Alcatel-Lucent OmniAccess 8550 Web Services Gateway

The Alcatel-Lucent OmniAccess™ 8550 Web Services Gateway (WSG) protects sensitive information from misuse satisfying regulatory compliance requirements and makes business process data available when and where it is needed. The OmniAccess 8550 WSG provides a corporate wide compliance infrastructure for secure automated business processes within a company and among its partner organizations. The OmniAccess 8550 WSG is a service oriented network appliance that reduces the traditional complexity and cost of securing internal corporate and business-to-business (B2B) automated business processes.

The OmniAccess 8550 WSG, based on the Alcatel-Lucent Web services run-time message inspection technology, provides a scalable and reliable service oriented infrastructure for information system in such areas as human resources, enterprise resource planning (ERP), customer relationship management (CRM), and finance with security and regulatory compliance (policy enforcement and audit trail) that is required for secure business process automation. It is deployable within data centers to secure business processes within an organization and in the DMZ for automating business processes with partners. The OmniAccess 8550 WSG provides a significant competitive advantage by reducing IT system total cost of ownership (TCO).

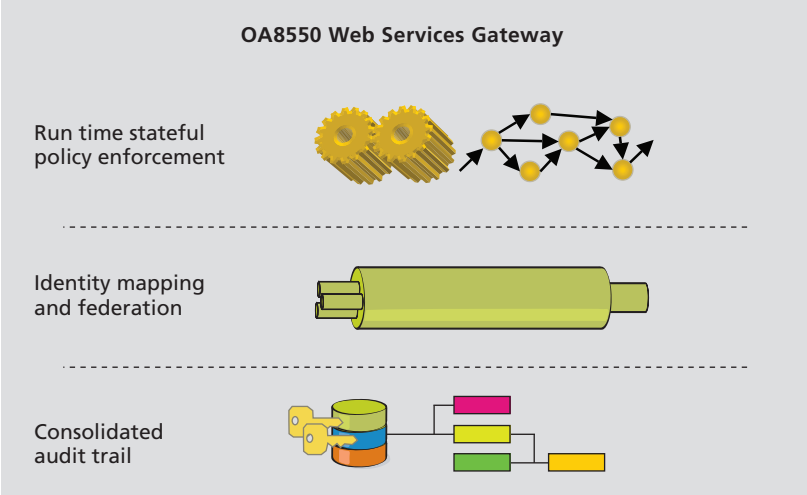
Product Features

The deployment of an OmniAccess 8550 WSG provides corporate-wide security and regulatory compliance so organizations can secure automated business processes to meet increased government regulations and safely automate business processes with partners, creating a secure automated partner ecosystem. With the OmniAccess 8550 WSG securing business processes, highly skilled employees have access to information whenever they require it, even when at a partner site.

The OmniAccess 8550 WSG also provides unique, stateful (multi-transaction), run-time policy enforcement and consolidated audit trails to ensure and demonstrate compliance with government regulations (see Figure 1). The OmniAccess 8550 WSG also has the ability to mitigate risk through consistent policy enforcement across information systems with a user contextual knowledge of system events. To protect private data, the OmniAccess 8550 WSG provides information access and change control as well as data encryption with digital signatures. This enables a single digital identity within an organization that accepts authentication from trusted partners—the foundation for a consolidated corporate-wide access policy.

Secure B2B processes are further enhanced by the OmniAccess 8550 WSG through security features such as the application firewall and auditing, tracking and control functions that can be used to monitor all partner activity, including access to information by partner employees when on-site.

Figure 1. Core OmniAccess OA8550 WSG features

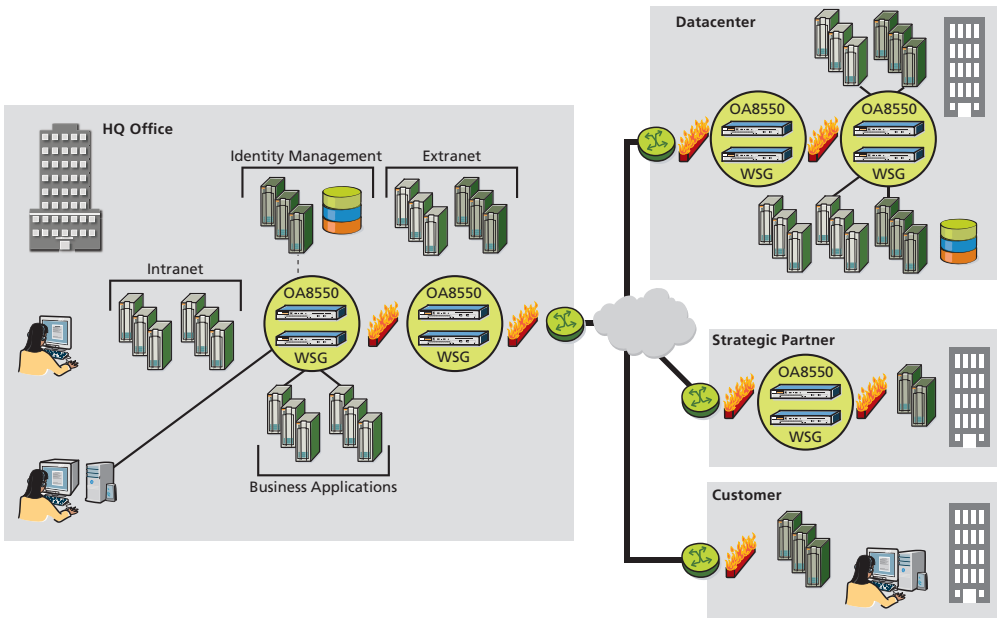


Deployment architecture

The OmniAccess 8550 WSG is designed to be deployed in the DMZ of an organization to secure business process automation with partners (see Figure 2). The OmniAccess 8550 WSG is typically installed behind the IP firewall and provides service virtualization as well as key security functions to protect the internal domain and ensure data security.

Alternatively, the OmniAccess 8550 WSG can be installed in the data center to secure business processes within the organization. It allows information access policy to be consistently enforced at run time across information systems and can demonstrate regulatory compliance through a user centric consolidated audit trail. Risk is mitigated with the proper controls and monitoring points in place as well as through consistent policy enforcement across information systems with a user contextual knowledge of system events.

Figure 2. Typical OmniAccess 8550 WSG network deployment



Feature group	Benefit	Feature	Feature description
Security & governance	Ensures compliance with corporate governance policy and government legislation	Application sessions	Stateful model for Web service run-time policy
		Stateful run-time policy enforcement	Run-time policy enforced across multiple transactions per credentialed user
		User-centric audit trail	Consolidated audit trail capturing each information record viewed or modified per credentialed user, encrypted and signed to survive legal audit
		Application access control	Stateful policy enforcement on access to individual Web services
		Information access control	Stateful policy enforcement on access to individual information records
Secure online B2B	Enhanced security through single point of control to enable secure automated workflow among business partners	Partner authentication	Strong authentication for partner institutions (X509, XKMS, RSA, 3DES, DES, AES, SHA, PKCS, CRLs, OCSP)
		Service virtualization	Map external URL used by partners to private internal URL
		Secured proxy point	Stateful policy enforcement with cross-referenced audit on all partner activity
		Data protection	Data encryption and digital signing to survive legal audit
		User mobility	Enables end users to seamlessly connect to web services at any partner site
		Multiple partner groups	Allows web services to be offered to distinct partner groups
Identity mapping & federation	Consistent enterprise-wide enforcement of policy per credentialed user	Single identity	Dynamic identity translation allowing access to multiple IT systems with single credential for corporate-wide consistent policy enforcement
		Identity interoperability	Enables acceptance of user validations from partners while meeting all traceability and user privacy requirements (SAML, WS-Trust)
		Integration with existing identity infrastructure	Integrates with existing identity management infrastructure (LDAP, SAML, WS-Trust)
Corporate agility	Enables scaleable and reliable re-use of existing IT systems	Application interoperability	Provides mediation through message and content translations for applications (XSLT)
		Web service load balancing	Provides round robin load balancing with session stickiness and automatic failover
		Reliable messaging	Provides policy-controlled, guaranteed delivery of web service messages
Threat protection & XML firewall	Protects from deliberate attacks and malicious XML messages	XML message validation	Ensures all messages are well formed
		XML message control	SQL Injection, Recursive Payload, Oversized Payload, Buffer Overflow, External Entity Attacks, Oversize Attachments, Cross Site Scripting
		Denial of service (DoS) protection	Prevents DoS attacks focused at web services, replay attacks
Management	Easily managed appliance integrating with existing management platforms	Fault management	SNMP reporting to enterprise network management platforms
		Configuration management	Provides Web-based GUI interface with role based management control
		Change management	Enforces policy and configuration privileges by role and provides audit of all policy and configuration changes
Secure hardware accelerated appliance	Hardened appliance to comply with security standards	High availability	Provides automatic stateful failover for paired nodes
		Open standards compliant	Compliance with Web services standards W3C, SOAP, UDDI, WS-Policy, WS-Trust, WS-Security, WS-Reliable Messaging, WS-Addressing
		Secured appliance	No direct operating system access - encrypted hard drive - no internal devices allow for alternate re-boot of system - all ports disabled - configuration files digitally locked.
		Dedicated Web services infrastructure	Hardware accelerated XML parsing & encryption with digital signing & SSL & HTTPS

Technical specifications

System configuration

The Alcatel-Lucent OmniAccess 8550 WSG is a high–performance, 2U, rack-mountable network element consisting of:

- Two Quad-Core Intel E5345 Xeon processors (2.33 GHz, 80 watts, 1333 FSB), each with 8 MB of L2 cache
- 8 GB of CPU memory with advanced ECC (multi-bit error) protection
- 146 GB hot-pluggable hard drives with RAID1 SAS disk array
- Fully redundant power supplies
- Fully redundant fans
- Six 10BaseT/100BaseTX/1000BaseTX network interfaces that support bonding for redundancy
- Built-in high-performance SSL/TLS and crypto-graphic hardware
- Built-in high-performance XML processing hardware
- Front panel hardware alarm indicators
- Includes universal rail kit for 19-inch racks

Physical dimensions

- Height: 3.38 in. (8.59 cm.)
- Width: 17.54 in. (44.54 cm)
- Depth: 23.65 in. (60.07 cm)
- Weight: 60 lb (27.22 kg)

Power Specifications

- Input (per power supply)
  - ¬ Line voltage: 100 VAC - 132 VAC
200 VAC - 240 VAC
  - ¬ Input current: 3.3 A (at 120 VAC)
2.3 A (at 220 V AC)
  - ¬ Input power: 370 W (at 120 VAC)
470 W (at 220 VAC)
- BTU rating max: 1272 (for 120 VAC)
1610 (for 220 VAC)

Standards compliance

- WSRM 1.1
- WSS 1.0
- WSS-Signature
- WSS-Encryption
- WS-Trust
- WSSE 1.0
- WSDL 1.1
- SOAP 1.1/1.2
- XSLT 1.0
- XPath 1.0
- UDDI 3.0
- HTTP 1.0/1.1
- TLSv1/SSLv3
- DES, 3DES, AES, RC4, SHA-1, MD5, PKCS #10, X.509, RSA, DSA
- LDAP 3.0
- SAML 1.1
- SNMP
- SFTP
- IEEE 802.3, 802.3u, 802.3ab

Regulatory

EMC	
ICES-003	Interference causing equipment standard for digital apparatus
FCC Part 15 Class B	FCC rules for radio frequency devices under FCC 15 of the rules of FCC
EN55022, Class A/B	Information technology equipment (ITE) - Radio disturbance characteristics - Limits and methods of measurement - Class A/B
EN55024	ITE - Immunity characteristics - Limits and methods of measurements
CISPR 24	ITE - Immunity characteristics - Limits and methods of measurements
AS/NZS CISPR22	Limits and methods of measurement of radio disturbance characteristics of information technology equipment

Safety	
CAN/CSA C22.2 No 60950-1-03 / UL 60950-1	ITE - Safety - Part 1: General Requirements
FDA 21 CFR 1040	Performance Standard for Light-Emitting Products
IEC 60825-1 (2001)	Safety of laser products - Part 1: Equipment classification, requirements and user's guide.
IEC 60825-2 (2000-05)	Safety of laser products - Part 2: Safety of optical fiber communication systems
EN60950-1	Safety of information technology equipment
IEC 60950-1	Information technology equipment - Safety - Part 1: General requirements
AS/NZS 60950-1:2001	Approval and test specification - Safety of information technology equipment including electrical business equipment

Telecom	
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and PHY Layer Specification

EC Directives	
ROHS 2002/95/EC	Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the Restriction of the use of certain Hazardous Substances in Electrical and Electronic Equipment (ROHS)

www.alcatel-lucent.com

Alcatel·Lucent