WALLIX

BASTION 8.2

January 2021

Disclaimer

The following describes WALLIX's confidential current view of its product development cycle and future directions. It is intended for information purposes only and should not be interpreted as a commitment on behalf of WALLIX. WALLIX makes no warranties, conditions, undertakings or representations of any kind, either express or implied, statutory or otherwise in relation to the content of this proprietary document.
Recipients of this document should not base their purchasing decision on the sole information contained in the present document.

Disclaimer

The following describes WALLIX's confidential current view of its product development cycle and future directions.
It is intended for information purposes only and should not be interpreted as a commitment on behalf of WALLIX.
WALLIX makes no warranties, conditions, undertakings or representations of any kind, either express or implied, statutory or otherwise in relation to the content of this proprietary document.
Recipients of this document should not base their purchasing decision on the sole information contained in the present document.

WALLIX BASTION

CONTROLLED RELEASE 8.2
January 2021

Bastion 8.2 – January 2021 – Features map

Cloud images
Yandex image
AWS marketplace image

Log filtering for SIEM
Manage costs of exporting logs to a SIEM

Session improvements
WinSCP recording + DLP/AV
Session Sharing extension
./.

Security improvements
Hyper-V Gen 2 in cloud images
Database password change
Bastion cryptography unlocking CLI

UI Improvements
Continuous page migration
Default language on RDP Proxy login

Performance improvements
Parallelization of password rotation
QoS on session

Logs retention policy
Rotation of audit

Cloud images

New Yandex image to complete cloud deployments

Microsoft Azure	▪Bastion version 8 ▪All functionalities : Session manager, Password manager, Access manager ▪All APIs and interoperability (AD, Splunk, HashiCorp, etc.)	▪Available and visible on the Azure Marketplace ▪Deployment through the Azure Console or JSON template or Azure-cli or Terraform
amazon web services		▪Available even if not visible on the AWS Marketplace(private AMI shared by Wallix) ▪Deployment through the AWS Console or thru Terraform script or AWS shell
Google Cloud Platform		▪Available even if not visible on the GCP Marketplace (GCP image to be built by user based on Wallix input) ▪Deployment through the GCP Console or thru Terraform script or Google SDK
Yandex		▪Available even if not visible on the Yandex Marketplace ▪Shareable by WALLIX
openstack		▪Available even if not visible on the OpenStack Marketplace (private Qcow2 shared by Wallix) ▪Deployment through the OpenStack Console

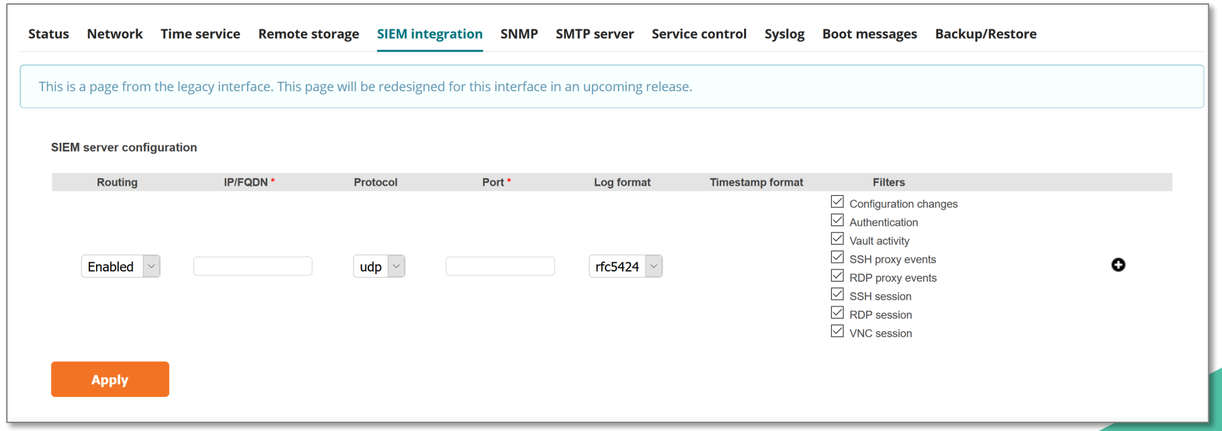
Log filtering for SIEM

Manage costs of exporting logs to a SIEM

- Objective:
  - Provide the capacity to filter logs sent to an external SIEM
- Improvements this version brings:
  - Extension of the SIEM integration page
  - Checkboxes to select which logs are to be sent via syslog
  - Alternative through filters with migration capacities for advanced usage
    - Support custom filtering by manual syslog configuration

KEY BENEFITS

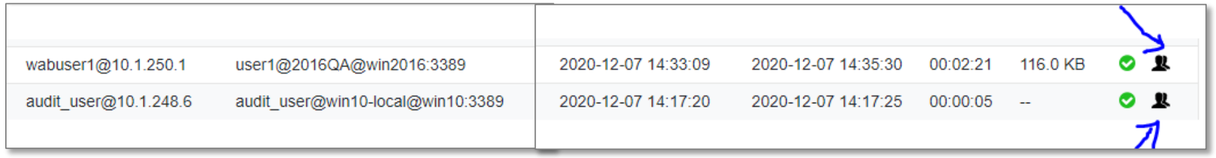
- Cost effective usage of Bastion logs with SIEM
- Facilitation of policy extension for the customer



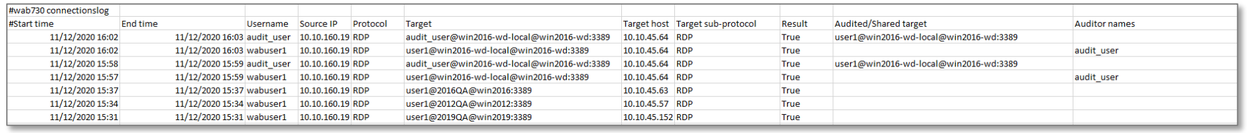
Session improvements 1/4

Improvements and extension of session sharing

- Session sharing improvements:
  - If a session sharing occurred on a session, it is visible on the session list
  - Recording of auditor when in 4 Hands
  - Logging
  - When a 4 eyes session is started, the user is informed

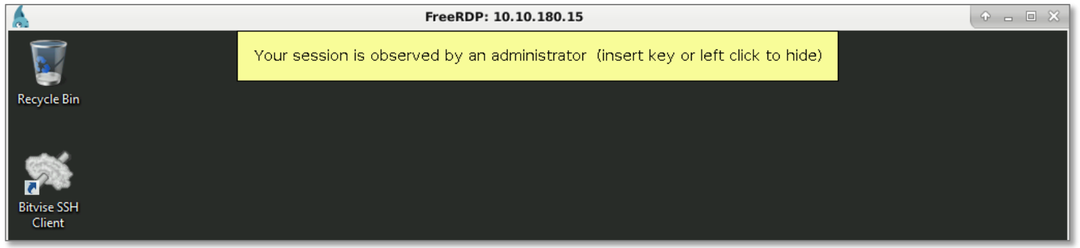


wabuser1@10.1.250.1	user1@2016QA@win2016:3389	2020-12-07 14:33:09	2020-12-07 14:35:30	00:02:21	116.0 KB	
audit_user@10.1.248.6	audit_user@win10-local@win10:3389	2020-12-07 14:17:20	2020-12-07 14:17:25	00:00:05	--	



#wab730 connectionslog

#Start time	End time	Username	Source IP	Protocol	Target	Target host	Target sub-protocol	Result	Audited/Shared target	Auditor names
11/12/2020 16:02	11/12/2020 16:03	audit_user	10.10.160.19	RDP	audit_user@win2016-wd-local@win2016-wd:3389	10.10.45.64	RDP	True	user1@win2016-wd-local@win2016-wd:3389	
11/12/2020 16:02	11/12/2020 16:03	wabuser1	10.10.160.19	RDP	user1@win2016-wd-local@win2016-wd:3389	10.10.45.64	RDP	True		audit_user
11/12/2020 15:58	11/12/2020 15:59	audit_user	10.10.160.19	RDP	audit_user@win2016-wd-local@win2016-wd:3389	10.10.45.64	RDP	True	user1@win2016-wd-local@win2016-wd:3389	
11/12/2020 15:57	11/12/2020 15:59	wabuser1	10.10.160.19	RDP	user1@win2016-wd-local@win2016-wd:3389	10.10.45.64	RDP	True		audit_user
11/12/2020 15:37	11/12/2020 15:37	wabuser1	10.10.160.19	RDP	user1@2016QA@win2016:3389	10.10.45.63	RDP	True		
11/12/2020 15:34	11/12/2020 15:34	wabuser1	10.10.160.19	RDP	user1@2012QA@win2012:3389	10.10.45.57	RDP	True		
11/12/2020 15:31	11/12/2020 15:31	wabuser1	10.10.160.19	RDP	user1@2019QA@win2019:3389	10.10.45.152	RDP	True		



Session improvements 2/4

Improvements and extension of analysis

- New protocol analysis and recording: WinSCP
  - WinSCP is a multi-channel protocol
  - It is audited by default
- Data Loss Prevention / Anti-Virus (DLP/AV)
  - WinSCP and SFTP are now analyzed and can be blocked

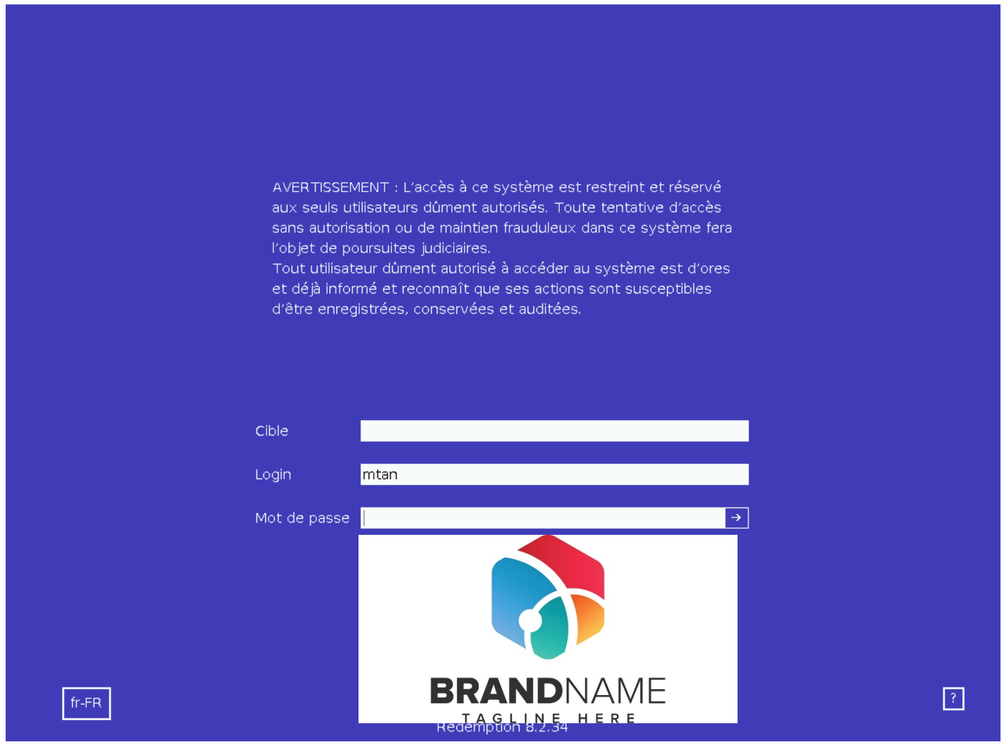
KEY BENEFITS

- Increased coverage of session and file transfer protocols
- Increased security in audit and forensic pertinency

Session improvements 3/4

Theming of RDP proxy pages

- Global options now propose to:
  - Configure colors
  - Define a picture to be displayed



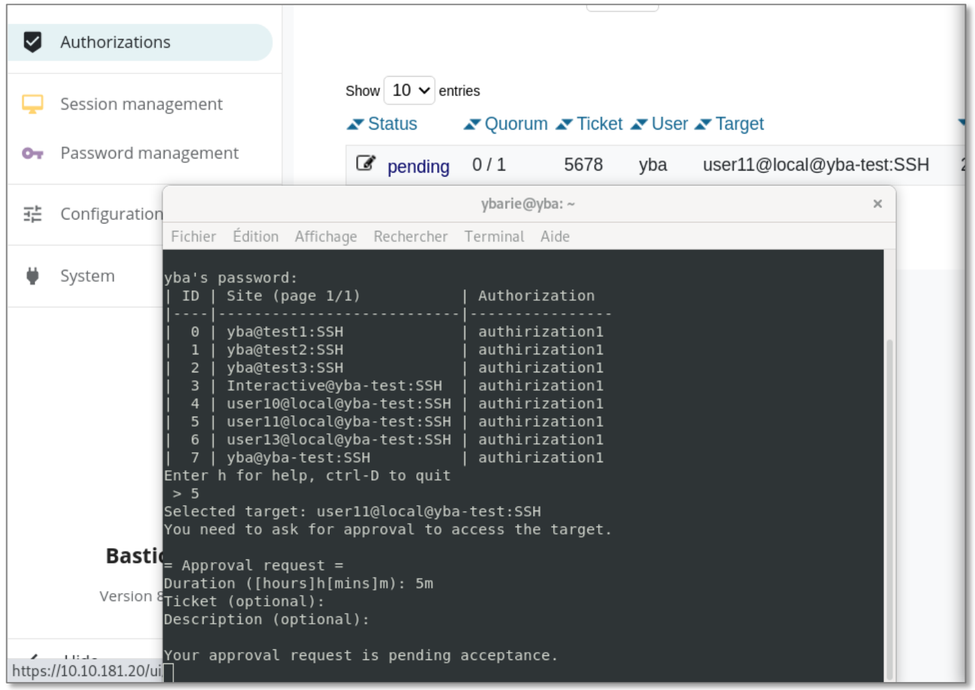
Session improvements 4/4

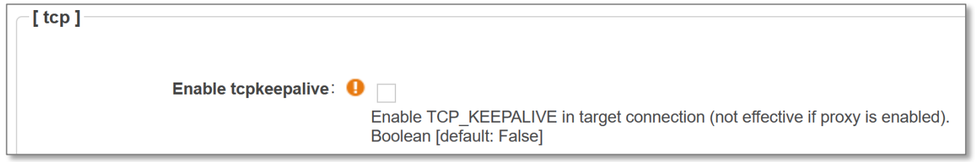
Other improvements

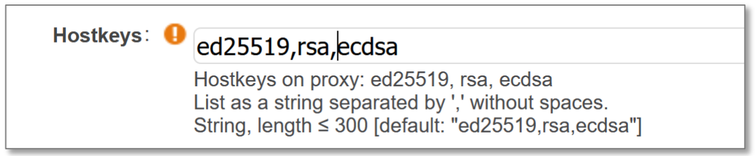
- ITSM ticket number is store on approval, and is displayed in session history
- TCP keepalive for SSH sessions
- ECDSA key for SSH hosts
- Appdriver:
  - edge chromium support:

    __APP_DRIVER_EDGE_CHROMIUM_UIA__
  - HTTP authentication support: to add in parameters:

    /e:HTTPAuthentication=Yes







Security improvements

- Hyper-V Generation 2 support when using ISO (UEFI deployment)
  - WALLIX Bastion .vhdx disk image must be imported to create a generation 1 virtual machine.
  - WALLIX Bastion .iso disk image must be imported to create a generation 2 virtual machine.
    - Hyper-V Generation 2 VM will solely boot in EFI.
  - More information here:

https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-on-windows-server.

- Database password can be changed by root: WABDatabasePassphrase
- WABUnlockPassphrase: allows wabsuper and root to decrypt the Bastion without having to go type the password on the GUI.

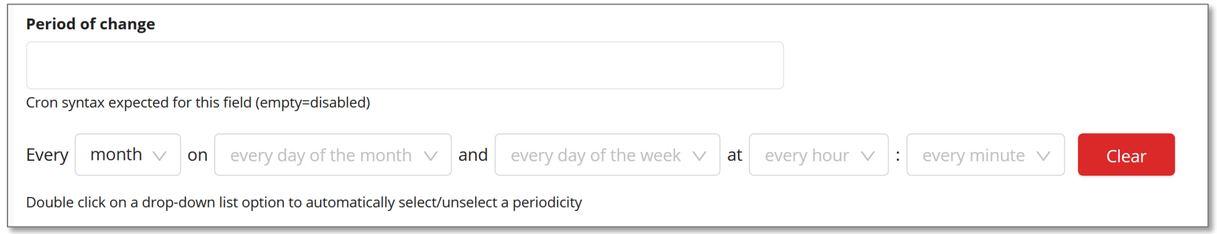
UI improvements

Continuous UI UX improvements

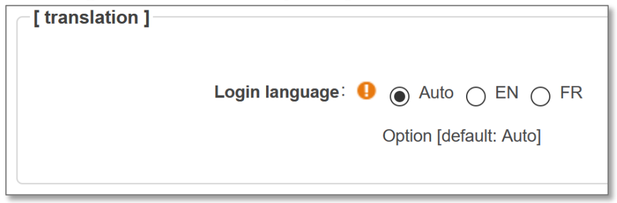
- Password change policies
  - Cron component
- License screen
  - Revoke button
- Default language on RDP Proxy login
  - Can be auto, fr, en

KEY BENEFITS

- Improvement of UX UI



Configuration: RDP proxy



Performance improvements

Password rotation performance

- Password plugins execution in parallel
  - For AD, check that this AD supports N parallel password changes (see Microsoft doc here: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/view-set-ldap-policy-using-ntdsutil)
- Credential change operation : 1000 accounts/one domain/one target: 355s

  ➔ 1000 accounts in 6 minutes

  ➔ **10X faster than before !**

Session QoS tracking

- Tracked metrics in seconds:
  - Primary connection (network time)
  - Primary authentication (bastion cpu/db time)
  - Rights retrieval (bastion cpu/db time)
  - Credentials retrieval (bastion cpu/db time)
  - Target connection (network time)
  - Total
- Added to /var/log/wabproxy.log with tag "TIME_METRICS" once target connection is done.

```
sshproxy: [sshproxy] psid="158824182123304" user="bob" type="TIME_METRICS" checkout_target="0.098" target_connection="0.037" session_id="171ca96fb8f66eb0005056b64024" primary_connection="0.43" primary_authentication="0.139" fetch_rights="0.013" total="0.717"
```

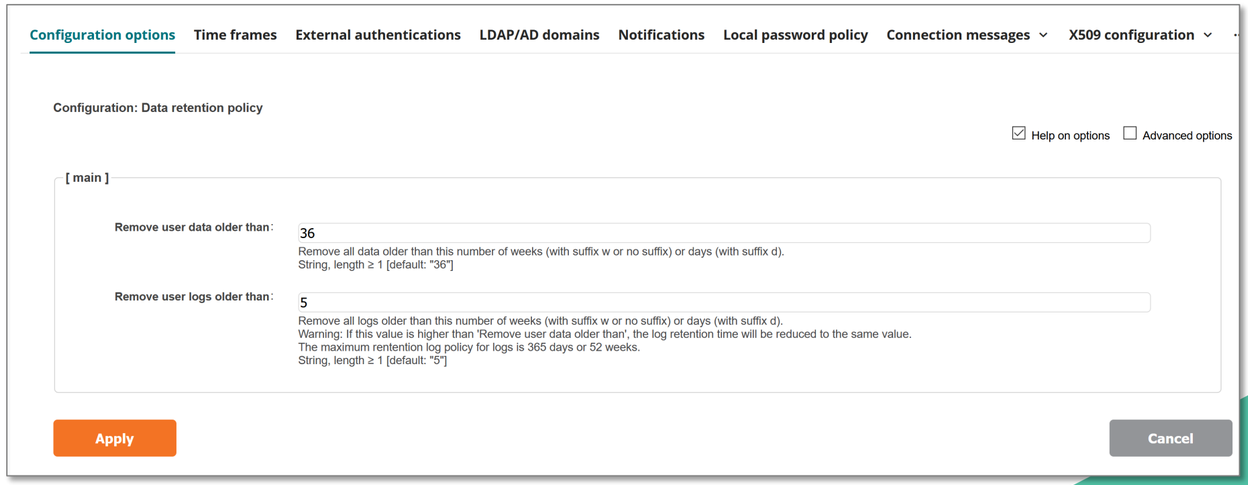
Log retention policy

Rotation of audit configurable policy

- Objective: configurable data retention policy
  - Audit logs and metadata can be automatically removed after a configurable period of time
  - That will concern both Bastion and AM regarding:
    - Username and IP association
    - Audit and metadata
    - Transaction data that would contain start/end/duration of session
  - Default rotation period will be 252 days, configurable by UI.

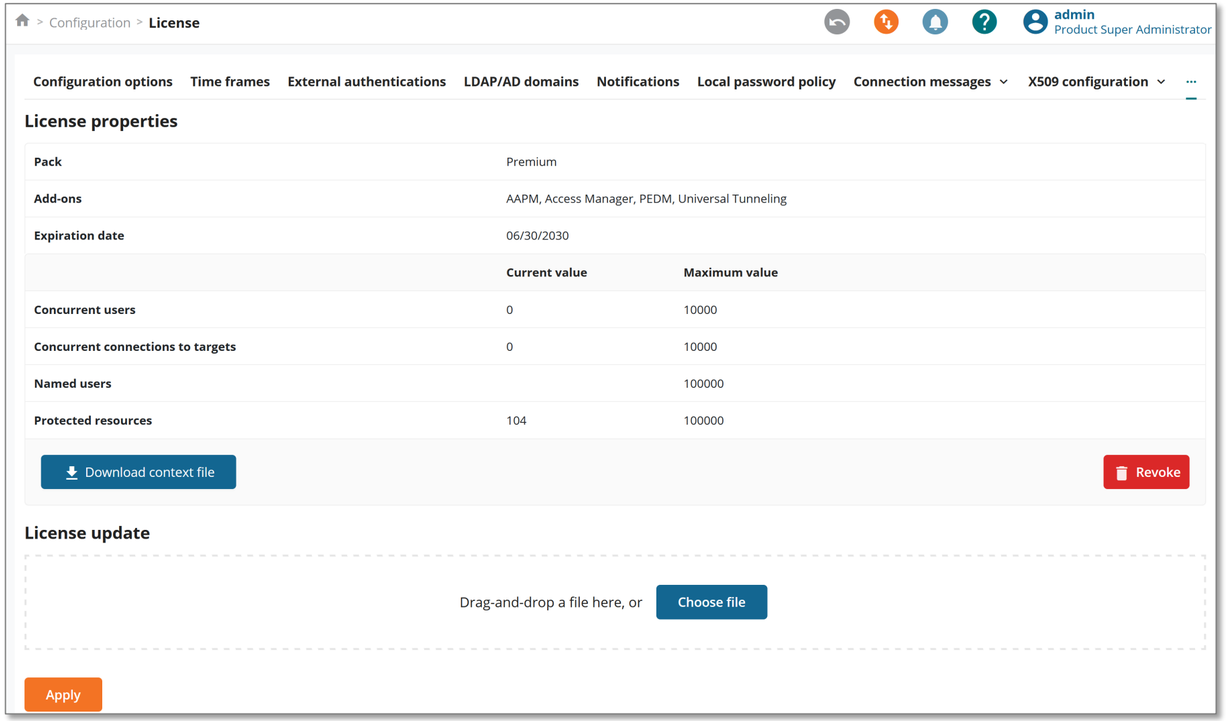
KEY BENEFITS

- Data retention for all personal information can be configured by Bastion
- Similar policy is available in Access Manager 3.0



License improvement

- New license management system: packs, options and metric display improvement
- Integrated revocation capability



KEY BENEFITS

- License management with integrated revocation system and fingerprint for license renewal
- Integrated capability to increase volume management of metrics

Product Lifecycle

End Of Life:

- WALLIX Bastion 6.0 – December 2020
- WALLIX Bastion 7.0 – April 2022
- WALLIX Access Manager 2.0 – May 2021
- WALLIX Access Manager 2.1 – March 2021

Migration compatibility

- All Access Manager version 2.0 and 2.1 are tested against the supported Bastions
- Tested migrations matrix:

From / To	6.0	7.0	8.0	8.1
6.0	-	-		
7.0	✔	-		
8.0	-	✔		
8.1		✔	✔	
8.2		✔	✔	✔

Long Term Release: Long Term releases benefit from 3 years of support & maintenance. Long Term releases terminology is "Releases X.0" [6.0, 7.0, etc.].

Hotfixes: WALLIX commits to develop hotfixes only for supported releases. WALLIX commits to develop hotfixes for Long Term supported releases and Intermediary supported releases

WALLIX

Thank You

250 bis, rue du Faubourg Saint-Honoré
75008 Paris, France

+33 1 53 42 12 81
info@wallix.com