WALLIX Bastion 12.1.0

Sessions Audit Guide

WALLIX PAM

Contents

1. Introduction

About this guide

This document is the Sessions Audit Guide for WALLIX Bastion 12.1.0. It is intended to guide users in auditing session data, including connection history and session recordings.

The following guides are also provided by WALLIX:

- The Deployment Guide
- The System Operations Guide
- The Functional Administration Guide
- The Users and Approvers Guide
- The SIEM Logs Guide

Who can audit sessions?

The privileges required to audit session data are available to users with either:

- the default **auditor** profile
- the default **product_administrator** profile
- a custom profile that includes the **View** right for the **Session audit** feature

1.1. General principles

What is WALLIX Bastion?

A *Bastion* is a machine that serves as a single point of entry for employees to securely connect to other devices in an infrastructure. It stands between the user and a remote server. Essentially, WALLIX Bastion provides authentication, authorization, traceability, and auditing throughout the whole infrastructure.

The role of WALLIX Bastion is to:

- relay SSH or RDP connections to the target devices and accounts
- control which connections users can access based on the authorizations defined in their profile
- record user actions to ensure safe and responsible use (only if the option is enabled by the WALLIX Bastion administrator)

Main notions of WALLIX Bastion

WALLIX Bastion can be used with a browser-based graphical user interface (GUI), a command line interface (CLI), or a dedicated client for SSH or RDP sessions. The CLI is available to administrators only.

Approval workflow

Approval workflow is a mechanism to restrict user access to targets. With an approval workflow, users must submit a request to approvers for the target they want to use. This request must be accepted by a defined number of approvers for the user to obtain access to the target.

User profile

The user profile determines the rights and authorizations of a user in WALLIX Bastion. For example, an administrator has access to administrative configurations of WALLIX

Bastion and an auditor has access to session data for auditing purposes, but the opposite is not true.

Authorization-based access

Administrators of WALLIX Bastion configure your authorizations. These authorizations define the:

- target devices and accounts you can connect to
- target devices and accounts for which you are authorized to view the passwords
- connection protocols you can use
- time frames during which you are authorized to connect to the target accounts
- restrictive source IP address (optional)

Contact your administrator if you have questions about your authorizations.

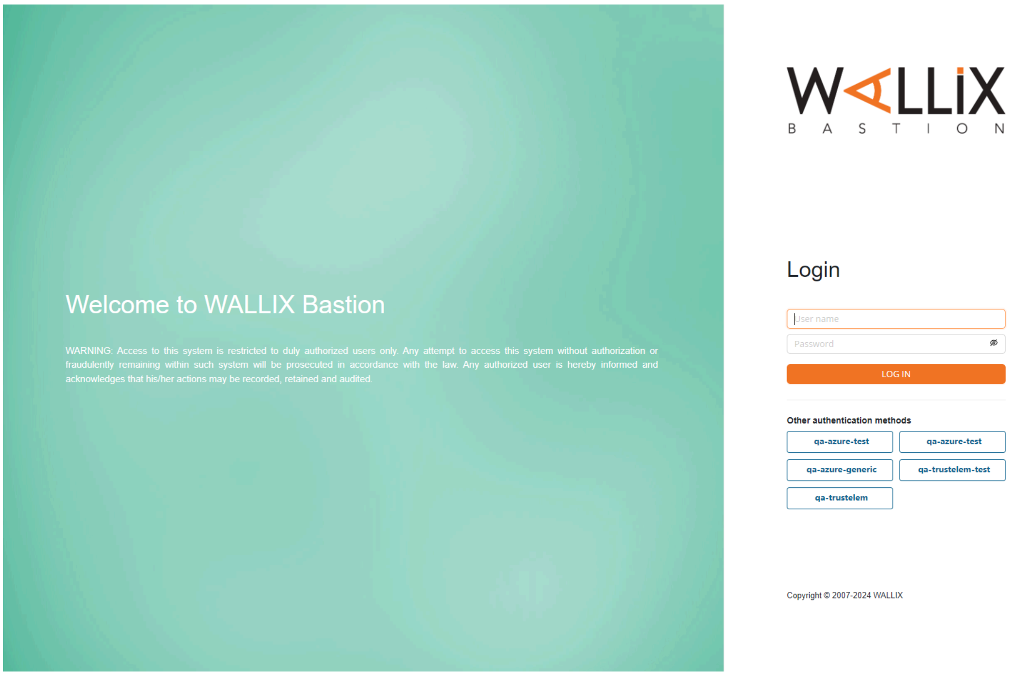
2. WALLIX Bastion authentication

You can access WALLIX Bastion from the `https://<bastion_name>/ui` address. The login page is displayed according to your browser's language preferences. After the authentication, you can select a different preferred language for WALLIX Bastion.

Note:

To access the web interface, your browser must be configured to accept cookies and run JavaScript.

Internet Explorer is not supported by the default interface.



Welcome to WALLIX Bastion

WARNING: Access to this system is restricted to duly authorized users only. Any attempt to access this system without authorization or fraudulently remaining within such system will be prosecuted in accordance with the law. Any authorized user is hereby informed and acknowledges that his/her actions may be recorded, retained and audited.

Copyright © 2007-2024 WALLIX

The login method to WALLIX Bastion depends on the configuration set by the administrator. If you are unsure what login method to use, ask your administrators.

Attention:

If you encounter an issue with the certificate while logging to WALLIX Bastion, contact your administrator.

Related information

Authentication with a login and password *(on page 7)*
Authentication with an X.509 certificate *(on page 7)*
Authentication with an Identity Provider *(on page 7)*
Authentication with Kerberos *(on page 8)*

2.1. Authentication with a login and password

Procedure

1. Open the `https://<bastion_name>/ui` URL in your browser.
2. Enter the credentials provided by your administrator.

   The password is case-sensitive.
3. Click **LOG IN**.
4. If a two-factor authentication is required, follow the corresponding authentication method.
5. If your administrator set authentication from your Active Directory, you can be asked to update your password after its expiration.

2.2. Authentication with an Identity Provider

Procedure

1. Open the `https://<bastion_name>/ui` URL in your browser.
2. Click the dedicated button in the **Other authentication method** section.
3. Click **LOG IN** or, if available, copy and paste the provided URL.
   You are redirected to the identity provider login page.
4. Enter the credentials of your identity provider account.
   You are redirected to the WALLIX Bastion web interface.
5. If a two-factor authentication is required, follow the corresponding authentication method.

2.3. Authentication with an X.509 certificate

About this task

WALLIX Bastion can provide strong authentication using an X.509 certificate through the interface if your administrator authorizes its use for your user account.

Before you begin

Your administrator must provide you with a certificate either in the form of software certificate or on a physical device (USB key, smart card, etc.). Depending on where your certificate is stored, the prerequisites differ:

- If your certificate is stored on a physical device, you must first insert the device so that the certificate is available in the system.
- If your certificate is stored in a file, you must first import the certificate into your browser so that it can be used to provide your authentication. The procedure to follow depends on your browser:

Browser	Steps
Mozilla Firefox	1. Click **Tool > Settings > Privacy & Security**. 2. In the **Certificates** section, click **View Certificates...**. 3. On the **Your Certificates** tab, click **Import...**.

Browser	Steps
Google Chrome	1. Click **Customize and control Google Chrome→Settings→Privacy and security**. 2. In the **Privacy and security** section, click **Security**. 3. In the **Advanced** section, click **Manage certificates**. 4. On the **Personal** tab, click **Import...**.
Microsoft Edge	1. Click **Settings and more→Settings→Privacy, search and services**. 2. In the **Security** section, click **Manage certificates**. 3. On the **Personal** tab, click **Import...**.

Procedure

1. Open the `https://<bastion_name>/ui` URL in your browser.
2. Choose a login method.
   - Select **Password** in **Other authentication method**, enter a login and password, and click **LOG IN**.
   - Select **X509 Authentication** in **Other authentication method** and click **LOG IN**. In this case:
     - if you have more than one certificate and you did not yet save your choice, your browser asks you to choose a certificate.
     - if the certificate is password-protected, you must enter the password for the certificate.

> **Note:**
>
> If your certificate is stored on a physical device, the smart card or USB key concerned must remain inserted throughout the authentication phase.

Results

If the certificate is linked with a WALLIX Bastion account, you are immediately authenticated and logged in with this account.

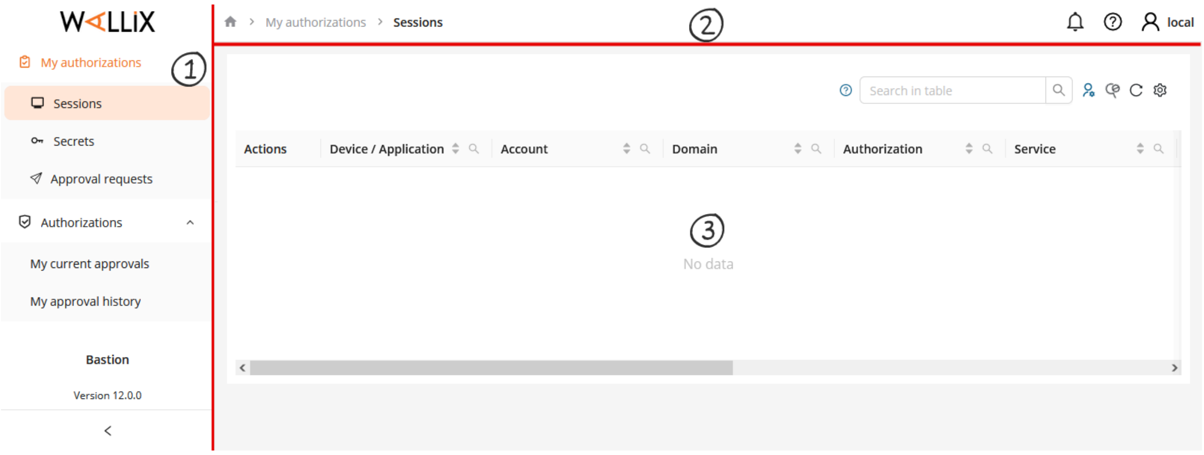
2.4. Authentication with Kerberos

Procedure

1. Open the `https://<bastion_name>/ui` URL in your browser.
2. Click the dedicated button in the **Other authentication method** section.

3. Navigating the WALLIX Bastion web interface

After logging in to WALLIX Bastion, you are redirected to the homepage.



1. The navigation menu on the left provides access to features. The list of features varies depending on your user profile and authorizations.
2. The header at the top of the page provides information such as a breadcrumb, access to your notifications (🔔) and the online documentation (?). It also contains a user menu for accessing your preferences, switching your interface layout, and logging out.
3. The main area provides access to or management of information related to the feature selected in the navigation menu.

Logging out

Logging out from the web interface only logs users out of WALLIX Bastion. This means that a user authenticated with SAML or OIDC on Entra ID or any other Identity Provider (IdP) is not disconnected from their session on that IdP.

4. Configuring your account

As a WALLIX Bastion user, you can manage your personal information and configure preferences.

4.1. Update my e-mail

Procedure

1. From any page of the WALLIX Bastion web interface, click your name, and click **My preferences**.
2. On the **Profile** tab, enter the new e-mail address to use for login and notifications in the **Email** field.
3. Click **Apply**.

4.2. Update my password

Before you begin

> **Attention:**
>
> Depending on the configuration set by the administrator, you may not be allowed to change your password.

Procedure

1. From any page of the WALLIX Bastion web interface, click your name, and click **My preferences**.
2. On the **Password** tab, enter your current password.
3. Enter your new password and confirm your new password.
4. Click **Apply**.

Results

Your password is updated if it respects the required criteria.

A password can be rejected for various reasons. For example:

- the password is part of the list of forbidden passwords defined by the WALLIX Bastion administrator
- the password is too short or does not include any special characters, numbers, or uppercase letters
- the password is the same as the user login
- the password is the same as a previous password
- the password is weak, using common words, logical or repeated patterns (such as `Password123!`, `abcabcABCABC`, etc.).

If the new password is rejected, modify the password, and repeat the procedure.

4.3. Update my preferred language

About this task

Choose a preferred language for both the interface and messages on proxies.

Procedure

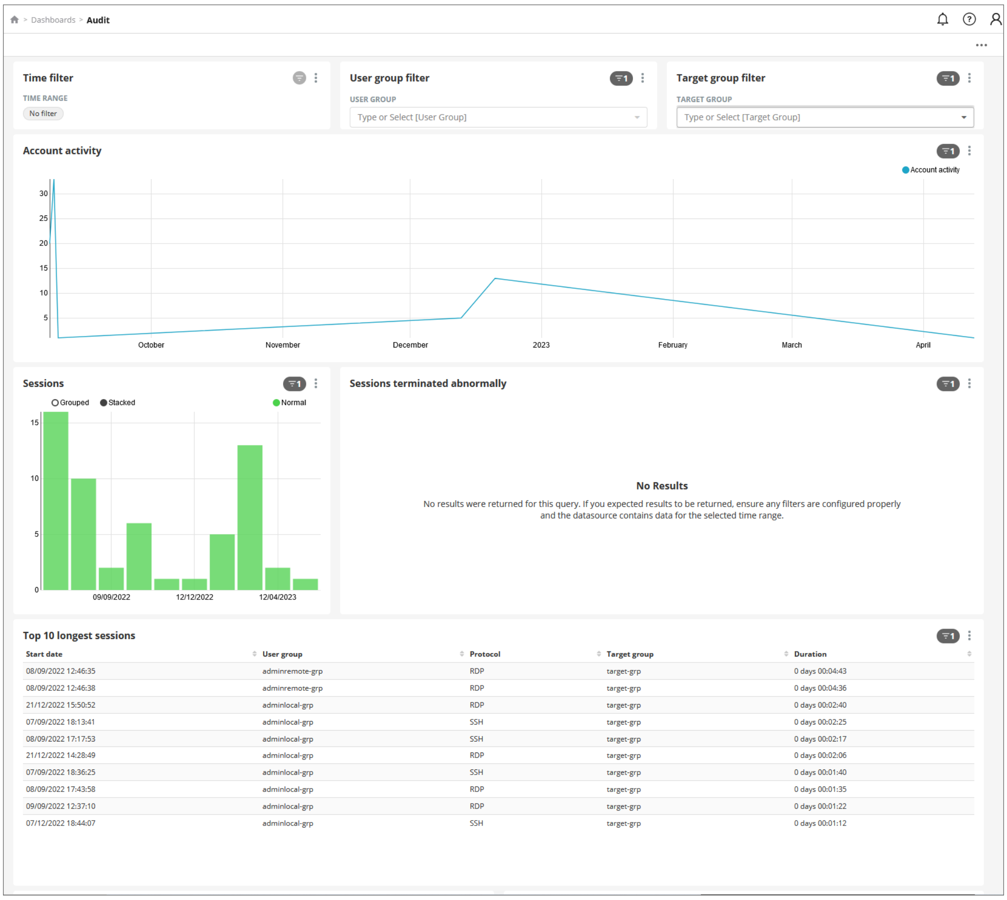
1. From any page of the WALLIX Bastion web interface, click your name, and click **My preferences**.
2. On the **Profile** tab, select one of the available languages from the **Language** drop-down list.
3. Click **Apply**.

5. Audit dashboard

Note:

The dashboard is only available in English.

The **Dashboards > Audit** page provides a detailed analysis of all the connections made by users through WALLIX Bastion. Metrics are provided as numerical data, tabular views, and charts over a given period of time. The data viewable from this dashboard corresponds primarily to account, session, user group, and target account group activities.



No Results

No results were returned for this query. If you expected results to be returned, ensure any filters are configured properly and the datasource contains data for the selected time range.

Top 10 longest sessions

Start date	User group	Protocol	Target group	Duration
08/09/2022 12:46:35	adminremote-grp	RDP	target-grp	0 days 00:04:43
08/09/2022 12:46:38	adminremote-grp	RDP	target-grp	0 days 00:04:36
21/12/2022 15:50:52	adminlocal-grp	RDP	target-grp	0 days 00:02:40
07/09/2022 18:13:41	adminlocal-grp	SSH	target-grp	0 days 00:02:25
08/09/2022 17:17:53	adminlocal-grp	SSH	target-grp	0 days 00:02:17
21/12/2022 14:28:49	adminlocal-grp	RDP	target-grp	0 days 00:02:06
07/09/2022 18:36:25	adminlocal-grp	SSH	target-grp	0 days 00:01:40
08/09/2022 17:43:58	adminlocal-grp	RDP	target-grp	0 days 00:01:35
09/09/2022 12:37:10	adminlocal-grp	RDP	target-grp	0 days 00:01:22
07/12/2022 18:44:07	adminlocal-grp	SSH	target-grp	0 days 00:01:12

Data filters

Applying filters to the dashboard allows to generate charts and tables for a specific data set. Filters include:

Time filter

Define the period of time for which you want to view the data. By default, this period corresponds to the last week.

There are five range types available:

- **Last** provides a choice between last day, week, month, quarter, or year.
- **Previous** provides a choice between previous calendar week, calendar month, or calendar year.
- **Custom** provides the possibility to define a specific time range.

- **Advanced** provides the possibility to define a regex rule.
- **No filter**

If you modify the default filter, you must click **Apply** to generate the boards for this period.

User group filter

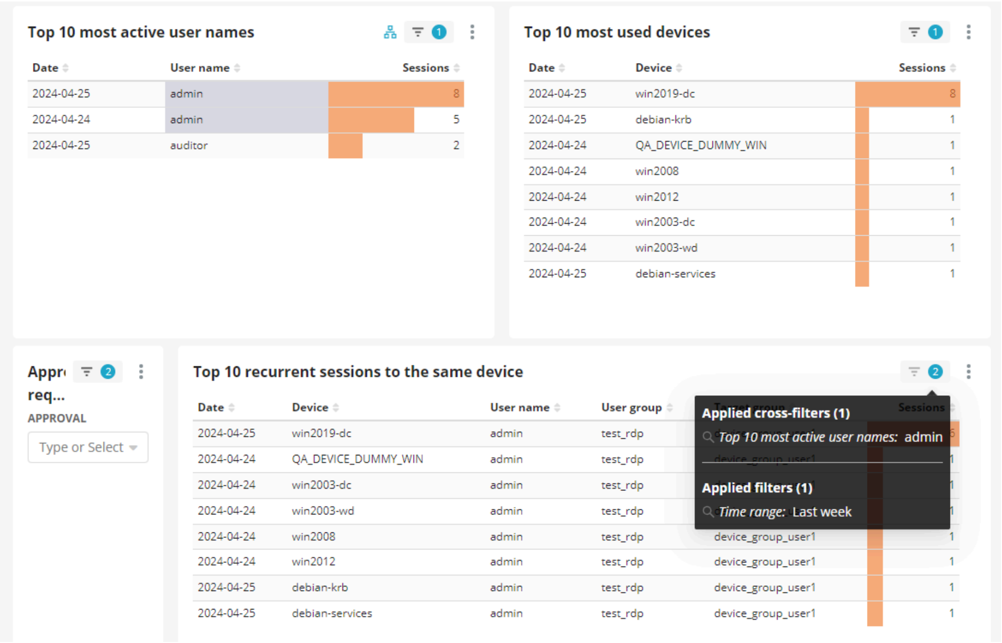
Restrict the metrics display to one or more user groups.

Target group filter

Restrict the metrics display to one or more target groups.

There is a fourth filter, the **Approval request filter** which applies only to the last three boards. With this filter, you can restrict the display to only sessions that did not go through an approval workflow.

You can also use cross-filters. Cross-filters are values selected inside a data board which restrict the data set of other data boards. For example, clicking John Doe in the **Top 10 most active user names** applies a John Doe filter to the **Top 10 recurrent sessions to the same device** board.



Top 10 most active user names

Date	User name	Sessions
2024-04-25	admin	8
2024-04-24	admin	5
2024-04-25	auditor	2

Top 10 most used devices

Date	Device	Sessions
2024-04-25	win2019-dc	8
2024-04-25	debian-krb	1
2024-04-24	QA_DEVICE_DUMMY_WIN	1
2024-04-24	win2008	1
2024-04-24	win2012	1
2024-04-24	win2003-dc	1
2024-04-24	win2003-wd	1
2024-04-25	debian-services	1

Appr req...

APPROVAL

Type or Select

Top 10 recurrent sessions to the same device

Date	Device	User name	User group	Target group	Sessions
2024-04-25	win2019-dc	admin	test_rdp	[illegible]	6
2024-04-24	QA_DEVICE_DUMMY_WIN	admin	test_rdp	device_group_user1	1
2024-04-24	win2003-dc	admin	test_rdp	[illegible]	1
2024-04-24	win2003-wd	admin	test_rdp	[illegible]	1
2024-04-24	win2008	admin	test_rdp	device_group_user1	1
2024-04-24	win2012	admin	test_rdp	device_group_user1	1
2024-04-25	debian-krb	admin	test_rdp	device_group_user1	1
2024-04-25	debian-services	admin	test_rdp	device_group_user1	1

Applied cross-filters (1)

Top 10 most active user names: admin

Applied filters (1)

Time range: Last week

Data boards

Charts and tables include two types of data:

- the activities of the accounts and sessions over the selected time filter
  - Account activity
  - Account activity outside working hours
  - Sessions
  - Sessions terminated abnormally
  - Sessions outside working hours
- the rankings of sessions, user groups, target account groups and devices
  - Top 10 longest sessions
  - Top 10 most active user groups
  - Top 10 most used target groups
  - Top 10 most active user names

    - Top 10 most used devices
    - Top 10 recurrent sessions to the same device

> **Tip:**
>
> For charts, you can display the numerical data by hovering graph points.

Data options

For each data board, a menu offers the following actions:

- Sort table values by ordering a column alphabetically or not (▲▼)
- View filters applied to the board (≡ 1)
- **Force refresh**: instantly refresh the data of the board. The time stamp of the last refresh is also indicated.
- **Enter fullscreen**: display the full screen view of the board. It is possible to return to the condensed view by clicking the “Minimize chart” icon.
- **Download as image**: download the data of the board as a JPG file.
- **Export to CSV**: download the data of the board as a CSV file.
- **Export to Excel**: download the data of the board as a XLSX file.

6. Real-time monitoring of target sessions

From the **Audit > Current sessions** menu, auditors can view the list of ongoing connections during which RDP or SSH sessions are initiated from WALLIX Bastion.

If administrators authorized it, auditors can also share the connections. Session sharing is a real-time audit capability which grants auditors access to a user session, guaranteeing the security of the session. For RDP sessions, the feature also provides auditors with the ability to remotely control the user session.

How to read session information

> **Tip:**
>
> By default, the current session data is automatically refreshed. Auditors can change the refresh frequency or deactivate the **Automatic refresh** option. This can be useful when selecting the ongoing connections to close.

For each current session happening, there are several pieces of information available:

Status

This column indicates if the user is connected and lets the auditor observe or join the session when applicable.

User

The account which initiated the session, identified with the user name and IP address of the workstation such as `<user>@<workstation_IP>`.

In the context of the Session invite feature, an additional line shows the connected guest user, as follows: `_GUEST_identifier@<source_IP>`.

Target

The target which is accessed during this session, identified as `<ACCOUNT>@<DEVICE>:<SERVICE>`.

Target host/IP

The target host or IP address.

SRC/DST protocol

The description of the source (RDP or SSH) and destination protocols.

For example `SSH/TELNET`, `RDP/RDP`, `APP/RDP`, etc.

Start time

The date and time of the session launch.

Duration

How much time has passed since the start of the session.

You can filter the list of current session using keywords. For example, you can refine the search for RDP sessions with the following keywords:

- `rdp:app` to view only application sessions
- `rdp:notapp` to exclude application sessions

6.1. Share current RDP session

About this task

RDP allows sessions to be remotely audited or controlled by an auditor. The feature is available through WALLIX Bastion for targets under Windows Server 2012 and later that support the **Remote Desktop Shadowing** feature for remote control.

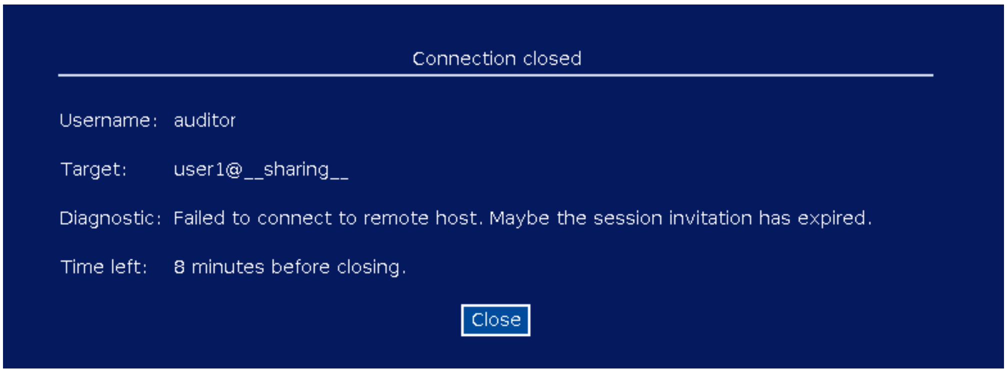
The audited user is warned before the session that they can be audited in real time. They consent to being audited when launching their session.

> **Important:**
>
> Only one remote control request can be sent during a user session.
>
> The auditor's session is only recorded if the user's session is recorded.

Procedure

1. Go to the **Audit > Current sessions** page.
2. Click **Remote control** for the session you want to join.
   This downloads a file to establish a connection to the user session.
3. Execute the downloaded session file to initiate a connection to the user session.

   You have 30 seconds to execute the file or the invitation expires as shown in the following screenshot.

   Connection closed

   Username: auditor

   Target: user1@__sharing__

   Diagnostic: Failed to connect to remote host. Maybe the session invitation has expired.

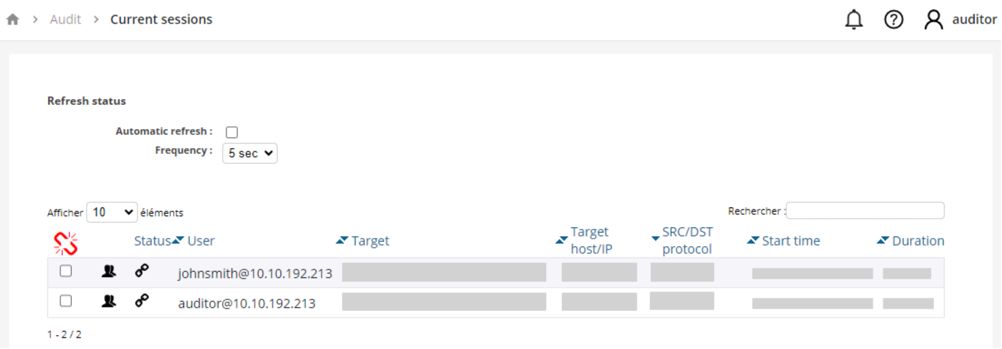
   Time left: 8 minutes before closing.

4. The user receives a **Remote Control Request** as soon as the auditor requests access. The user must accept the request within 30 seconds or the request is canceled.

   The auditor cannot remotely control the user's session as long as the user does not accept the request. A **Waiting for Shadow Session Invitation** message appears while waiting for the user approval on the request.

Results

Auditing a user session adds another current session for the auditor. However, on session logs, actions from user and auditor are not differentiated when control is shared.



Audit > Current sessions

auditor

Refresh status

Automatic refresh : □

Frequency : 5 sec

Afficher 10 éléments

Rechercher :

	Status	User	Target	Target host/IP	SRC/DST protocol	Start time	Duration
□		johnsmith@10.10.192.213	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
□		auditor@10.10.192.213	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

1 - 2 / 2

6.2. Share current SSH session

About this task

SSH sessions can be remotely viewed by auditors, but they cannot be remotely controlled. The audited user is warned before the session that they can be audited in real time. They consent to being audited when launching their session.

Procedure

1. Go to the **Audit > Current sessions** page.
2. Click **Observe** for the session you want to view.
   This opens a window to view the session in real-time.

Results

You can close the audit window before the end of the user session, this does not end the user session.

6.3. Close current session

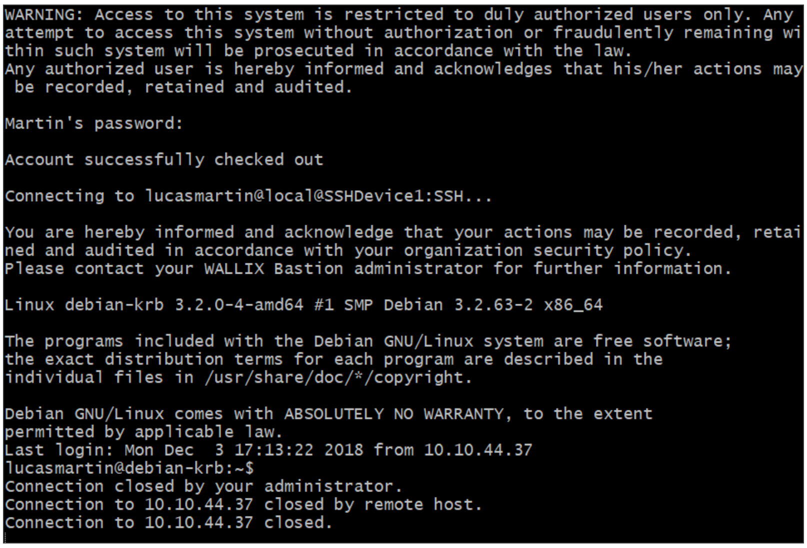
Procedure

1. Go to the **Audit > Current sessions** page.
2. Select the session you want to interrupt by clicking the checkbox.
3. Click **Close connections** to close the current session.
4. In the pop-up dialog box, confirm that you want to disconnect the user from the session.

Results

Users connected through RDP or SSH are informed that the connection was closed, as shown in the following screenshot.

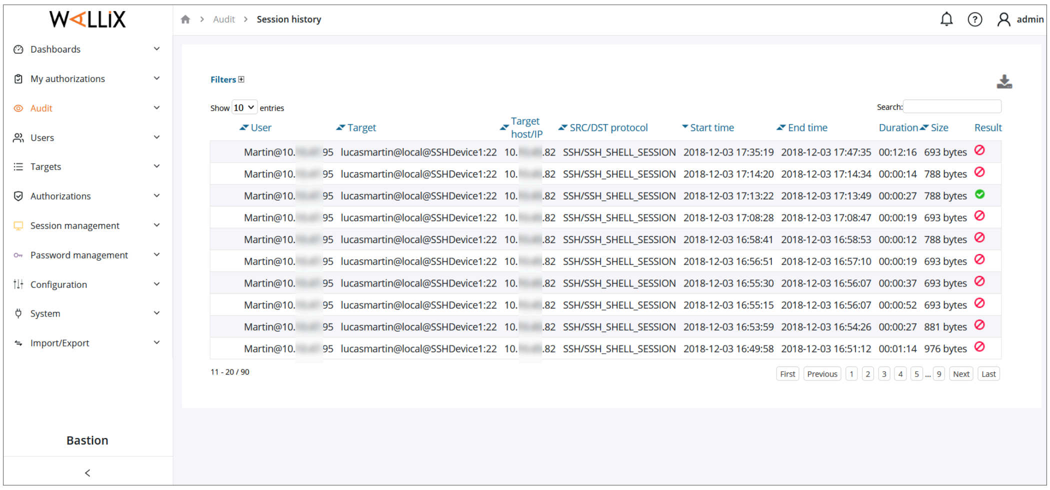
Example of a closed SSH connection.



```
WARNING: Access to this system is restricted to duly authorized users only. Any
attempt to access this system without authorization or fraudulently remaining wi
thin such system will be prosecuted in accordance with the law.
Any authorized user is hereby informed and acknowledges that his/her actions may
 be recorded, retained and audited.

Martin's password:

Account successfully checked out

Connecting to lucasmartin@local@SSHDevice1:SSH...

You are hereby informed and acknowledge that your actions may be recorded, retai
ned and audited in accordance with your organization security policy.
Please contact your WALLIX Bastion administrator for further information.

Linux debian-krb 3.2.0-4-amd64 #1 SMP Debian 3.2.63-2 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Dec  3 17:13:22 2018 from 10.10.44.37
lucasmartin@debian-krb:~$
Connection closed by your administrator.
Connection to 10.10.44.37 closed by remote host.
Connection to 10.10.44.37 closed.
```

7. Session history

From the **Audit > Session history** page, auditors can view the history of all connections made to targets through WALLIX Bastion and also visualize the session recordings.



Show 10 entries

User	Target	Target host/IP	SRC/DST protocol	Start time	End time	Duration	Size	Result
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 17:35:19	2018-12-03 17:47:35	00:12:16	693 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 17:14:20	2018-12-03 17:14:34	00:00:14	788 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 17:13:22	2018-12-03 17:13:49	00:00:27	788 bytes	✓
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 17:08:28	2018-12-03 17:08:47	00:00:19	693 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 16:58:41	2018-12-03 16:58:53	00:00:12	788 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 16:56:51	2018-12-03 16:57:10	00:00:19	693 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 16:55:30	2018-12-03 16:56:07	00:00:37	693 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 16:55:15	2018-12-03 16:56:07	00:00:52	693 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 16:53:59	2018-12-03 16:54:26	00:00:27	881 bytes	⊘
Martin@10.[redacted]95	lucasmartin@local@SSHDevice1:22	10.[redacted].82	SSH/SSH_SHELL_SESSION	2018-12-03 16:49:58	2018-12-03 16:51:12	00:01:14	976 bytes	⊘

11 - 20 / 90

First Previous 1 2 3 4 5 ... 9 Next Last

How to read session information

Note:

Only the last 1,000 records are displayed on the web interface. The occurrence filter is applied to these 1,000 records. Older sessions can only be retrieved through the date range filter.

For each past session, there are several pieces of information available:

User

The user name and source IP of the connection, such as `<name>@<source_IP>`.

In the context of the session invite feature, an additional line can be displayed for the invited user who shared the host user's session, as follows: `_GUEST_identifier@<source_IP>`.

Target

The accessed target, as follows: `<ACCOUNT>@<DEVICE>:<SERVICE>`

Target host/IP

The target host or IP address.

SRC/DST protocol

The description of the source (RDP or SSH) and destination protocols.

For example `SSH/TELNET`, `RDP/RDP`, `APP/RDP`, etc.

Start time

The date and time of the session launch.

End time

The date and time of the end of the session.

Duration

Total duration of the user session, in the `HH:MM:SS` format.

Size

If the session was recorded, this information indicates the size of the recording file

Result

This shows the result of the session. There are three different result statuses and an additional contextual information:

⛔ The session connection failed. Clicking the icon expands the information related to the session and provides the cause of termination. For example, wrong password, authentication to target failed, or target not available.

✅ The session ended successfully.

⊘ The session was killed by another user. Hovering the icon mentions the name of the user who killed the session.

👥 If a session was shared or controlled by another user thanks to the session invite feature or the session sharing feature, this icon is displayed. Hovering the icon shows the name of that second user as well as start date, end date, and total duration of the guest user session.

You can filter the list of past sessions to only display relevant records. The available filters are the following:

- a sort on the display of all data or only the existing device or only the existing application
- the definition of a date range with a start and end date
- the definition of the last N days, weeks, or months
- a search by text occurrences in the columns. For example, you can refine the search for RDP sessions with the following keywords:
  - `rdp:app` to view only application sessions
  - `rdp:notapp` to exclude application sessions

Actions

Depending on the configuration for user sessions, there are several actions available on session recording to auditors:

- Add a personal description to the session (for more information, refer to Provide session description *(on page 23)*)
- Download session recording in TTYREC format or TXT format
- Download all session data from this page as a CSV file
- Display the session recording (for more information, refer to Session recordings *(on page 20)*)

7.1. Session recordings

WALLIX Bastion embeds a session video player. It allows auditors to view RDP or SSH session recordings without requiring the installation of any specific browser plugin, application, or video codec. Only sessions that authorized the session recording in the authorization for the user group and the target group are recorded and can be viewed.

Some icons can be displayed at the beginning of the lines to perform specific actions:

- 💾: download the session recording in the unprocessed TTYREC format for SSH sessions or in the PCAP format for Universal Tunneling sessions
- 📄: download the visible content of the SSH session in the TXT format
- 🔍: display the recording of the RDP or SSH session

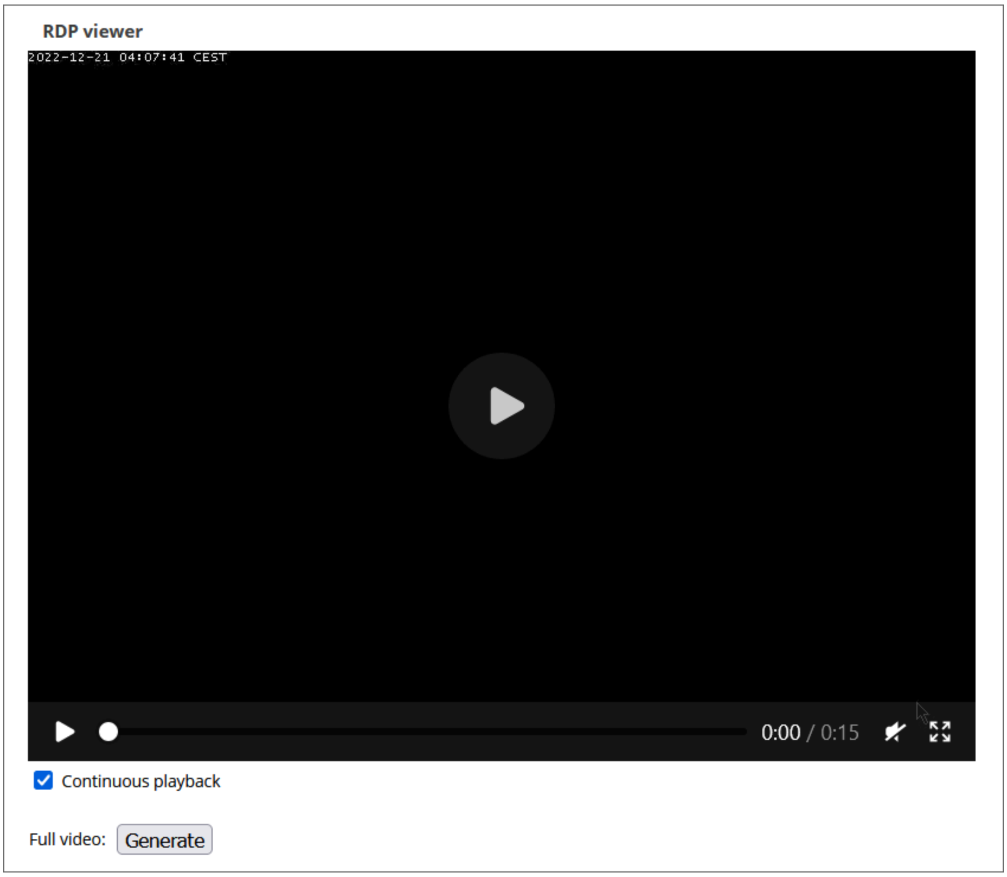
Note:

A missing 🔍 icon for a recording-enabled session with a successful authentication can indicate an integrity error.

7.1.1. Recorded RDP sessions

Viewing the record

As auditors, you have access to the entire video recording of the RDP session. This video can be viewed any number of times. By default, the **Continuous playback** option is activated and shows the video in loops.



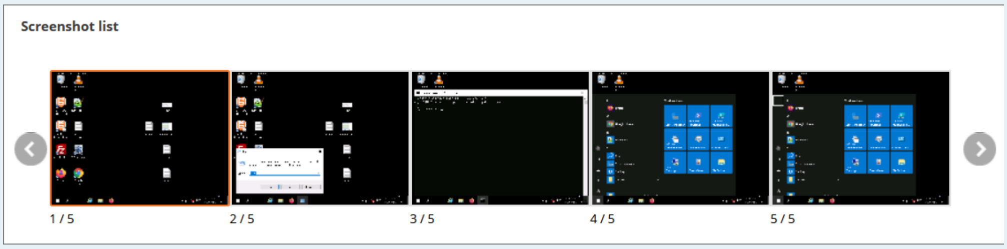
☑ Continuous playback

The recording for a session based on the RDP protocol includes both video and automatic Optical Character Recognition (OCR) of the applications running on the remote machine by detecting title bars.

The algorithm used to detect the title bar content allows real-time execution. However, it only works with the Windows Standard windows and a default font size of 96PPP with a color depth of 15 bits or more. In its current version, the OCR function does not work if the title bar style is changed, even to a style that is visually very similar. For example it does not work if the style is changed to Windows classic, or if there is a modification in the title bar color, style, font size, or resolution. In addition, OCR is configured to detect only the title bars of applications closed using the three icons: close icon, minimize icon, and maximize icon. If the title bar contains an icon, this is replaced by a question mark before the recognized text.

Tip:

Browse through the video by clicking the thumbnails on the **Screenshot list** area. Thumbnails identify new events in the session.

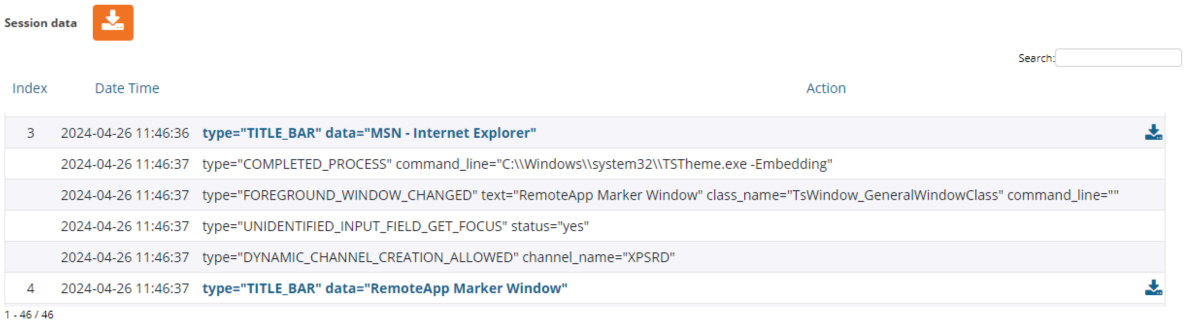


Download the record

You can generate and download the entire video by clicking the **Generate** button under the viewer, then by clicking the 🖫 icon displayed after the generation is completed.

Session data

You can download the entire session data by clicking the ⤓ download icon next to **Session data**. This downloads a META file with the descriptive logs. You can also view and browse the same log directly from the **Session data** section which lists, in order, each recorded action.



Index	Date Time	Action	
3	2024-04-26 11:46:36	**type="TITLE_BAR" data="MSN - Internet Explorer"**	⤓
	2024-04-26 11:46:37	type="COMPLETED_PROCESS" command_line="C:\\Windows\\system32\\TSTheme.exe -Embedding"	
	2024-04-26 11:46:37	type="FOREGROUND_WINDOW_CHANGED" text="RemoteApp Marker Window" class_name="TsWindow_GeneralWindowClass" command_line=""	
	2024-04-26 11:46:37	type="UNIDENTIFIED_INPUT_FIELD_GET_FOCUS" status="yes"	
	2024-04-26 11:46:37	type="DYNAMIC_CHANNEL_CREATION_ALLOWED" channel_name="XPSRD"	
4	2024-04-26 11:46:37	**type="TITLE_BAR" data="RemoteApp Marker Window"**	⤓

1 - 46 / 46

If the OCR option is enabled, the titles of applications detected in the record by the OCR module are indexed and displayed in this area. It is possible to click the entries in the list to quickly browse through the recording from the viewer. It is also possible to download only the relevant action as an MP4 file by clicking the download icon (⤓) next to the indexed action.

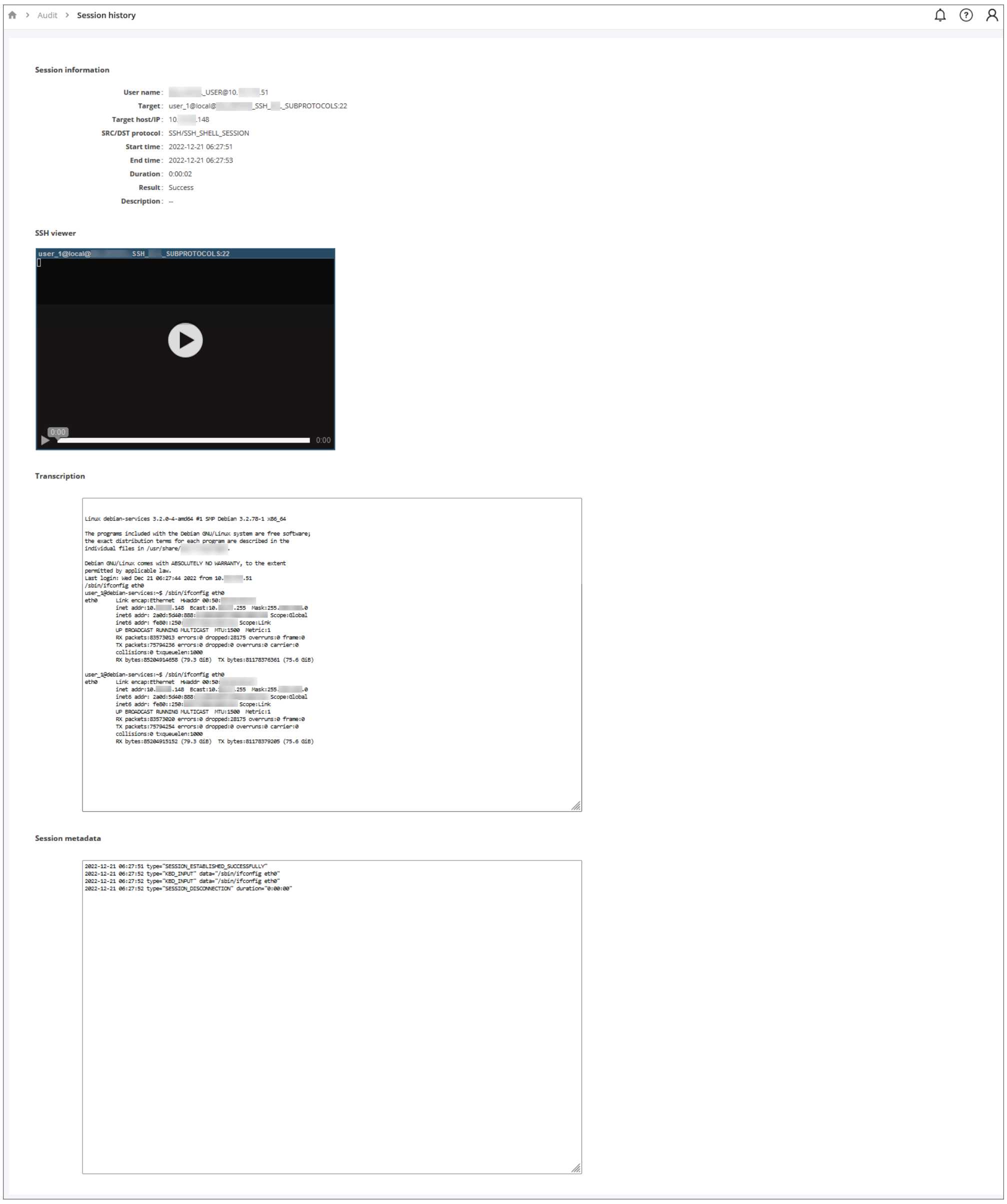
If files were transferred during the session, these files are available to download from the **Transferred files** area.

If the session went through an approval workflow, the 👍 icon is present. This icon allows auditors to display a detailed page of the approval request (including all the answers and comments from approvers).

7.1.2. Recorded SSH sessions

As an auditor, you have access to the entire video recording of the SSH session. This video can be viewed any number of times. Additionally, you have access to the entire transcript of the session and to the session metadata.

If files were transferred during the session, you can download the same files from the **Transferred files** area.



Session information

User name : [redacted]_USER@10.[redacted].51
Target : user_1@local@[redacted]_SSH_[redacted]_SUBPROTOCOLS:22
Target host/IP : 10.[redacted].148
SRC/DST protocol : SSH/SSH_SHELL_SESSION
Start time : 2022-12-21 06:27:51
End time : 2022-12-21 06:27:53
Duration : 0:00:02
Result : Success
Description : --

SSH viewer

Transcription

```
Linux debian-services 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/[redacted].

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 21 06:27:44 2022 from 10.[redacted].51
/sbin/ifconfig eth0
user_1@debian-services:~$ /sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:[redacted]
          inet addr:10.[redacted].148  Bcast:10.[redacted].255  Mask:255.[redacted].0
          inet6 addr: 2a0d:5d40:888:[redacted] Scope:Global
          inet6 addr: fe80::250:[redacted] Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:83573013 errors:0 dropped:28175 overruns:0 frame:0
          TX packets:75794236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85204914658 (79.3 GiB)  TX bytes:81178376361 (75.6 GiB)

user_1@debian-services:~$ /sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:[redacted]
          inet addr:10.[redacted].148  Bcast:10.[redacted].255  Mask:255.[redacted].0
          inet6 addr: 2a0d:5d40:888:[redacted]Scope:Global
          inet6 addr: fe80::250:[redacted] Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:83573020 errors:0 dropped:28175 overruns:0 frame:0
          TX packets:75794254 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85204915152 (79.3 GiB)  TX bytes:81178379205 (75.6 GiB)
```

Session metadata

```
2022-12-21 06:27:51 type="SESSION_ESTABLISHED_SUCCESSFULLY"
2022-12-21 06:27:52 type="KBD_INPUT" data="/sbin/ifconfig eth0"
2022-12-21 06:27:52 type="KBD_INPUT" data="/sbin/ifconfig eth0"
2022-12-21 06:27:52 type="SESSION_DISCONNECTION" duration="0:00:00"
```

7.2. Provide session description

About this task

You can use the session description field as a reminder for yourself. For example, if you kill a session, you can add a description to mention the reason you decided to end the session.

Descriptions are not shared with other users, but they are stored in the Bastion logs.

Procedure

1. Go to the **Audit > Session history** page.
2. Click the line that corresponds to the session you want to.
   This expands the row with a new **Description** option.
3. Click **Add**.
4. Enter the description and click **Save**.

Results

You can edit your description at any time by clicking the corresponding line and then clicking **Edit**.

8. Account history

From the **Audit > Account history** page, auditors can control the activity on the target accounts, including access to the password change history.

How to read account history information

For each account, there are several pieces of information available:

Account name

The name of the target account.

Domain

The name of the domain on which the target account is registered.

External vault

Whether the target account credentials are stored in an external vault or not.

Device name

The name of the attached device, if any.

Application name

The name of the attached application, if any.

Activity

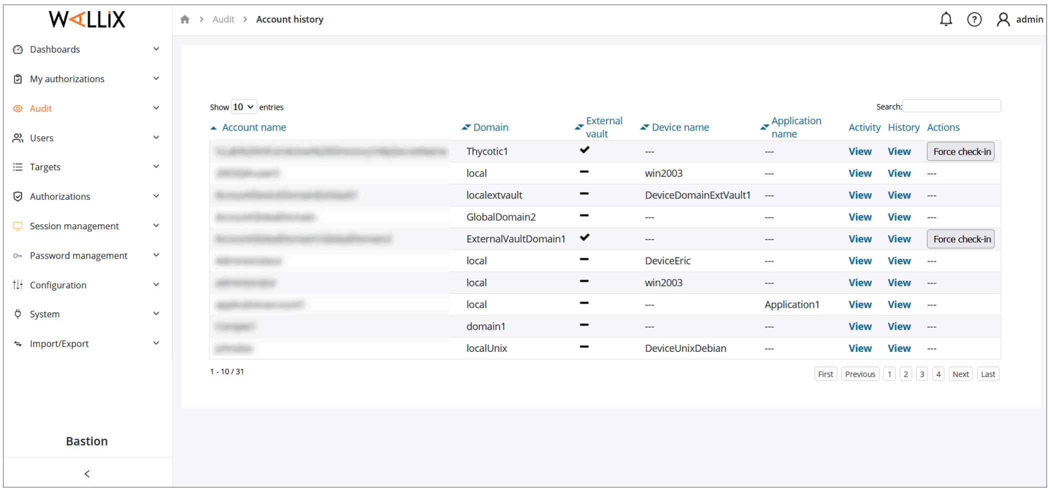
Access the activity history for the account on a dedicated page. This dedicated page displays a table listing the check-in and checkout operations on the account's credentials recorded for a given date and time.

History

Access the account's password change history on a dedicated page. This dedicated page displays information related to the account's password or SSH key changes for a given date and time.

Actions

The **Force check-in** option is available for accounts checked out by users to check-in the credentials for the account. For more information on the procedure, refer to [Force check-in *(on page 26)*](#).



Account name	Domain	External vault	Device name	Application name	Activity	History	Actions
[redacted]	Thycotic1	✓	---	---	View	View	Force check-in
[redacted]	local	−	win2003	---	View	View	---
[redacted]	localextvault	−	DeviceDomainExtVault1	---	View	View	---
[redacted]	GlobalDomain2	−	---	---	View	View	---
[redacted]	ExternalVaultDomain1	✓	---	---	View	View	Force check-in
[redacted]	local	−	DeviceEric	---	View	View	---
[redacted]	local	−	win2003	---	View	View	---
[redacted]	local	−	---	Application1	View	View	---
[redacted]	domain1	−	---	---	View	View	---
[redacted]	localUnix	−	DeviceUnixDebian	---	View	View	---

8.1. Force check-in

About this task

The current RDP or SSH session is not closed when the credentials of the account check-in is forced.

The **Force check-in** option is always available for the accounts defined on a global domain associated with an external password vault.

Procedure

1. Go to the **Audit > Account history** page.
2. Find the account for which you want to force the check-in.
3. Click the corresponding **Force check-in** button.
4. Explain why you are forcing the check-in on this target account and click **Force check-in**.

9. Approval history

The approval workflow feature makes it mandatory for users to send a request before they can access and use a target. The approval request is sent to trusted users called **Approvers** who must approve or deny the user request to access a target. From the **Audit > Approval history** page, auditors can view all the approval requests for session connections, including pending or expired requests.

How to read approval information

> **Note:**
>
> Only the last 1,000 records are displayed in the web user interface. The occurrence filter is applied to these 1,000 records. Older sessions can only be retrieved through the date range filter.

For each approval request, there are several pieces of information available:

Status

The current status of the approval request. It can be accepted, rejected, pending, closed, or expired.

Quorum

The number of current approvals against the number of required approvals to validate the user request.

Ticket

If the approval request is linked by the requesting user to a ticket number, this shows the ticket reference number.

User

The name of the user who requested access to the target.

Target

The name of the target that the user wants to access.

Beginning

The request start date and time for the session.

End

The request end date and time for the session.

Duration

The request duration for the user session.

Answers

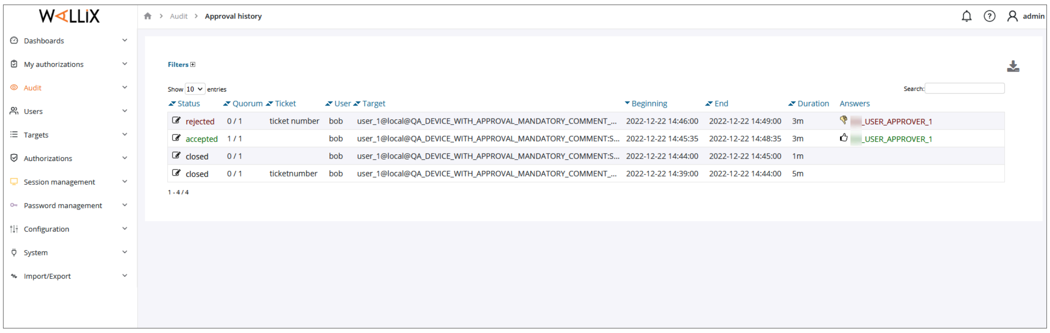
The answers of solicited approvers.

You can apply filters to refine the search and only display relevant records. The available filters are the following:

- the definition of a period, with a start and end date
- the definition of the last N days, weeks, months
- a search by text occurrences in the columns

A click on the ✎ icon located at the beginning of the line allows the auditor to get a detailed view of the request.

All data listed on this page can be downloaded as a .csv file.



Status	Quorum	Ticket	User	Target	Beginning	End	Duration	Answers
rejected	0 / 1	ticket number	bob	user_1@local@QA_DEVICE_WITH_APPROVAL_MANDATORY_COMMENT_...	2022-12-22 14:46:00	2022-12-22 14:49:00	3m	[redacted]_USER_APPROVER_1
accepted	1 / 1		bob	user_1@local@QA_DEVICE_WITH_APPROVAL_MANDATORY_COMMENT:S...	2022-12-22 14:45:35	2022-12-22 14:48:35	3m	[redacted]_USER_APPROVER_1
closed	0 / 1		bob	user_1@local@QA_DEVICE_WITH_APPROVAL_MANDATORY_COMMENT:S...	2022-12-22 14:44:00	2022-12-22 14:45:00	1m	
closed	0 / 1	ticketnumber	bob	user_1@local@QA_DEVICE_WITH_APPROVAL_MANDATORY_COMMENT_...	2022-12-22 14:39:00	2022-12-22 14:44:00	5m	

1 - 4 / 4

10. Authentication history

From the **Audit > Authentication history** page, auditors can view the authentication attempts on the RDP and SSH proxy interfaces (respectively on ports `3389` and `22`).

How to read authentication information

> **Note:**
>
> Only the last 1,000 records are displayed on the web interface. The occurrence filter is applied to these 1,000 records. Older sessions can only be retrieved through the date range filter.

Each line provides the following information:

Timestamp

The date and time of the authentication attempt.

User name

The name of the user account who attempted to authenticate.

For the Session invite feature, an additional line is displayed for the name of the guest user who logged into a shared session (as follows: `_GUEST_identifier`).

Authentication attempts with an expired OTP are not attributed to a user and are logged as `[unknown username]`.

Source IP

The IP address from which the authentication originated.

Result

The result of the authentication attempt in the form of a success or failure icon.

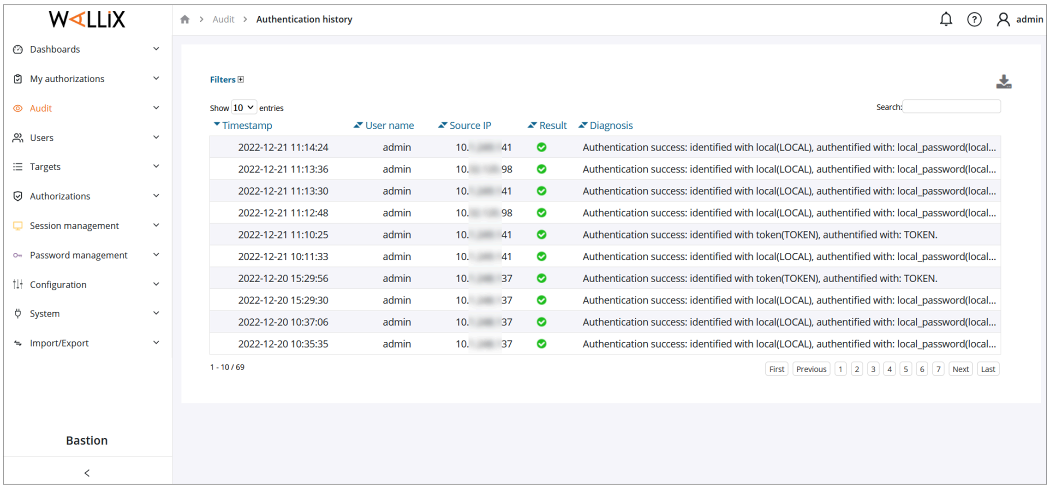
Diagnosis

The diagnosis provides more details on the authentication result.

You can filter the list of authentication attempts to only display relevant records. The available filters are the following:

- the definition of a date range with a start and end date
- the definition of the last N days, weeks, or months
- a search by text occurrences in the columns. For example, you can search for attempts by a specific user name.

> **Tip:**
>
> All data on this page can be downloaded as a .csv file.



Timestamp	User name	Source IP	Result	Diagnosis
2022-12-21 11:14:24	admin	10.[redacted]41	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-21 11:13:36	admin	10.[redacted]98	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-21 11:13:30	admin	10.[redacted]41	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-21 11:12:48	admin	10.[redacted]98	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-21 11:10:25	admin	10.[redacted]41	✓	Authentication success: identified with token(TOKEN), authentified with: TOKEN.
2022-12-21 10:11:33	admin	10.[redacted]41	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-20 15:29:56	admin	10.[redacted]37	✓	Authentication success: identified with token(TOKEN), authentified with: TOKEN.
2022-12-20 15:29:30	admin	10.[redacted]37	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-20 10:37:06	admin	10.[redacted]37	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...
2022-12-20 10:35:35	admin	10.[redacted]37	✓	Authentication success: identified with local(LOCAL), authentified with: local_password(local...

1 - 10 / 69

11. Metrics and reports

11.1. View connection statistics

About this task

Auditors can view statistical information on connections made through WALLIX Bastion for a given period of time.

Procedure

1. Go to **Audit > Connection statistics**.
2. From filters, ensure **Statistics** is selected from the drop-down list.
3. Define how many elements you want to include in the reports. The maximum is 35.

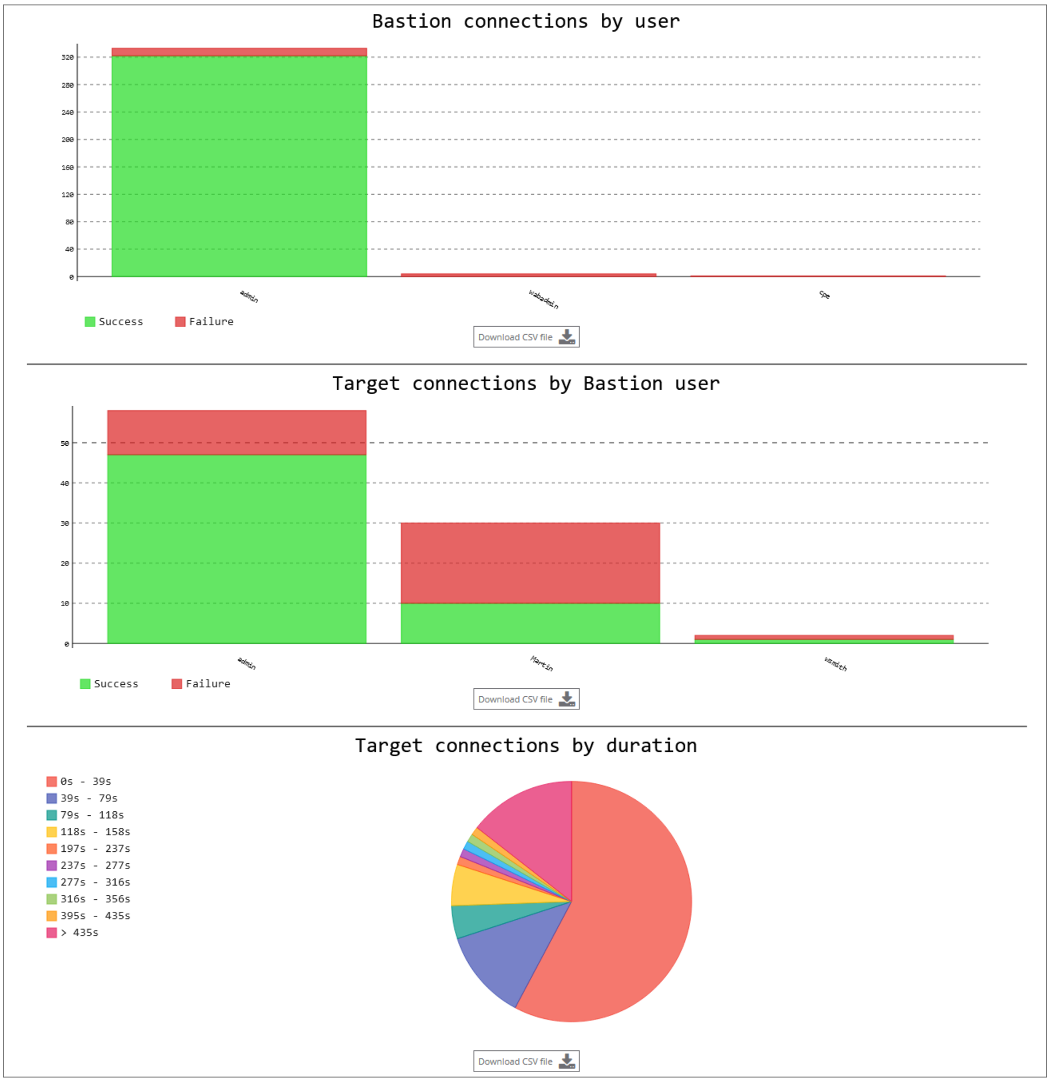
   By default, the most frequently occurring events are included in the report. You can display the less frequently occurring events instead by enabling **Reverse top N data**.
4. Select which elements you want to include in the report:
   - the number of target connections by device
   - the number of target connections by target account
   - the number of WALLIX Bastion connections by user
   - the number of target connections by user
   - the target connections by duration
   - the total target connection duration by user
   - the number of target connections by date
   - the maximum parallel target connections by date
5. **Optional:** If you want to restrict the report to relevant records, enable **Advanced filters**.

   The available filters are based on the selection among the WALLIX Bastion users and/or devices and/or targets. A summary of all the selected elements is displayed.
6. Select the timeframe for which you want to generate statistics.
   - **Start date** lets you configure a start and end date to define a period of time.
   - **Last** lets you define a number of days, weeks, or months until a specific date.
7. Click **Generate charts**.

Results

When the charts are generated, a table in the header lists the selected filters. There is a button under each graph to download a CSV file presenting the related data. The auditor can click charts related to the WALLIX Bastion and target connections to get the corresponding detail on the authentication_history or the session_history.

Example of statistical report



11.2. View unused user accounts

Procedure

1. Go to **Audit > Connection statistics**.
2. From filters, select **Unused resources** from the drop-down list.
3. Select **Users**.
4. Select the timeframe for which you want to retrieve the list of unused user accounts.
   - **Start date** lets you configure a start and end date to define a period of time.
   - **Last** lets you define a number of days, weeks, or months until a specific date.
5. Click **View data** or **Download data**.

11.3. View unused targets

Procedure

1. Go to **Audit > Connection statistics**.
2. From filters, select **Unused resources** from the drop-down list.
3. Select **Targets**.
4. Select the timeframe for which you want to retrieve the list of unused targets.

  - **Start date** lets you configure a start and end date to define a period of time.
  - **Last** lets you define a number of days, weeks, or months until a specific date.

5. Click **View data** or **Download data**.

12. Annex

12.1. Glossary

4 eyes

Mechanism allowing an auditor to monitor the session of another user without gaining control over it.

4 hands

Mechanism allowing an auditor to gain control over the current session of another user.

Access control list (ACL)

System allowing a thorough management of resource access (an equipment, a file, etc).

Account

Entity managed by WALLIX Bastion or by an external secrets vault allowing a user to be authenticated to a system and to be granted a certain level of authorization to access resources on that system, for management purposes. An account belongs to a domain.

Account lock

Mechanism preventing the concurrent use of an account.

Account mapping

Mechanism allowing a user to establish a connection to a resource using their credentials (user name and password), especially when the user account is declared on a company directory and is granted access to the target resource.

Appliance

Model under which WALLIX Bastion is available. The machine is either physical (already mounted, configured and ready to be plugged in and booted) or virtual (requiring images deployment and installation before its configuration).

Application cluster

Group of jump servers allowing application load balancing and High-Availability (HA).

Approval request

Request submitted by a user to receive access to a target. The request is sent to approvers who then accept or reject it via the WALLIX Bastion.

Approval workflow

Mechanism meant to restrict and control connection or user access to targets or target credentials. Users need to send a request to approvers before they can access a specific target and its sensitive information.

Audit

Set of processes and features allowing the monitoring, recording, and analysis of user activities when they have access to systems and resources from WALLIX Bastion, for security purposes.

Authentication agent

Component of authentication allowing to check the identity of a user before granting access to secured resources.

Authentication transfer

Option embedded in WALLIX Bastion allowing a transparent and secured authentication in which the user does not need to know or use the credentials.

Authorization

Object in the Bastion configured by administrators to give users rights to access sessions on targets and their secrets.

Auto-deployment upgrade

Approach for WALLIX Bastion upgrade in HA Database Replication mode that enables a clone of the cluster to immediately deploy to production when the upgrade finishes. This straightforward approach carries higher risks and does not provide testing opportunities.

Auto logon

Process allowing an automatic connection to a target without viewing or knowing its password.

Automatic credential injection

Mechanism where users do not have to not know or access credentials to open a target resource, the credentials are provided to the target automatically.

Backup

Process generating a copy of the configuration and settings of a WALLIX Bastion at a given moment in time.

Bastion cluster

Set of Bastion servers allowing load balancing and High-Availability (HA). WALLIX Bastion uses clusters whose architecture contains a number of database instances working together to manage the storage of sensitive information.

Break Glass

Feature which allows a trusted user, in case of emergency, to obtain the credentials for target groups gathered in WALLIX Bastion (including logins, common names, passwords, and SSH keys.)

Check-in

Operation consisting in releasing the credentials of a given account, complementary to the checkout action.

Checkout

Operation consisting in recovering and displaying the credentials of an account. The lock of the account can be configured during this operation to prevent concurrent use by multiple users.

Checkout policy

Rules determining the settings concerning the account checkout process. When the lock is enabled in the checkout policy associated with a target account currently changing password, the account remains locked for the duration defined in this policy.

Client

Application connecting to a company's IT resources via communication protocols (SSH or RDP) through the Bastion. The latter secures these connections by providing access management and control meant to increase security.

Connection policy

Security rules determining what conditions are required of users to access resources protected by the Bastion. They apply to users or user groups, target resources, protocols and other access methods, access conditions, as well as audit configuration.

Connection scenario

Scenario meant to automate connection to a device that does not offer protocols supporting the automated sending of credentials (TELNET or RLOGIN).

Controlled deployment upgrade

Approach for WALLIX Bastion upgrade in HA Database Replication mode ensuring minimal disruptions to the production environment. The upgrade impacts are tested and validated on a copy of the cluster before deploying it to production.

Credential / Authentication information

Information meant to check the identity of a user and which corresponds to their user name and password. Credentials include access rights and authorizations that are specific to the user after authentication.

Critical session

Session considered high-risk regarding its sensitive information and coming with additional warnings and notifications.

Device

Physical or virtual device which can be associated to an account whose access to sessions or secrets is managed by WALLIX Bastion.

Discovery

Module allowing the automatic and continuous discovery of resources (devices and accounts) on configured networks and Active Directories and providing the ability to onboard the discovered resources.

External authentication

Authentication managed by a third-party external to WALLIX Bastion in the context of a primary connection, meaning the authentication of users to WALLIX Bastion.

Global account

User account providing access to multiple targets or target groups in the infrastructure of the organization whose management is centralized in WALLIX Bastion.

Global domain

Management entity grouping multiple target accounts that can be used to authenticate across multiple devices. A secret rotation process can be applied to all accounts in the global domain which can then be associated with an external secrets vault.

HA Database Replication

High-availability feature ensuring that a cluster of Bastions can manage potential disruptions and guaranteeing continuous data availability. This is due to automatic replication of data from one server to other servers, whether these are physical appliances in the same environment or hosted on virtual machines. WALLIX Bastion offers two different modes: Master/Master and Master/Slaves.

Interactive login

Mechanism allowing a user to dynamically enter credentials to access a target resource.

Local account

User account specific to a given target (such as a server, an application, or a database) and configured locally on the target.

Local authentication

Authentication managed by WALLIX Bastion in the context of a primary connection, meaning the authentication of users to WALLIX Bastion. In this situation, WALLIX Bastion manages and stores all information for user authentication.

Local domain

Management entity grouping multiple target accounts that can be used to authenticate on a single device. A secret rotation process can be applied to all accounts in the local domain. Users can be directly defined in WALLIX Access Manager, given that a local domain is created for each of its organizations.

Local storage

Storage of data directly on the server where the WALLIX Bastion is installed as to provide quick access to recent data.

Login transformation rule (LTR)

Rule based on a character string defining the transformation of a login retrieved for connecting on a target account.

Log

Recording in detail of events and actions occurring in the WALLIX Bastion infrastructure so as to keep total track of every user and administrator activity, for auditing purposes.

Major upgrade

Upgrade providing the product with new features, or even its restructuring.

Manual logon

Target connection mode allowing a manual connection using the password.

Minor upgrade

Upgrade done regularly to make sure the product is up to date and secured, often through bug fixing.

Multi-tunneling

Option allowing the user to access as many IPv4 network interfaces as configured by the WALLIX Bastion administrator in the Universal Tunneling service in one session.

Pattern detection

Detection of certain character sequences leading to restriction actions ("Kill" to disconnect the session and "Notify" to send a notification). The data analyzed is either the data entered by the user or the data displayed on the screen.

Permission profile

Set of user rights and authorizations that are assigned either as default profiles or customized profiles to further refine the delegation of rights.

Primary connection

Connection initiated between a user and WALLIX Bastion.

Remote storage

Storage of large volumes of data in the long term on an external storage system or a remote server.

Resident agent

Software installed on target systems whose access is managed by WALLIX Bastion through the control and monitoring of their activities. The client's authentication parameters, which are automatically transferred to WALLIX Bastion, are then used for authentication when logging on to target devices.

Resource

Association either of a service and an equipment, or of a service and an application. A target is the association of a resource and a target account.

Restoration

Mechanism allowing to roll back from a configuration using a backup. This can undo a misconfiguration, or retrieve the prior state of a database, etc.

Scenario account

Type of account designed to automate repetitive tasks that are then executed on target systems. For example, target accounts can be used by a startup scenario at the beginning of an SSH session.

Seamless connection

Option allowing the user to access targets using Universal Tunneling without having to reconfigure the fat client or workstation to successfully redirect traffic through the SSH tunnel.

Secondary connection

Connection initiated between WALLIX Bastion and a target.

Secret

Credentials required to access systems, applications or secured databases. Access rights to secrets allow users to access secrets related to targets.

Secret rotation plugin

Previously called "Password rotation plugin."

Extension allowing the configuration of secret rotations for targets.

Secret rotation policy

Previously called "Password rotation policy."

Rules determining the settings for password or SSH key rotations.

Secret rotation

Process used to automatically or manually change the password or SSH key of target accounts before spreading these modifications to the targets. A secret rotation plugin applies these modifications to each domain.

Secrets vault

Structure allowing the secure storage of secrets (passwords, SSH keys) and their automatic rotation. The external or local vault also allows account configuration through policies meant to enforce a specific account usage.

Secret vault plugin

Extension linking the local Bastion instance to the external vault. It represents the secrets vault of the remote Bastion instance.

Session invite

Feature allowing a user (the host) to share their session with an external user (the guest) who does not have an account in WALLIX Bastion or WALLIX Access Manager.

Session

Period of time during which the user (or a service account) is connected to a system, an application or an IT resource through WALLIX Bastion. Access rights to sessions allow users to access sessions on targets.

Sessions access are configured by administrators and enable users to access targets in a tracked and controlled way.

Session probe

Mode only available on RDP Windows target servers allowing the collection of a rich set of session metadata related to user activities. It creates passive monitoring, especially through session recording, and interrupts neither sessions nor user actions.

Session recording

Recording of RDP or SSH sessions authorized and viewed by auditors through a session video player embedded in WALLIX Bastion. Their encryption allows only the WALLIX Bastion instances which created them to access these recordings.

Session sharing

Feature allowing real-time audit capability which grants auditors access to a user's session, thus guaranteeing its security. Auditors of RDP sessions can remotely control a user's session.

Startup scenario

Scenario which can be used at the beginning of the SSH Shell session to perform some actions such as assigning the user the "root" privileges using "su" and "sudo" commands without having knowledge of the password.

Target account

Association of a device, a service and an account, which corresponds to every device isolated by WALLIX Bastion with their associated accounts. These accounts are used on the target.

Target application

Association of an application and an account that can be accessed by users through the Bastion. This type of target separately gives access to an application without giving access to an entire remote desktop session.

Target group

Feature embedded in WALLIX Bastion which allows the gathering of different systems or servers (targets) with similar characteristics or management requirements : every target from a group is handled according to the same authorizations. The definition of these authorizations creates a link between a target group and a user group that determines access rights.

Transparent mode

Feature allowing the Bastion to intercept network traffic for a target even when the user specifies the target's address instead of using the WALLIX Bastion address.

Universal Tunneling (UT)

Previously called RAW TCP/IP.

Feature allowing the user to redirect TCP traffic from their workstation to the target. The traffic is always redirected to a local address but can also be redirected to a temporary interface to allow a transparent and fluid configuration using Seamless connection.

User group

Set of users defined to simplify access management and authorizations to targets by applying them to different users at the same time and according to their authorizations to access resources.

Vault transformation rule (VTR)

Rule based on a character string and defined to retrieve the credentials of an existing account in the WALLIX Bastion vault for a target account configured for account mapping.

Index

Our WALLIX Support Team is available to help you during hours defined in your support contract:

Web: https://support.wallix.com/

Phone: (+33) (0)1 70 36 37 50 for Europe, Middle East and Africa and (+1) 438-814-0255 for the Americas.

About WALLIX

A software company providing cybersecurity solutions, WALLIX is the European specialist in Identity and Access Security Solutions. WALLIX PAM, the unified access and privilege management solution, enables companies to respond to today's data protection challenges. It guarantees detection of and resilience to cyberattacks, which enables business continuity. The solution also ensures compliance with regulatory requirements regarding access to IT infrastructures and critical data.

WWW.WALLIX.COM