

## [Intelligent Application Gateway \(IAG\)](#)

### Intelligent Application Gateway Frequently Asked Questions

Published: February 1, 2007

Learn more about Microsoft's Intelligent Application Gateway (IAG) 2007 by reading answers to frequently asked questions. Discover how IAG 2007 can help you control user access, protect IT assets, and safeguard business information.

---

#### Q. [What is Intelligent Application Gateway 2007?](#)

- A. IAG 2007 with Application Optimizers provides secure socket layer (SSL) virtual private network (VPN), a Web application firewall, and endpoint security management that enable access control, authorization, and content inspection for a wide variety of line-of-business applications. Together, these technologies provide mobile and remote workers with easy and flexible secure access from a broad range of devices and locations including kiosks, PCs, and mobile devices. IAG also enables IT administrators to enforce compliance with application and information usage guidelines through a customized remote access policy based on device, user, application or other business criteria. In particular, IAG 2007 provides:
- Access solutions that are better integrated with business applications
    - Application-centric, policy based access with granular Web application firewall security and controls
  - Easy to use, secure network and application access
    - To more business resources and data from more locations
    - From more devices, managed and unmanaged (for example, Smartphones, PDAs, and kiosks)
    - Automated tools that simplify configuration while helping maintain a secure deployment
  - Integrated security with application protection
    - Helps IT administrators ensure the integrity and safety of network and application infrastructure
    - Blocks malicious traffic and attacks, with client-side security checks and clean-up
  - Comprehensive policy enforcement
    - Provides the IT group greater asset and access control
    - Enables businesses to comply with legal and regulatory guidelines on information usage to limit exposure and liability

#### Q. [What's new in IAG 2007?](#)

- A.** Integrated with Microsoft Internet Security and Acceleration (ISA) Server 2006, IAG 2007 delivers a single, consolidated appliance for network perimeter defense, remote access, and application-layer protection over both SSL and IPsec connections, providing businesses with a broader set of choices for their remote access requirements. Integration of SSL VPN into existing Microsoft infrastructure supports secure access to both Microsoft and non-Microsoft applications and services from a single appliance.

IAG 2007 features a new streamlined and cost-effective design that can help lower cost of ownership and removes the need for multiple devices from multiple vendors for different access methods. In addition, all Intelligent Application Optimizers and Connectivity Modules are now included with the base product offering, further simplifying the purchase and deployment process. Your corporate IT group can adopt a consolidated security appliance solution that is flexible and easy to deploy.

**Q.** [Who should consider IAG 2007, and when should I choose IAG 2007 instead of ISA Server 2006?](#)

- A.** Your choice of access mechanism should be dictated by both business and security needs.

Microsoft's goal is to provide a broad solution that can easily adapt to a variety of usage and deployment scenarios. For example, if you are looking for a network-edge gateway that provides fast and secure access with both IP-level filtering, domain-independence and IPsec VPN granular access policy and quarantine, you may choose to deploy ISA Server alone. If, however, you need to improve remote worker productivity by providing access to a range of line-of-business applications from behind existing security infrastructure, or if you need to provide business partners and customers access to applications and resources from unmanaged endpoints and networks, then IAG 2007 plus ISA Server 2006 should be your choice. For more detailed information on differentiating between ISA Server and IAG, read the [secure remote access scenario](#).

Buy ISA Server when you need:

- Branch office gateway for site-to-site connectivity and security
- Data center Internet access control and Web caching
- Advanced security with inbound and outbound firewall
- Publishing, securing, and pre-authenticating access to specific Web services such as Microsoft Exchange Server and Microsoft SharePoint Server (when more advanced client options aren't required)
- Full network connectivity for managed PCs (via VPN)
- High-security client access via Windows 2000 or Windows XP that needs host checking and quarantine and IPsec (or other) encryption and authentication

Add the Intelligent Application Gateway when you need:

- Browser-based clientless access with granular policy control of data and application

components

- More advanced security and manageability control over the client when accessing Web- and non-Web-based resources
- Remote access to a broader range of third-party and line of business applications
- Access from unmanaged PCs or mobile devices on unknown networks
- Strong end point security verification
- No IPsec VPN clients available for the target host platform
- Extend policy-based access to partners and customers

**Q.** [How does IAG 2007 compare with other similar solutions on the market today?](#)

**A.** [IAG has been recognized by industry analysts and the press](#) as possessing a market-leading design by combining broad access capabilities, comprehensive Web application security, and endpoint security management into a single solution. Features such as [Intelligent Application Optimizers](#), which include predefined application-specific policies and security for many enterprise applications (such as Exchange Server, SAP, Lotus Domino, and others) enable IAG 2007 to provide a level of protection and customization that no other solution on the market currently offers. With the integrated network-layer firewall services of ISA Server 2006, IAG 2007 delivers a single, consolidated appliance for network perimeter defense, remote access and application-layer protection, providing customers with a broader set of choices for their remote access requirements.

**Q.** [How can I buy IAG 2007?](#)

**A.** IAG 2007 is available now as an appliance through our [OEM partners](#).

While each OEM sets the exact configuration and pricing details of their own product offerings, Microsoft has instituted a new pricing and licensing structure to make it easier and more cost effective to deploy an SSL VPN in your organization.

IAG 2007 now aligns with Microsoft's broader server and tools licensing schemas, with a server CAL model. This means you purchase the server or appliance from an OEM (as you do today with ISA Server appliances), and CALs are sold separately for each named, authenticated user. To find out more, please visit the [How to Buy page](#).

The non-volume license price for a single CAL is \$22 (USD), with volume discounts applying at higher purchase or contract levels such as Open/Select and Enterprise Agreements.

**Q.** [Where can I get more information about IAG 2007?](#)

**A.** Please read the [IAG 2007 Product Overview](#) for a detailed summary of IAG's features and

functionality. You can also read about deployment and usage scenarios for [secure remote access](#) solutions, and evaluate the software on the [trial software](#) page, which includes links to live online demos and downloadable test environments.

**Q.** [Will I receive a free upgrade \(from older Whale Communications eGap appliances\)?](#)

**A.** Existing customers with current service and support contracts will be provided with a migration path. Those without maintenance agreements will need to purchase new appliances and CALs.

**Q.** [Will there be new or updated appliances running IAG 2007?](#)

**A.** Yes, we are working with OEM partners to deliver IAG 2007-based appliances. Please go to our [OEM partners](#) page for more information.

**Q.** [How and where do I deploy IAG 2007?](#)

**A.** IAG provides granular access control, policy enforcement, application protection, and endpoint security management, yet delivers a cost savings advantage since businesses can adopt a consolidated security appliance solution that is flexible and easy to deploy. The following table elaborates on specific uses you may have for a comprehensive secure access gateway.

Scenario	Definition	IT Tasks
<a href="#">Secure Application Access</a>	Employee access from managed endpoints to Exchange Server, SharePoint Server, file shares, and other intranet resources through a policy-defined application-layer connection.	<ul style="list-style-type: none"> <li>• Enforce policy controls on actions within an application.</li> <li>• Protect my infrastructure from malicious Internet traffic.</li> <li>• Provide an easy to use, customizable portal.</li> </ul>
<a href="#">Customizable Enterprise Security</a>	Employee and partner access from unmanaged endpoints to extranet Web and client/server applications with restrictive policies defined by endpoint state.	<ul style="list-style-type: none"> <li>• Enable access to internal resources from unmanaged endpoints.</li> <li>• Enforce granular access based on endpoint</li> </ul>

		profiles.
<a href="#">Granular Information Protection</a>	Access from diverse endpoints to Internet-facing Web applications and data with deep content inspection (WAF) and session-state cleanup.	<ul style="list-style-type: none"> <li>• Enable partners to access relevant information on my network.</li> <li>• Ensure network integrity by restricting access based on endpoint profile.</li> </ul>

**Q.** [Can I purchase IAG 2007 directly?](#)

**A.** No, at this time IAG 2007 is sold only as an appliance through our [OEM partners](#).

**Q.** [What happened to AirGap?](#)

**A.** ISA Server, combined with IAG 2007, serves the need for network separation and full control of inbound and outbound content and adds significant edge security functionality to address a broad set of customer requirements. The consolidated appliance provides a flexible software-driven solution that is responsive to the need for performance, management, and scalability in addition to comprehensive security. The blending of stateful packet filtering, circuit filtering, application-layer filtering, Web proxy, and endpoint security into a single appliance affords the administrator with a variety of options for configuring policy-driven solutions for access to applications and network resources.

ISA Server delivers the ability to filter traffic rather than rely on a mechanistic solution, providing three types of firewall functionality: packet filtering (also called circuit-layer), stateful filtering, and application-layer filtering. The ability to apply rule-based filtering to all traffic that traverses the network boundary enables the combined solution to directly address threats such as worms or malware that may originate from authenticated users.

The solution combines ISA's robust IPsec and firewall security features, content inspection capabilities and Web caching features with IAG's full-featured application-layer SSL VPN, endpoint compliance, and application security functionality to provide a cost-effective integrated network protection and remote access solution providing superior inbound and outbound security.