

# Nokia Secure Access System



Nokia Secure Access System is an SSL remote access solution that enables enterprises to provide secure, authenticated, and controlled access to any intranet or extranet from browser-based devices connected to the Internet.

With the variety of wireless devices and wide availability of Internet access, CIOs and IT managers are faced with the challenge of providing employees access to corporate data anytime, anywhere and from virtually any device all while managing cost. They also face the challenge that increased flexibility and mobility demands enhanced security measures. They must be able to identify the remote user, the access device being used and the security of that device. Only then, can the user be granted access to the appropriate corporate data and allowed to view, locally store or upload data back to the corporate network.

Nokia uniquely provides a portfolio of system level Mobile Connectivity solutions based on both IPSec and SSL technologies designed to address the specific challenges faced by IT departments.

As a key component of the Nokia Mobile Connectivity solution, Nokia Secure Access System provides enterprises with cost-effective SSL browser-based access to corporate email and applications for employees and partners. With Nokia, enterprises can control what information can be accessed, locally stored, and/or uploaded to the network based on the user, what device they are using, and how secure that device is at a given time. Nokia

enables the freedom to do business anywhere, anytime, and from any device while ensuring the integrity of the network.

## Business Benefits

**Increase productivity and reduce time-to-market:** With Nokia Secure Access System, enterprises can securely connect mobile employees, telecommuters and employees who do not have enterprise-issued devices. The ability to use readily available remote access devices streamlines information flow and optimizes business processes.

**Reduce total cost of remote access:** A significant cost associated with remote access systems stems from the installation and management of numerous remote clients. By utilizing standard SSL browsers, Nokia Secure Access System enables easy management and high ROI.

**Protect enterprise information assets:** Nokia Secure Access System provides a simple, scalable and secure way to connect employees and partners to approved enterprise applications. The ability to control access to different corporate information ensures security of the overall enterprise information assets.

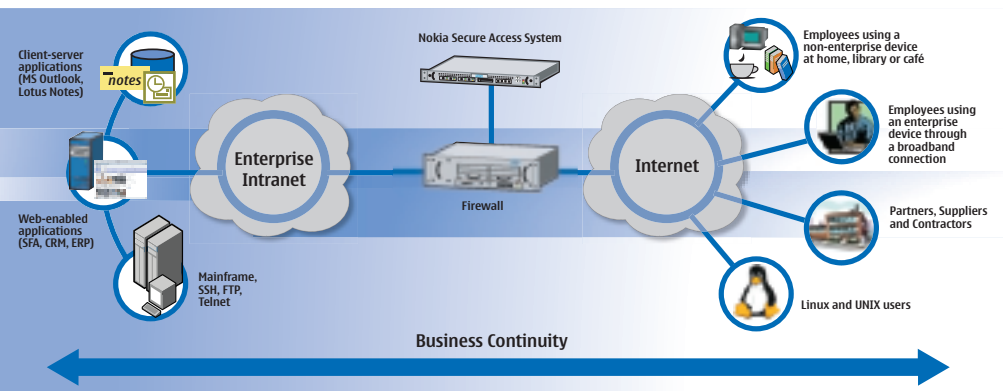
**Mobilize information:** Intranets and extranets are widely deployed in the enterprise today. E-mail and mission-critical applications can be mobilized and easily accessed through various mobile devices connected to the Internet.

**Increase efficiency around the globe:** The ability to support multiple languages simultaneously on a single Nokia Secure Access System simplifies access to enterprise data and applications from partners and employees around the globe.

## Key Features and Benefits

**Advanced Access Control:** Nokia Secure Access System uniquely improves security by providing access control based on user session properties. The level of authorization granted to the remote user can be adjusted dynamically based on the authentication method being used and/or the result of the Client Integrity Scan. The administrator can choose if a user may be allowed/denied access to certain file servers based on whether or not the remote device has the latest anti-virus definition. Deployment and configuration is simplified by assigning users to groups based on the authentication method used. Groups are assigned different access to enterprise resources and an administrator can simply provide a user with access to more resources by adding the user to more groups. Nokia Secure Access System can retrieve the user/group properties from the existing enterprise directory.

**Client Integrity Scan:** A unique feature of Nokia Secure Access System, Client Integrity Scan allows the administrator to configure scripts that test the integrity of the client system logging onto the network. This feature goes beyond simple firewall and anti-virus features by including tests for open network connections, malicious software and other indications of compromised clients. The Client Integrity Scan can also be used to help identify devices that are allowed to access the network.



**Session Persistence:** Another unique feature of Nokia Secure Access System, Session Persistence, allows users to resume work without losing data if the user session has timed out due to lack of activity.

## Authentication and Audit

Nokia Secure Access System provides support for a wide range of authentication methods including local passwords, RADIUS, LDAP, NT Domain and NIS. Administrators can also deploy two-factor authentication using SecurID over RADIUS.

The gateway logging system allows the administrator to configure a variety of options for enabling different amounts of logging information for particular users, resources, authentication methods, and gateway components. The gateway logging messages are stored on the appliance in log files that only the gateway application use. The logging messages can also be sent to the Syslog Daemon running on the gateway appliance, which can be configured to send its logging messages to a remote server.

The two types of logging produced by the gateway are:

- General Gateway Logging
- Audit Logging

The General Gateway Logging provides general information about gateway activity, including debug messages used to troubleshoot problems. Audit Logging feature provides information about user events, such as user sign-on, sign-off, authentication failures, and resource accesses.

The administrators can use the View Gateway Log page to search and display gateway logging messages. You can filter the logging messages by limiting the displayed messages to those pertaining to a particular username, resource, authentication method, or gateway

component. You can also specify the minimum severity level for messages, as well as an optional query string used to further limit the displayed log messages.

### Uses Standard Web-Browser as Client:

Widely deployed SSL-enabled browsers eliminate the need for distribution of remote clients. It reduces the cost and complexity of managing a corporate remote access system.

**SSL Encryption:** By combining access control, authentication and audit with SSL cryptography, as well as integrating unique security and productivity features, the Nokia solution enables secure, authenticated and controlled access to enterprise applications from any device with a web-browser connected to the Internet. By leveraging widely deployed SSL-enabled browsers for secure mobile connectivity, enterprises can increase the remote access ROI.

**Port-Forwarding Proxy:** With Nokia Secure Access System, enterprises can connect clientserver applications to partners and employees securely. Employees with laptops who are connecting from a remote location can use Nokia Secure Access System to access email using the Outlook client. A contract manufacturer using an ERP client can be connected securely to enter up-to-the-minute production data.

### Benefits of the Nokia Complete System

**Approach:** By leveraging the well-established Nokia complete system approach, Nokia Secure Access System brings trusted security, reliability and manageability to its customers. Nokia IP Security Platforms have been trusted globally by leading companies and service providers to run mission critical firewall, VPN and IDS functions. Nokia Secure Access System is backed by an SCP-certified global support and services organization.

## Specifications

### Supported Nokia IP Security Platforms

- Nokia IP130
- Nokia IP350
- Nokia IP380
- Nokia IP1260

### Security Features

- Secure appliance with hardened Nokia IPSO™ operating system
- Communication security through SSL/TLS encryption
- Supported SSL encryption algorithms: RSA, 3DES, AES, RC4, DES, RC2
- Advanced Access Control
- Authorized based on user session properties
- Dynamically adjusts the level of access depending upon identity of remote device
- Client Integrity Scan
- Enterprise web content not cached on client system
- Multiple Ethernet ports for physical security partitioning

### Authentication and Audit Features

- Wide range of authentication methods: local passwords, RADIUS, LDAP, NT Domain, NIS
- Two-factor authentication: SecurID over RADIUS
- Client certificates for authenticating users within a Public-Key Infrastructure
- RSA public key user authentication using non-PK1 X.509 certificates

### Application Support Features

- Browsers: IE5.0+, Netscape 6.2x and 7.x, Mozilla 1.0
- Web protocols: HTTP, HTTPS
- Web standards: HTML, Java Applets, Javascript
- File access protocols: Windows (CIFS), UNIX (NFS), FTP
- Client-server applications: Exchange, Lotus Notes, Citrix
- Email and File transfer protocols: SMTP, POP, IMAP
- Client-server terminal emulation applications such as telnet providing TN3270, VT100 support

### Management and Ease-of-Use Features

- Web-based management interface
- Telnet, FTP, HTTPS, SSH for configuration and management
- Nokia Horizon Manager
- Session persistence prevents data loss due to user inactivity

## European Customer Enquiry Number

France +33 170 708 166

Germany +49 692 222 203 68

Italy +39 236 003 652

Spain +34 914 140 777

Sweden +46 856 610 789

UK +44 161 601 8908

Email: [mobile.business.emea@nokia.com](mailto:mobile.business.emea@nokia.com)

[www.nokia.com](http://www.nokia.com)