Intelligent Application Gateway Key Features

Published: February 1, 2007

The following table provides an overview of the key features of Microsoft's Intelligent Application Gateway (IAG) 2007.

Scalability	
Users	Supports large numbers of users on a single gateway.
High availability	Scales linearly with up to 64 high-availability node configurations.
Manageability	
Flexibility	Delivers out-of-the-box software configurations for widely-deployed enterprise applications, as well as customization capabilities including authentication, authorization and endpoint compliance profiles, and context-sensitive Web portals. Supports positive-logic rule sets and URL filter customization, and has the ability to develop rule sets for customized or proprietary applications.
SSL VPN portal	A secure socket layer (SSL) virtual private network (VPN) portal enables a convenient single access point for applications, yet supports multiple access points with distinct policy parameters such as partner extranets and employee portals on a single gateway.
Logging and reporting	Supports monitoring, logging, and reporting for integrated management and accounting (system, user security, and session views): ● Event Monitor provides comprehensive event monitoring by user, application, and time period. ● Integrated Event Logger that records system usage and user activities, and sends alerts about security events to an administration console. ● Integrated Event Query tool with preconfigured query templates and full reporting capabilities.
Comprehensive policy framework	● Out-of-the-box application access settings and endpoint policy configurations designed to ensure minimal integration overhead and low ongoing management costs. ● Supports Intelligent Application Optimizer Toolkit for defining positive-logic rule sets, URL filters to supplement Optimizer settings and to develop policies for customized or proprietary applications. ● Supports Intelligent Application templates that provide a framework to build an Application Optimizer for both generic Web applications and complex enterprise applications incorporating components, Web parts and objects.
Access Policy	

Endpoint compliance checks	Endpoint policy allows administrators to define compliance checks according to out-of-the-box variables including presence of security software and IAG-specific components such as Attachment Wiper. Supports complex endpoint policy rules with customizable compliance checks using Boolean operations.
End user experience	• Delivers a highly-customizable SSL VPN portal and login pages to enable easy set up and low administrative overhead.
	• Supports comprehensive portal and login page customization to replicate existing intranet.
	• Does not require conformance to a vendor portal template.
Integrated certificate authority management	Provides a built-in certificate authority in the event the administrator chooses not to use an external certificate authority. Enables administrators to grant a user a trusted endpoint certificate for a specific machine on request.