# ArubaOS Client Integrity Module

As mobile networks become pervasive, the risk is higher than ever of devices becoming infected when exposed to unsecure networks such as public hotspots and, in turn, infecting the enterprise network. The ArubaOS Client Integrity module provides integrated on-demand security to protect the mobile edge of the network by automatically detecting, quarantining, and repairing infected or misconfigured devices before network access is granted. The solution works through a simple browser-based application download. The Aruba Client Integrity module integrates technology from Sygate Technologies®, a leading supplier of client integrity and network access control solutions for the large enterprise.
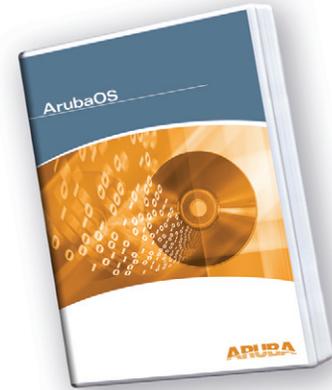
## FLEXIBLE POLICY CREATION

Enables the creation of detailed compliance policies to which endpoints must adhere before gaining network access

## HOST INTEGRITY

Ensures that devices are secured with antivirus software, updated virus definition files, personal firewall, critical service packs, and patches

Prevents non-compliant devices from accessing network resources

Provides a remediation mechanism to bring devices into compliance with corporate policies

## VIRTUAL DESKTOP

Creates a virtual environment in which users may download, manipulate, and upload confidential data without permanently storing it on the endpoint

Enables employees, partners, customers, and visitors to securely access confidential data while using third-party-owned devices
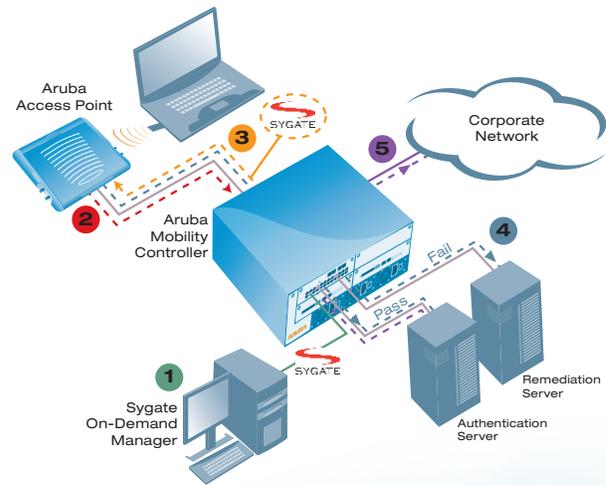
## DATA SANITIZATION AND CACHE CLEANER

Ensures confidential data that is downloaded to third-party-owned devices is completely removed
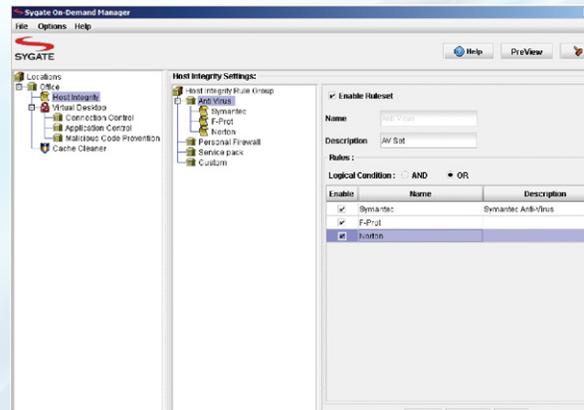
Erases browser information such as cookies, history, auto-complete, stored passwords and temporary files

Conventional network security solutions were not designed to address mobility. Traditionally, network managers set up a perimeter defense working in combination with endpoint software on client machines. However, with the growing use of laptops and other portable devices, shared computing devices in environments such as schools and manufacturing facilities, and the presence of visitors and contractors on corporate networks, this approach is inadequate. The presence of authorized, but uncontrolled, devices on the corporate network threatens the IT infrastructure.

Aruba's Client Integrity module, through a unique integration with Sygate Technologies' Sygate On-Demand Agent (SODA), eliminates these threats in a way that is seamless for the user and does not impact the existing network infrastructure. SODA, an agent defining corporate security policies, is downloaded to the client device when it requests network access, and the connection is only permitted if the endpoint is in full compliance with security policies.

## FLEXIBLE POLICY CREATION

The Client Integrity module allows network administrators to define a set of policies with which a client device must comply before being granted network access. Policies are created using an intuitive, graphical interface and may include the presence, specific type, or patch revision of anti-virus software, personal firewall software, service pack, operating system, or other installed software. Once the policies are defined, the system creates a downloadable Sygate On-Demand Agent that resides on the Aruba mobility controller.

*Sygate On-Demand Manager for flexible policy creation*

1) Corporate security policies defined and SODA sent to Aruba mobility controller.

2) Client requests network access.

3) SODA downloads to client and scans system for compliance.

4) If user fails security checks, Aruba mobility controller redirects to URL for remediation. If user passes security checks, user authenticates.

5) After authentication, network access is allowed per corporate policies

for that user.

## HOST INTEGRITY

The Client Integrity module and Aruba's captive portal authentication system place clients connecting to the network in a system role that isolates the client and prevents network access until policy compliance is verified and the user is authenticated. When a user connects to the network, the Sygate On-Demand Agent is downloaded and launched on the endpoint. SODA verifies the integrity of the endpoint according to the previously defined policies. Clients that pass the integrity check are permitted to authenticate via the Aruba captive portal screen. Clients that fail the integrity check are redirected to another customizable web page where instructions and download links are provided to enable the user to bring the device into compliance.

## VIRTUAL DESKTOP

Caches and downloaded data on third-party and shared devices can put confidential information at risk. To mitigate this risk, the Aruba Client Integrity module provides a Virtual Desktop to isolate each user's data. After completing the integrity check, SODA launches a "clean" web browser within the Virtual Desktop environment, permitting the user to log in through the Aruba captive portal. Once authenticated, the user can access web-based corporate resources such as e-mail and other servers. It is also possible to deny certain applications, such as P2P applications, from being used in this Virtual Desktop environment.

## DATA SANITIZATION AND CACHE CLEANER

When a Virtual Desktop session is terminated or times out after a configurable interval, SODA can automatically erase all data from the session. If not deleted in a secure manner, data downloaded to third-party and shared devices may be compromised. Alternatively, the Virtual Desktop can be configured to create an encrypted and password-protected virtual desktop environment that remains on the computer for the next time the same user accesses the device. Additionally, Cache Cleaner can be used to erase browser information such as cookies, history, auto-complete, stored passwords, and temporary files.

## MALICIOUS CODE PROTECTION

The Client Integrity module detects, blocks, and eliminates malicious code such as keystroke loggers from capturing usernames and passwords, Trojans from creating backdoor accounts, and screen scrapers from spying on user activity. To protect against hardware keystroke loggers, the module requires that passwords and confidential information on specific websites be input via a Virtual Keyboard. Additionally, signatures for known exploits and behavior detection are used to protect against unknown threats.

### SYSTEM REQUIREMENTS

**Host Integrity**

Windows 98, ME, NT4 (SP6), 2000, XP
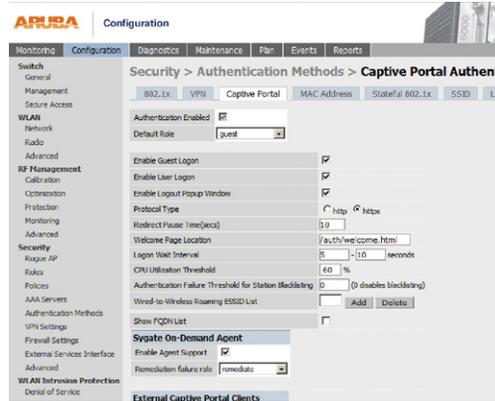
**Virtual Desktop**

Windows NT 4.0 (SP6), 2000, XP

**Cache Cleaner**

Windows 98, ME, NT4 (SP6), 2000, XP, Mac OSX, Linux

**Sygate On-demand Manager**

Windows 2000, XP, Server 2003



*Aruba Captive Portal configuration with Sygate On-Demand integration*

| FEATURE | BENEFIT |
|---|---|
| Host Integrity | • Protects the corporate network by ensuring devices accessing the network and confidential data are secured by current antivirus software, a personal firewall, critical service packs, and patches. |
| Client Remediation | • Permits non-compliant devices to access servers to install or update software. Enables a self-service portal to minimize administrator intervention. |
| Virtual Desktop | • Isolates a user's session from the general operating system to provide a clean environment in which to access web-based applications. Provides for optional encrypted and password-protected saving of the virtual desktop for later use. |
| Data Sanitization and Cache Cleaner | • Ensures that confidential data downloaded to client devices, as well as browser information, is securely deleted after session termination. |
| Malicious Code Protection | • Detects, blocks, and eliminates malicious code such as keystroke loggers, Trojans, and screen scrapers. |
| Connection Control | • Protects against the dissemination of confidential information by restricting network connections based on domain, IP address, port, and service. |
| Integration with Aruba Policy Enforcement Firewall and Role-Based Access Control | • Provides isolation and separation of users based on identity, client integrity, location, time of day, and authentication method. Prevents clients with failed integrity checks from accessing the network, while permitting access to remediation servers. |



**The Mobile Edge Company**

**www.arubanetworks.com**

1322 Crossman Avenue
Sunnyvale, California 94089
Tel: 408.227.4500 • Fax: 408.227.4550

10.5.SSCI.kh.10.1