

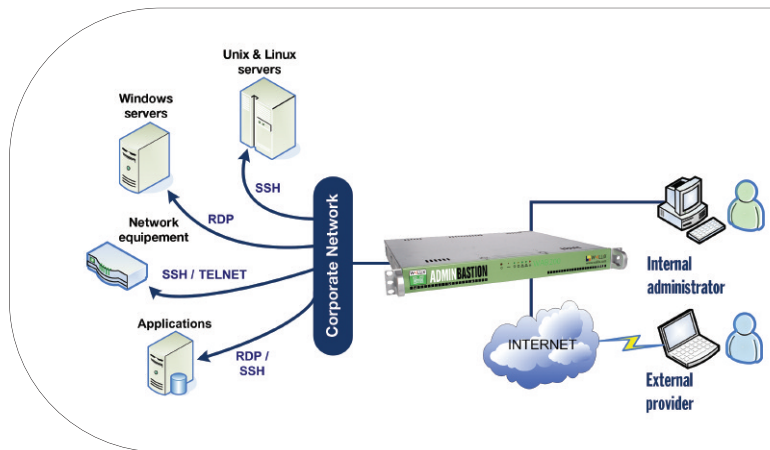
Release
2.0

WAB Wallix AdminBastion



Control and Trace your IS Key users over your IT system

- ACCESS CONTROL
- SINGLE SIGN-ON
- SESSION RECORDING
- TRACEABILITY
- AUDIT



Wallix AdminBastion V2

The WAB appliance allows organizations to **control connections and record all the operations done on the equipments** of your corporate IT system.

WAB appliance provides IT Management a greater fine-grained access control to address important audit and compliance questions.

The recording capabilities allow IT organization to **better answer not only “who” and “when” but also “what” and “how” was done over the IT infrastructure.**

Traceability

Find out who does what, when and how, in real-time or off-line. Wallix AdminBastion traces all connections and actions performed by IS teams and providers on the systems being tracked. Using the Web-based console, connections can be monitored in real-time or via the log.

Authentication - SSO

Each System administrator connects to the various equipments using central point of authentication. The authentication data can be stored within AdminBastion or in an external directory (e.g. LDAP, Active Directory, Radius etc.).

Session recording - Audit

The actions performed on the target equipment are continuously recorded for later review, whether they take place through command line sessions (SSH, telnet, rsh) or Windows Terminal Server sessions (RDP).

Access control

You control access to your IT equipment using simple, powerful rules. These are based on criteria such as IP address, login, time or session type (interactive, file transfer etc.).

Agentless monitoring capabilities

Wallix AdminBastion works without installing any agent on either the equipment being monitored or the desktops.



To find more information : <http://www.wallix.com>

Key Features	Description	Key Benefits
Access control	WAB applies an access control policy to each user according to his or her profile, allowing access to an account (login) or to SSH file transfers to be granted or refused for a particular system.	WAB fine-grained control over access policies makes it possible to define very precisely which equipment and accounts an IS provider can access - avoiding the need to provide more access to the IT system than strictly necessary.
Single Sign-On	Each IS provider or internal administrator connects to the various different equipments with a single password , the one used for WAB authentication. The authentication data can be stored within WAB or in an external directory (such as LDAP, Active Directory, Radius etc.).	The IS provider does not need to know the target equipment passwords to log in - avoiding the need to divulge sensitive passwords outside the company.
Session recording	The actions performed on the target equipment are recorded continuously for later review , whether they take place through command line sessions (SSH, telnet, rsh) or graphical Windows Terminal Server sessions (RDP).	Session recording allows the actions carried out by a service provider or administrator to be known precisely - making it much easier to diagnose abnormal events.
Connection traceability	The connection log preserves all the details of each connection. WAB also allows active sessions to be viewed in real time.	In the event of an audit or an incident, it is easy to find out who has connected to which server and for how long. Thanks to session recording, the content of the connection can then be viewed.
Agentless monitoring capabilities	WAB works without installing any agent on either the systems being monitored or on workstations	The agentless feature makes WAB simple, fast and cheap to install, maintain and update.

Features

Protocols supported

- RDP, SSH, SFTP, Telnet, rsh/rcp

Features

- ACL-based access control
- Recording and viewing of all session content: access, commands, actions taken etc.
- User authentication via login/password, private/public key (SSH) or a robust third-party authentication solution
- Single Sign-On
- Control over permissions based on user groups and devices
- Log of connections and connection attempts
- Alerts when critical servers are accessed
- Equipment and user data can be imported from CSV or LDIF files

Packaging

- Range of appliances
- Specific solution for virtualised environments
- Documentation in French and English

Operation

- Web-based console (HTTPS) compatible with IE 7+ and Firefox 2+
- Command-line mode (SSH)

Interoperability

- SNMP control
- Interface with Radius, LDAP, Active Directory & Kerberos authentication servers
- Command-line control by external applications
- Activity data available through control panels

Security and continuity of service

- Password encryption
- High availability through active/passive clustering
- Configuration backup/restoration

Support/Maintenance

- On-site maintenance
- Phone and e-mail support
- Software/Hardware maintenance and support contracts

Document and images for information only, subject to modification at any time without notice.

All product and company names mentioned are the brands or trademarks of their respective owners.