIS. The plug-in's function is to intercept internet.access commands (requests for Web pages, posting data to the server, etc.) and re-direct them to the MAS 90 Web Engine. IIS will call the plug-in whenever it finds a link with the extension of (.PVX).

The ISAPI plug-in to IIS directs Internet requests for Web pages to the MAS 90 Web Engine.

The ISAPI plug-in supports POST and SEND commands only. POST is used to request a Web page. SEND is used to send information from the Web page to the server for updates. Subsequently, the returned HTML stream is processed by the ISAPI plug-in to correct any information needed as part of the redirection. The HTML stream is then posted back to the user through IIS.

Figure 1, located at the end of this document, shows an overview of how the ISAPI plug-in operates. IIS handles all the functionality of the Web site. A good working knowledge of IIS is required to maintain the Web site and integration with MAS 90 internet.access. IIS provides Secure Sockets Layer (SSL) encryption so that pages can be transmitted to users securely. IIS can also provide integrated security for the Web site and File Transfer Protocol (FTP) access for uploading and downloading large data files. These features function independently of the MAS 90 internet.access module, but make the Web site more functional.

MAS 90 Web Engine

The MAS 90 Web Engine dynamically builds Web pages and populates them with data directly from MAS 90 data files.

The server running the MAS 90 Web Engine may be simply referred to as the Web Engine. The internet.access Web components are installed on this server, and this is where HTML files merge with MAS 90 data to form a dynamic Web page. These are served back to the user through IIS. There is no user interface associated with this server. It is only responsible for servicing and merging Web requests between IIS and the MAS 90 server.

A request comes into the Web Engine from the Internet via a standard port defined in the MAS 90 Web Engine configuration program. The request is then queued up until a Task Handler is available to process the request. The Task Handler informs the Web Server that it can handle a request and process it. Most requests will make calls into the MAS 90 internet.access programs.

The Web Engine obtains information from the MAS 90 database and creates the HTML files, which are re-routed back to the user. When completed, the Task Manager becomes available to handle another incoming request. While this is running, other requests can come in to the Web Engine, which are routed to Task Manager as they become available.

Please refer to Figure 2, located at the end of this document, to see an overview of the MAS 90 Web Engine and how the functions of MAS 90 integrate with it.

MAS 90 Server

This is the server where MAS 90 and the MAS 90 data files are located. If the data files are in an alternate directory on another server, the MAS 90 server and the MAS 90 Web Engine must have the appropriate permissions to access that server and its data files (read and write). The internet.access host components are installed on this server, and from here, users can configure their Web sites for integration with MAS 90 data.

From an installation perspective, users can install the MAS 90 Web Engine and the MAS 90 server to the same physical box. The installation routines will be distinct and both need to be run, even if they are being installed on the same server.

Security and Considerations

For maximum security, all access to sensitive data is through a single port in the firewall.

Obviously, security is first and foremost when talking about e-commerce. Security issues relating to e-commerce are not much different in concept than security issues have always been. At the most basic level, you want to make sure that you keep everyone away that could potentially cause problems with your Web site. You want to give everyone just enough permission to be able to access the data they need, and nothing else.

To maintain security for the MAS 90 data, both the MAS 90 Web Engine and MAS 90 server are located inside the firewall, where only authorized, authenticated users can access them. The Internet Information Server is placed in what is commonly known as the "DMZ" or "demilitarized zone," a location inside the firewall that Internet users can access, but does not allow access to other servers on the user's network. Refer to Figure 3 at the end of this document for a graphical representation of how a typical firewall is configured.

The ISAPI plug-in opens a port through the firewall to the MAS 90 Web Engine. Incoming requests and outgoing generated Web pages pass through this port between the internal network and the IIS server.

Users need to configure their firewalls to allow for this single port to be open from the IIS server's IP address. This allows IIS access to data behind the firewall, but does not open the possibility for hackers or other unauthorized users to gain access to sensitive internal data. The public can access the user's standard Web page. From there, links can be created to connect registered users to a MAS 90 internet.access login page, which gives them access to their account. Using IIS, users can create elaborate Web sites with standard third-party Web development tools, and provide links to internet.access.

You should exercise caution when using an HTML editor to modify the internet.access templates. Some editors may try to

correct your formatting, and use of these editors may produce unexpected results. You should always create a backup of your templates before making any changes – and then thoroughly test all changes to make sure they work correctly.

For a good introduction to Microsoft security, refer to http://www.microsoft.com/security/new.asp.

Hosting a Web site with an ISP is the easiest method of implementing the internet.access module.

Hosted and Non-Hosted Configurations

The Web site can be hosted at the end-user's site or with an Internet Service Provider (ISP). If the Web site is hosted, the IIS box resides at the ISP location instead of the client site, and the ISAPI plug-in must be installed on the ISP's IIS server. A dedicated line with sufficient bandwidth must be installed between the ISP and the end-user site.

Although the bandwidth requirements for internet.access are minimal (pages should not be larger than about 4K), the IIS box located at the ISP must be able to access the MAS 90 Web Engine located at the client's site on demand. If the connection is not available, users will not be able to access their account on the MAS 90 server.

Careful consideration must be given to all factors to ensure that adequate bandwidth is in place. The bandwidth requirements depend on many factors, including traffic volume and the size of graphic files. The recommended minimum for a hosted configuration is 128K of bandwidth, but depending on traffic, more could be required.

For the majority of end-users, the hosted configuration will be the most desirable. It can allow the end-user to install internet.access without the need for expensive Web consultants. In fact, a "hosted" implementation of internet.access may be accomplished with little more effort than installing and setting up any MAS 90 module. All issues regarding firewall setup and installation of a dedicated line for access to the Internet can be coordinated with the ISP to ensure that a secure and efficient solution is implemented.

A non-hosted configuration will work best for end-users who currently have most of the pieces already in place, such as their own Web site and firewall. Special consideration should

be given to ensuring that the firewall setup is comprehensive enough to provide the end-user with the best possible security. Figure 3, at the end of this document, shows all the pieces and how they interact.

Hardware and Software Requirements

Microsoft Internet Information Server 4.0:

- Windows NT Server 4.0 with Service Pack 5.
- Internet Information Server 4 (from Windows NT 4.0 Option Pack).
- Refer to IIS documentation for additional requirements. No additional resources are required to run ISAPI plug-in.

Web Server:

- Pentium® Processor running 166 MHz or faster.
- Windows NT Server 4.0 with Service Pack 5.
- 128 MB RAM.

(Requirements change based on users' needs. To achieve better performance, users may need to upgrade to faster processors or add additional RAM. Consult an authorized MAS 90/Windows NT reseller for a list of requirements based on your individual needs.)

Supported Browsers:

- Microsoft Internet Explorer 4 or above.
- Netscape 4.5 or above.

Certification Training

MAS 90 resellers planning to sell IT must meet the following requirements before they will be authorized:

1. The following Microsoft certification exams will need to be passed by the class attendee *before* attendance at Sage's MAS 90 internet.access class:

    1.1 Windows NT 4.0 (Exam 70-067).

    1.2 TCP/IP (Exam 70-059).

    1.3 Internet Information Server 4.0 (Exam 70-087).

    We also highly recommend Windows NT 4.0 Enterprise (Exam 70-068).

2. Attend Sage MAS 90 internet.access class, and receive a passing grade on the assessment test.

3. Must have a Web site (hosted or on site).

    3.1 Prefer internet.access running on reseller Web site on site (as opposed to hosted by an ISP).

Recommended Reading

Microsoft Certified Professional – MCSE+I Requirements:
http://www.microsoft.com/mcp/certstep/mcsein.htm

Microsoft Internet Information Server:
http://www.microsoft.com/ntserver/web/default.asp

Microsoft Security Advisor:
http://www.microsoft.com/security/default.asp

Glossary of Terms

Throughout this document, there are several references to technical terms which may not be familiar to people not used to working with the Internet.

Industry Terms

The following is a list of common terms encountered when dealing with applications integrating with the Internet, or the Internet in general.

Internet – A collection of switches located around the world that connects the world through a common protocol (TCP/IP). The Internet is not owned or managed by a single corporation or entity, but by the community as a whole.

Intranet – A term used to define a corporate infrastructure based around the TCP/IP protocols (as opposed to IPX/SPX or NetBEUI). The corporate intranet is accessible only from within the corporation via LAN, or through a direct-dial connection.

Extranet – A term being used to define the extended corporate infrastructure, connecting remote sites up to the internal intranet through the Internet. Connections in the extranet are secure and encrypted.

HTML – HyperText Markup Language. The language of the Internet used to create platform-independent Web pages.

ISAPI – Information Server Application Programming Interface. A collection of functions that provides an interface with IIS.

Firewall – A device used to prevent unauthorized access from the Internet to a corporate Intranet, but which allows people inside the firewall to access the Internet. Firewalls can be hardware- or software-driven. A software-driven firewall is called a Proxy Server.

SSL – Secure Sockets Layer. A mechanism to send Web documents over a secure network socket and a public encryption key. Data is encrypted to prevent hackers from viewing sensitive information (such as credit card numbers, etc.). All current browsers (IE 4, 5, Netscape 4) support SSL without any additional software or configuration.

MAS 90 Terms

The following is a list of terms used throughout this document relating to the internet.access product.

IT – The two-character module code for internet.access.

Applet – A collection of Web templates that perform a series of functions. Applets are designed to be distinct units that can be sold individually. However, some applets may require other applets to function properly.

Template – An HTML file that has been marked with ProvideX tokens and is replaced with data objects when merged.

Figure 1. MAS 90 ISAPI Plug-In

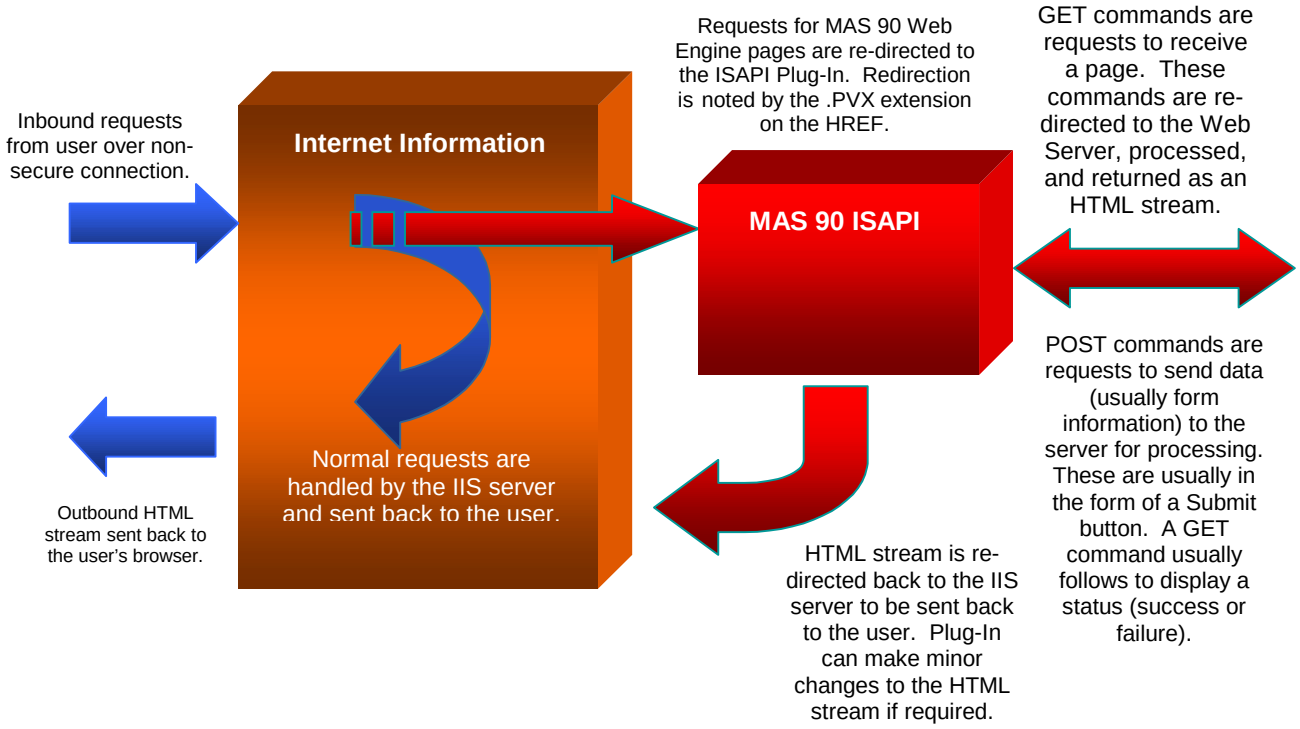


Figure 2. MAS 90 Web Engine

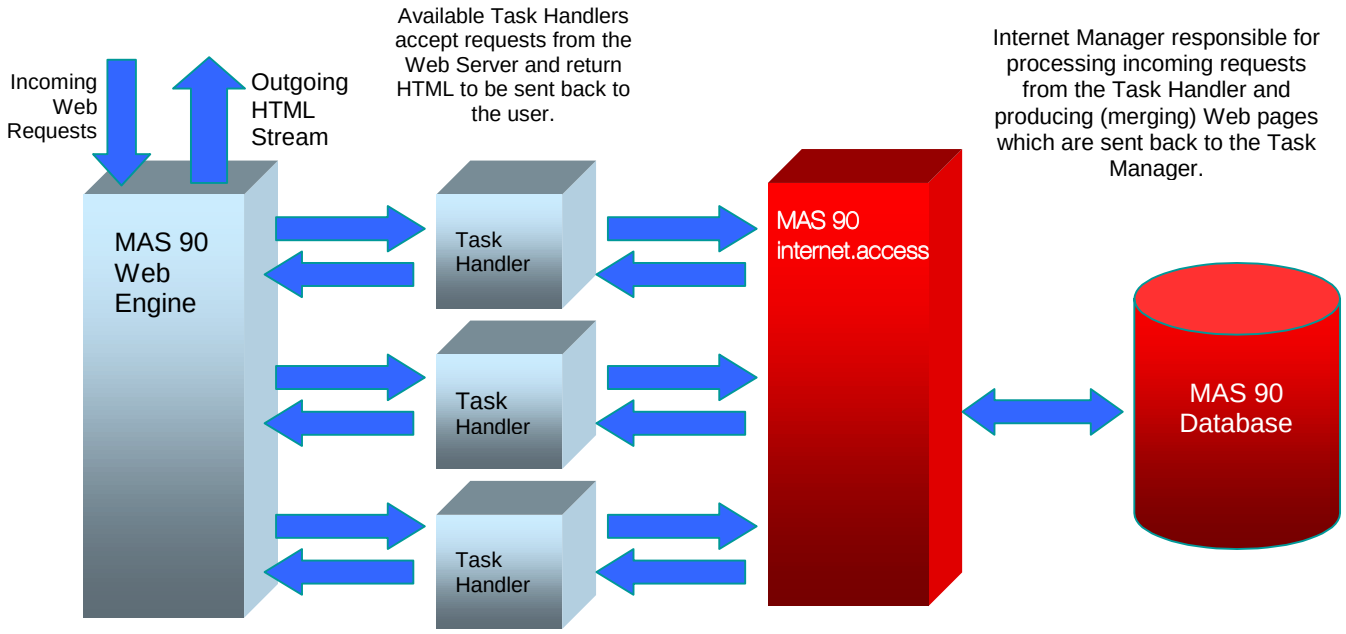
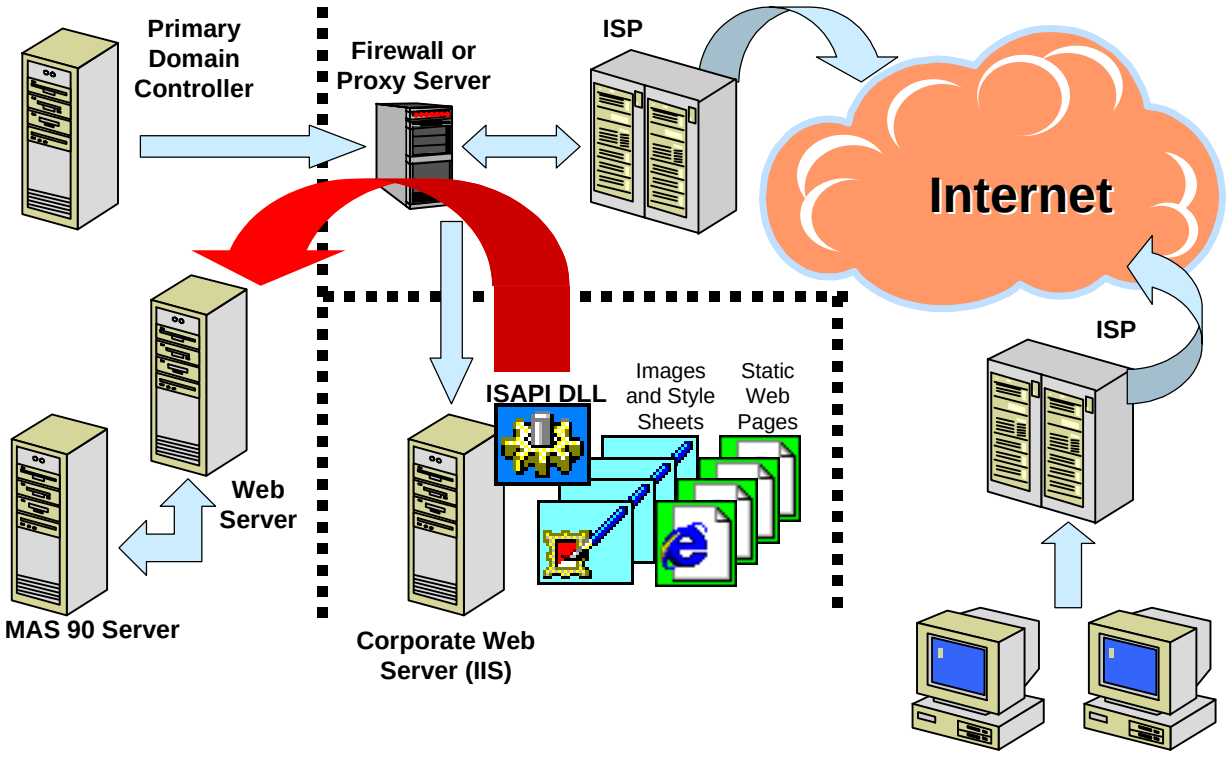


Figure 3. Putting It All Together



56 Technology Drive
Irvine, CA 92618-2301
800-854-3415
www.sage.com

99-1508 11/99