BASTION

ADMINISTRATION GUIDE

WALLIX Access Manager 5.0.3.0

Reference: https://doc.wallix.com/en/am/5.0.3.0/am-admin-guide

WALLIX

CYBERSECURITY SIMPLIFIED

Table of Contents

Chapter 1. Introduction

1.1. Preamble

Thank you for choosing WALLIX Access Manager, also called Access Manager.

The WALLIX Access Manager solution is marketed as a virtual device for the following virtual environments:

- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Kernel-based Virtual Machine (KVM)
- Microsoft Azure
- Microsoft Hyper-V
- Nutanix AHV
- OpenStack
- VMware vSphere

This product has been engineered with the greatest care by our teams at Wallix and we trust that it will deliver complete satisfaction.

1.2. Copyright, licenses

WALLIX Access Manager is subject to the WALLIX software license contract.

WALLIX Access Manager is based on open-source software. The related list is available from WALLIX. Please send your request on Internet by creating a new case at `https://support.wallix.com` or in writing to:

WALLIX
Service Support
250 bis, Rue du Faubourg Saint-Honoré
75008 PARIS
FRANCE

1.3. Legend

```
prompt $ command to input <parameter to replace>
command output
on one or more lines
prompt $
```

1.4. About this document

This document is the Administration Guide for WALLIX Access Manager 5.0.3.0. Use it to configure the product prior to roll-out, and also for its administration and day-to-day operation.

Chapter 2. Compatibility & limits

Please refer to the *Release Notes* document to check the compatibility of WALLIX Access Manager 5.0.3.0 with various clients or targets and learn more about the known issues and also the technical requirements and feature enhancements of this latest version.

2.1. Limits on RDP sessions

The connection to RDP sessions on tablets or smartphones has the following limitations:

- screen rotation is not possible
- multi-touch screens are not supported
- long press on an interface element to simulate a right mouse click is not supported.

Chapter 3. Overview

The WALLIX Access Manager (Access Manager) provides connection services between web browsers and targets on which users are authorized to log on. Target accesses are performed through Wallix Bastion appliances. The connections are done using HTML5 clients; no browser plug-in is required. Access Manager enables also users with the proper rights to display target passwords in the browser and/or to copy them directly to the clipboard.

Access Manager configuration supports multi-tenancy using containers named “Organizations” as described in Chapter 8, *Multi-tenancy and organizations*.

The database settings are configured as explained by Chapter 17, *Database settings*.

The configuration of the Wallix Bastion deployed by the organisation is described in Chapter 13, *Bastions*.

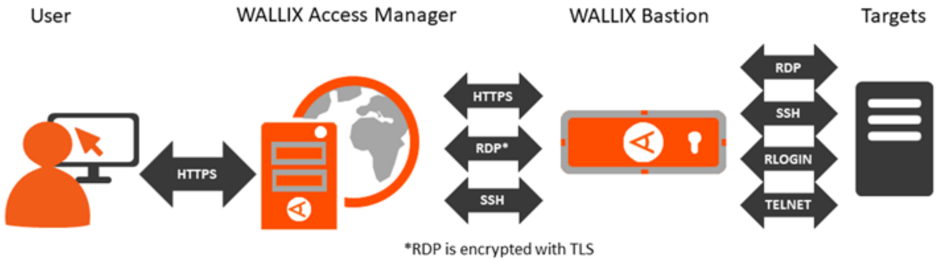

Figure 3.1. Flow diagram

Chapter 4. Licenses

Access Manager is controlled by a license key provided by WALLIX which contains the elements included in the sales contract.

Licenses are managed from the “Access Manager License” deployable area in the “About ...” page, accessible by clicking on the “i” icon located on the right part of the top menu bar.

> ***Important:***
>
> Only an administrator of the global organization can access the “Access Manager License” deployable area, and manage the licenses.
>
> During the initial installation, Access Manager creates a 31-day evaluation license which allows up to 5 concurrent users.

To obtain or upgrade a license, a context file must be created and sent to WALLIX Support (https://support.wallix.com/). To do so, click on the “Download Context File” button to generate and download a context file and send it to the WALLIX Support Team which will provide you with a license file.

Once you have received the license file, drag-and-drop it in the “Access Manager License” section and click on the “Upload License” button.

For each license installed on Access Manager, the following information is provided:

- the license validity period
- the license entitlements: either an unlimited number of concurrent users or a limited number of concurrent users

> ***Note:***
>
> Connections of the administrator of the global organization are not counted.

- the license type: EVALUATION, STANDARD, PROVISIONAL, EXPIRED and REVOKED
- the number of users connected and the total number of concurrent users allowed.

> ***Note:***
>
> When several licenses overlap, then the entitlements of these licenses add up. As an example: if two licenses are installed and allow 100 concurrent users and 50 concurrent users, then the number of concurrent users allowed is 150.

All standard licenses installed on Access Manager can be revoked by clicking on the `Revoke Licenses` button. After confirming the revocation, 15-day provisional licenses including the entitlements of each revoked license are created. At the end of those 15 days, Access Manager will no longer work.

4.1. Managing licenses from the command line

The licenses can be managed from the command line when logged in as “root”.

To display the list of the valid licenses with their validity date and metrics, the following command must be executed:

```
/opt/wab/sbin/wabam-license-list
```

To download the context file, the following command must be executed:

```
/opt/wab/sbin/wabam-context-file-download -c <path to the context file>/<name of
 the context file.json>
```

```
For example:
/opt/wab/sbin/wabam-context-file-download -c /tmp/licenses/
wabam_context_file.json
```

The `[--configfile -f]` option helps you to define the path to the configuration file and its name. If the option is not defined, the default configuration file path and name are automatically used.

To import a new license, the following command must be executed:

```
/opt/wab/sbin/wabam-license-import -l <path to the license file>/<name of the
 license.json>
```

```
For example:
/opt/wab/sbin/wabam-license-import -l /root/wallix_license.json
```

To revoke the licenses, the following command must be executed:

```
/opt/wab/sbin/wabam-revoke
```

Warning:

After confirming the revocation, 15-day provisional licenses including the entitlements of each revoked license are created. At the end of those 15 days, Access Manager will no longer work.

Chapter 5. SNMP

The Access Manager appliance includes an embedded SNMP agent with the following properties:

- Protocol versions supported: 2c, 3
- MIBs implemented: MIB 2, DISMAN-EVENT-MIB
- Support of alert mechanisms ("traps") and notifications related to disk consumption and CPU load
- No ACL on the source IP address

> ***Note:***
>
> Port 161 should be opened to allow communication to Access Manager for read/write access to OIDs.
>
> Port 162 should be opened to allow communication from Access Manager for trap notifications.
>
> A default minimum value set to 20 concurrent connections is required for each port.

From the "SNMP" page on the "System" menu of WALLIX Appliance, you can configure this agent by defining the related settings:

The "General Settings" section consists of the following fields:

- "Sysname": The name of the system, e.g., "WALLIX Access Manager 5.0.3.0"
- "Syscontact": The email address of the system administrator, in format "snmp@example.com"
- "Syslocation": The system location
- "Sysdescr": A description, if needed. This field is empty by default.
- "Status": Drop-down list to enable or disable the SNMP agent. The agent is disabled by default.
- "Enable trap notifications": Check box to enable SNMP trap notifications. Trap notifications are disabled by default.
- "Trap sink": The address of the receiver. This field is displayed and required when trap notifications are enabled.

The "SNMPv2 Settings" section consists of the following fields:

- "Disable SNMPv2 ": Check box to disable the SNMP protocol version 2c
- "Community": The community name used to connect to Access Manager. This field is displayed and required when the SNMP protocol version 2c has been enabled.
- "Trap community": The community name used when trap messages are sent. This field is displayed and required when trap notifications and the SNMP protocol version 2c have been enabled.

The "SNMPv3 Settings" section consists of the following fields:

- "Authentication passphrase": The authentication passphrase. This field must be longer than 8 characters. The authentication passphrase must be set at the same time as the encryption passphrase.
- "Encryption passphrase": The secret key for encryption. This field must be longer than 8 characters. The encryption passphrase must be set at the same time as the authentication passphrase.

- “Trap receiver configuration”: This sub-section is displayed when trap notifications have been enabled and the SNMP protocol version 2c has been disabled. It consists of the following fields:
  - “Trap user”: The user name used to authenticate on the trap receiver. This field is empty by default.
  - “Security level”: Button to select the appropriate security level and specify the related fields depending on the selection.

    If “Authentication only” is selected, enter and confirm the authentication passphrase and select the authentication ciphering scheme (SHA or MD5).

    If “Authentication and encryption” is selected, enter and confirm both the authentication and encryption passphrases and select the related ciphering schemes (SHA or MD5 for authentication and AES or DES for encryption).

The “Threshold values (%)” section consists of the following fields:

- “Disk consumption”: The percentage value related to the disk consumption. Notifications are sent when the disk consumption exceeds this value.
- “Average CPU load”: The percentage values related to the average CPU load for 1-minute, 5-minute and 15-minute time slices. Notifications are sent when these values are exceeded.

The values entered in this section can be reset by clicking on the “Reset default threshold values” button on the botton-left of the section.

Warning:

By default, the SNMP agent is disabled and can only be enabled via the Web interface.

By default, trap notifications are disabled and they can only be enabled via the Web interface. When enabled, only acknowledged traps (i.e. INFORM traps) are sent.

By default, the SNMP protocol version 2c is disabled on a fresh Access Manager and can only be enabled via the Web interface.

The SNMP protocol version 3 is always enabled. However, both authentication and encryption passphrases must be set at the same time for proper operation.

When Access Managers are configured in HA mode, the SNMP agent monitors all the nodes via the virtual IP address.

Example of use for SNMP protocol version 2c:

```
$ snmpget -v2c -c WALLIXdefault 192.168.0.5 system.sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: "Access Manager Version 5.0.3.0"
$ snmpget -v2c -c WALLIXdefault 192.168.0.5 system.sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (65833) 0:10:58.33
$ snmpget -v2c -c WALLIXdefault 192.168.0.5 IF-MIB::ifHCOutOctets.1
IF-MIB::ifHCOutOctets.1 = Counter64: 255823831
```

Examples of use for SNMP protocol version 3:

```
$ snmpget -v3 -l authPriv -u wabsnmp -a SHA -A <authpass> -x AES -X <privpass>
 192.168.0.5 system.sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: "Access Manager Version 5.0.3.0"
$ snmpget -v3 -l authPriv -u wabsnmp -a SHA -A <authpass> -x AES -X <privpass>
 192.168.0.5 system.sysUpTime.0
```

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (65833) 0:10:58.33
$ snmpget -v3 -l authPriv -u wabsnmp -a SHA -A <authpass> -x AES -X <privpass>
 192.168.0.5 IF-MIB::ifHCOutOctets.1
IF-MIB::ifHCOutOctets.1 = Counter64: 255823831
```

Warning:

The system OIDs are defined in the MIB “SNMPv2-MIB”. Please make sure this MIB is installed on your client environment.

Chapter 6. Metric measurement tool

Access Manager includes a tool for collecting numerical data within Access Manager. This data is used to estimate the capacity of the license and the size allocated to the resources. This tool is accessible by running the following command line:

```
docker exec -it access-manager_access_manager_1 /opt/wallix/wabam/bin/wabam-audit-data -b <date> -a <date> -t <type>
```

The `[--help -h]` option displays the help message listing the arguments that can be used.

The `[--after -a /(\d{2}|\d{4})-\d{2}-\d{2}/]` option allows you to get information posterior to the date specified. The format is as follows: YYYY-MM-DD or YY-MM-DD.

The option `[--before -b /(\d{2}|\d{4})-\d{2}-\d{2}/]` allows you to get information previous to the date specified. The format is as follows: YYYY-MM-DD or YY-MM-DD.

The option `[--type -t value]` allows to specify the information to be returned. The returned information corresponds to one of the following values:

- `NB_USERS`: number of distinct users who have connected to Access Manager over a period of time
- `NB_TARGET`: number of distinct connections to targets over a period of time
- `NB_CONCURRENT_USERS`: maximum number of users who have connected simultaneously to Access Manager over a period of time (only for a MySQL database)
- `NB_RDP_SESSION_OPENED`: number of RDP sessions opened over a period of time
- `NB_VNC_SESSION_OPENED`: number of VNC sessions opened over a period of time
- `NB_SSH_SESSION_OPENED`: number of SSH sessions opened over a period of time
- `NB_SFTP_SESSION_OPENED`: number of SFTP sessions opened over a period of time
- `NB_SCP_UP_DOWN`: number of uploads and downloads via SCP
- `NB_REMOTE_COMMAND`: number of remote commands executed
- `ALL`: all data listed above

The number of active SSH, RDP and RAWTCPIP sessions can also be retrieved from the Access Manager servers of a cluster, by executing the following command:

```
/opt/wab/sbin/wabam-session-count
```

The result of the command is:

```
{
  "<AM_instance_1>":<nb_session>,
  "<AM_instance_2>":<nb_session>,
  ...
}
```

Where `<AM_instance_x>` is the universally unique identifier (uuid) of the instance (i.e. the value of the `wabam.uuid` parameter in `wabam.properties`), and `<nb_session>` is the number of active sessions on this instance.

> ***Note:***
>
> If an instance has no current sessions, its uuid is not displayed in the result.

The `-i` optional parameter can be added to only retrieve the number of active SSH, RDP and RAWTCPIP sessions for the Access Manager server the command is executed on:

```
/opt/wab/sbin/wabam-session-count -i
```

The `-h` option displays the help message listing the options available:

```
/opt/wab/sbin/wabam-session-count -h

The options available are:
        --configfile -f value : name and path of config file to be used -
 already included in the executable.
        [--help -h] : list the arguments that can be used to get current number
 of target sessions.
        [--onlyCurrentInstance -i] : get the number of current sessions only for
 this AM instance
```

Chapter 7. User preferences

A logged-in user has the possibility to change his or her preferences at any time, regardless of his or her profile and the organization he or she belongs to.

Preferences can be changed from the "Preferences" page, which can be accessed by clicking on the logged-in user name on the right part of the top menu bar.

The user preferences are defined by the following attributes:

In the "Identity" section

- `Login`: The value provided by the user to identify himself or herself.
- `Name`: The value displayed to the screen as the logged-in user name.
- `Email`: The email address of the logged-in user. This address can be changed.
- `Organization`: The organization on which the user is currently logged in.
- `Domain`: The authentication domain of the organization on which the user is currently logged in.
- `Change Password`: Toggle button to change the password of the logged-in user. It must comply with the password policy requirements defined for the organization. For further information, refer to Section 8.3, "Password policies".

In the "Application Options" section

- `Language`: The interface display language chosen by the logged-in user. Another language can be selected from the list.
- `Approval Time Zone`: The time zone of the user. This attribute allows for optimal synchronization of the steps of the approval workflow when WALLIX Access Manager and WALLIX Bastion are running in different time zones. If this parameter is not defined, then the default time zone set in the `wabam.properties` file is used during approval workflows.

  This default time zone can be changed by editing the parameter *`approval.time.zone`* parameter in the `wabam.properties` file which is available in the configuration directory: `/var/wab/etc/wabam`.

  > **Warning:**
  >
  > The parameter *`approval.time.zone`* must be configured with the time zone of the server to ensure proper synchronization of approvals. If the parameter *`approval.time.zone`* does not exist in the `wabam.properties` file or if no default time zone is entered for this parameter, then WALLIX Access Manager uses the time zone of the server on which it runs.
  >
  > After changing the parameters in the `wabam.properties` file, the Access Manager service must be restarted by restarting the Docker container.

- `Tab Displayed by Default for Authorizations`: The tab displayed by default on the "Sessions" and "Passwords" pages of the "Authorizations" menu.
- `Hierarchy of Tag Tree Structure for Sessions`: The hierarchy of the folders in the tree structure, on the "Tag Explorer" tab, defined by the logged-in user. This hierarchy is defined by the tag key names separated by the "/" character. The key names are case sensitive. If this attribute is not defined, then the hierarchy of the folders in the tree structure will be the default one or will be the hierarchy defined by the administrator of the organization.

- `Hierarchy of Tag Tree Structure for Passwords`: The hierarchy of the folders in the tree structure, on the "Tag Explorer" tab, defined by the logged-in user. This hierarchy is defined by the tag key names separated by the "/" character. The key names are case sensitive. If this attribute is not defined, then the hierarchy of the folders in the tree structure will be the default one or will be the hierarchy defined by the administrator of the organization.
- `Show Information Message on Universal Tunneling Target Prompt`: Toggle button to display a message when downloading the Universal Tunneling configuration file. This message informs the user of the procedure to follow to establish a connection from a Universal Tunneling (RAWTCPIP) client.

In the "Session Options" section

- `Target Password Saved for Account Mapping with SAML`: The password used to automatically log in to the target in the case of an account mapping-base authentication with SAML. Note that the password is not stored in Access Manager and is only available for the duration of the user's session. If the field is not specified, the password will be requested when connecting to the target.

  Once the password is saved, it can be changed by setting the "Update Target Password Saved for Account Mapping with SAML" button to "Yes" and then entering the new password.
- `Short Title in Session Tabs`: The format of the title displayed in the browser tab for the RDP, SSH and SFTP sessions. By enabling this attribute, the format of the title will be "login@target name" instead of the full authorization name. If this field is not selected, the format of the title will be the one defined by the administrator of the organization.
- `Keyboard Layout for Application Sessions, RDP and VNC Sessions`: The keyboard language for the application sessions and the RDP and VNC sessions, selected by the logged-in user before connecting to the target. If this field is not selected, the language of the keyboard is the last value selected or, if no value was previously selected, the American keyboard. At the opening of a session:
  - the keyboard layout of the RDP target will correspond to the keyboard layout selected in the user preferences
  - the keyboard layout of the application session and VNC target will correspond to the keyboard layout selected in the user preferences, and must also correspond to the keyboard layout of the system.

  The keyboard language can be changed in the RDP session via the dedicated option in the header bar. After changing the language, the keyboard layout of the RDP target must correspond to the keyboard layout selected in the user preferences and to the target language.

  > ***Note:***
  >
  > The keyboard language cannot be changed in a current application session and VNC session. To change the language, it is necessary to disconnect from the session.
- `Shell Theme for SSH Session`: The SSH session theme chosen by the logged-in user. Three themes are available: "Dark" (default theme), "Light" and "Black and white". The theme can also be selected in the SSH session via the dedicated option located in the header bar.
- `Copy/Paste of Text via PuTTY Mode for SSH Session`: The PuTTY mode to copy-paste text in the SSH session using the mouse. This mode is, however, not supported in Mozilla Firefox. To use this mode:
  1. Select the text by holding down the left mouse button.
  2. Release the mouse button to copy the text to the clipboard.

3. Move the cursor to the desired location and right-click to paste the copied text.

- `Show Scrollbar in RLOGIN, SSH and TELNET Session`: Toggle button to display a vertical scrollbar in the RLOGIN, SSH and TELNET sessions.
- `Universal Tunneling - Debug Mode`: Toggle button to enable the debug mode for Universal Tunneling (RAWTCPIP) sessions. This mode must be enabled before downloading the target configuration file. It enables detailed logs to be generated, providing valuable information for analysis and troubleshooting. The logs are stored in a file with the same name as the downloaded configuration file, followed by the .log extension.

Chapter 8. Multi-tenancy and organizations

Multi-tenancy is the ability to host multiple configurations within the same Access Manager server. A configuration is associated to an “Organization” object. An organization is a set of users and a set of WALLIX Bastion instances. A user and a WALLIX Bastion can belong only to a single organization.

Organizations can be added from the “Organizations” page accessible from the “Configuration” menu.

An organization is defined by the following attributes:

- `Name`: The name of the organization as it will be displayed in the application. This is a string of length between 1 and 128 characters.
- `Identifier`: A mandatory string of length between 1 and 64 characters. The authorized characters are uppercase and lowercase Latin alphabetical characters (A to Z). The identifier is used either as a path element of the URL just after the context path or as the first element of the fully qualified domain name (FQDN) of the host. Access Manager searches first in the path and then in the FQDN to identify the organization to use for the connection.

  Examples:

  - `https://mycompany.tld/wabam/myorg`: In this example, the context path is `wabam`. The URL refers to `myorg` as organization. The FQDN `mycompany.tld` is used for all organizations.
  - `https://myorg.mycompany.tld/wabam`: In this example, the FQDN `myorg.mycompany.tld` refers to `myorg` as organization.

  If no identifier is mentioned in the URL, then Access Manager will apply the following rule:

  - if there is only the global organization, Access Manager automatically redirects the user to the latter
  - if there is a single local organization, Access Manager automatically redirects the user to the latter
  - if there are several local organizations, Access Manager then prompts the user to enter the relevant organization in the URL.
- `Default Domain`: The domain to use if no domain is provided in the URL as explained in Chapter 10, *Authentication domains*.
- `Local Domain Name`: The name to use for referencing the local domain, mainly for the `local` parameter of the URL as explained in Chapter 10, *Authentication domains*.
- `Password Policy`: The password policy to use for the organization. For further information, refer to Section 8.3, “Password policies”.
- `Theme`: The theme to use for the organization. For further information, refer to Section 8.4, “Themes”.

When editing the organization, the expandable area `Authenticators Associated with Local Domain` is displayed at the bottom of the page. This area allows the local domain to be associated with the available authenticators when configuring a single-factor or a multi-factor authentication. These authenticators are the LDAP, RADIUS and BASTION servers configured for the organization in Access Manager. For further information, refer to Section 10.2.2, “Configuration of the LDAP server”, Chapter 11, *RADIUS authentication* and Chapter 13, *Bastions*.

The field `Login type` indicates the format of the login used for the authentication.

The field `Factor` defines the order in which the authenticators are queried during the authentication. Each authenticator used for the authentication must return a positive response in the order which has been defined. The authentication succeeds when all the authenticators are validated. If an authenticator fails, then the authentication fails.

The field `Priority` defines the order in which the authenticators with the same factor are used for High-availability (HA). If the first server does not return a response, then the next one is queried until a response is returned. If no server responds, the authentication fails.

From the list displayed on the “Organizations” page, it is possible to:

- duplicate an existing organization by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The organization creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new organization.
- delete an existing organization by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

8.1. The global organization

The **global** organization is a built-in organization whose default name is **`global`**. Users of this organization have the ability to access other organizations for administration purposes. Only users from the global organization can create organizations. Users belonging to other organizations can access only objects located in their own organizations.

Users from the global organization cannot have authorizations to connect to targets.

8.2. The default organization

When deploying Access Manager, an organization called **`default`** is created and available for normal use. However, this organization can be renamed and deleted.

8.3. Password policies

Each time a new organization is created, a default password policy is created for it. It is possible to create additional policies within the organization, but only one is active at the same time.

Password policies can be added from the “Password Policies” page accessible from the “Configuration” menu.

A password policy is defined by the following attributes:

- `Name`: Name of the password policy.
- `Allow non-ASCII characters`: Toggle button to allow or forbid non-ASCII characters in the password.
- `Min Length`: The minimum number of characters in a password. The smallest number is 4.
- `Max Length`: The maximum number of characters in a password. The maximum is 64.
- `Min Lowercase Chars`: The minimum number of lowercase alphabetic characters which must be present in the password.

- `Min Uppercase Chars`: The minimum number of uppercase alphabetic characters which must be present in the password.
- `Min Special Chars`: The minimum number of non-alphanumeric ASCII characters in the password.
- `Min Digit Chars`: The minimum number of digit characters which must be present in the password.
- `Last Password Diff Chars`: The number of different characters that must be present in the new password compared to the previous one. It is only applied to the previous password and not to the other passwords present in the history because the history keeps only one-way hashes. Users have to provide the current password to be able to change it.
- `Password History Size`: The size of the password history to keep. This history keeps only one-way hashes.
- `Expiration Delay`: The number of days before the password expiration.
- `Expiration Warning Delay`: The number of days before the password expiration when the user must be warned to change his or her password.
- `No. of failures allowed`: The number of login failures allowed before the user account is locked.

From the list displayed on the “Password Policies” page, it is possible to:

- duplicate an existing password policy by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The password policy creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new password policy.
- delete an existing password policy by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

8.4. Themes

Access Manager offers the possibility to set a custom theme by organization. Multiple themes can be defined by organizations, however only a single one can be active.

The active theme is defined in the `Theme` field of the organization selected from the “Organizations” page accessible from the “Configuration” menu.

A theme is defined by the following attributes on the `Logos`, the `Colors` and the `Tag Colors` tabs:

- `Name`: Name of the theme.
- `Page Title`: String to display as page title.
- `Page Header Logo`: Image to be displayed in the page header. It should be encoded using either JPEG or PNG. The image file should not exceed a size of 200 kilobytes. The optimal size is 80 × 50 pixels.
- `Login Page Logo`: Image to be displayed in the login header. It should be encoded using either JPEG or PNG. The image file should not exceed a size of 200 kilobytes. The optimal size is 106 × 70 pixels.
- `Background Image`: Image to be displayed on the page background. It should be encoded using either JPEG or PNG. The image file should not exceed a size of 1 megabyte.
- `Primary Color`: Main color of the application like the header color.

- `Default Color`: Neutral color for graphic elements.
- `Success Color`: Indicate a successful or safe action.

- `Info Color`: Informative or action color.
- `Warning Color`: Warning or test action color.
- `Danger Color`: Error, danger or perilous action color.
- `Widget Text Color`: Text color for graphic elements.
- `Text Color`: Color of text.
- `Link Color`: Hypertext link color.
- `Pager Color`: Color used for pager elements.
- `Background Color`: Page background color.
- `Key Color`: Tag key color.
- `Value Color`: Reference color of the tag value. A set of eleven colors is defined to identify eleven values. If needed, lighter and darker shades of these reference colors will be applied to the values of the additional tags.

The “menu” icon on the bottom-left provides several actions for helping theme creation:

- `Try It`: Use the theme temporarily. To revert to the previous theme, just click on the drawbar eye icon on the header of the page.

  This action is only available during the modification of an existing theme.
- `Fill the form with built-in theme parameters`: This action can be used to fill the form with the parameters of the Access Manager default theme.
- `Export as XML`: This action can be used to download the parameters of the theme as an XML format file.
- `Import from XML`: This action can be used to upload from an XML format file the parameters to be used during the creation of a theme or the modification of an existing one.

From the list displayed on the “Themes” page, it is possible to:

- duplicate an existing theme by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The theme creation window is then displayed and the form is pre-filled with the theme parameters for the current session. The required field(s) must be specified for the new theme.
- delete an existing theme by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

Chapter 9. X509 Certificate Authorities

A Certificate Authority (or “CA”) is defined by a key pair (a private key and a public key). The CA private key signs the public keys of the user accounts in the domain. These signed public keys are also called “certificates” and are used by the user to authenticate to WALLIX Access Manager. The certificates are verified against the CA public key by the WALLIX Access Manager during connections.

X509 certificate authentication is supported by WALLIX Access Manager to allow LDAP domain users to authenticate with certificates.

> ***Note:***
>
> The X509 CA configured in WALLIX Access Manager cannot be used to trust SSL/TLS communications with WALLIX Bastion.

9.1. Configuration of the X509 Certificate Authority

X509 Certificate Authorities can be added from the “Certificate Authorities” page accessible from the “Configuration” menu.

An X509 Certificate Authority is defined by the following attributes:

- `Organization`: The organization with which to associate the CA.
- `Name`: The name of the CA. It is a string with a length between 1 and 128 characters.
- `Description`: An optional string to provide a description of the CA.
- `Certificate`: The file containing the CA certificate used for the organization in order to verify the signature of the client certificate. The file must be in PEM format (.pem, .crt or .cer, for example). Expired certificates are not accepted. The file size must not exceed 64 kilobytes.
- `Change Certificate`: Toggle button to provide a new file containing the CA certificate. The new CA certificate must be loaded in the dedicated field `Certificate` which will be displayed when this button is activated. This field is only displayed during the edition of a Certificate Authority.
- `Certificate Revocation Verification`: Drop-down list to enable or disable the verification of the certificates using a CRL file.
- `CRL File`: The file in PEM format containing the Certificate Revocation List (CRL) signed by the Certificate Authority that issued the listed certificates. During the authentication, the CRL will be used to verify that a certificate is valid and trustworthy. The size of the file must not exceed 2 megabytes. This field is only displayed when `CRL File` is selected in the `Certificate Revocation Verification` drop-down list.

> ***Note:***
>
> Only one file can be configured per Certificate Authority.

Once a CRL file is loaded, data is displayed to the administrator indicating the issuing Certificate Authority in `CRL Issuer` and its expiration date in `CRL Next Update`.

From the `Certificate Revocation Verification` drop-down, it is possible to disable the use of the CRL file for the certificate verification by selecting `None` or to re-enable the verification by selecting `CLR File`.

- `Change CRL File`: Toggle button to provide a new file containing the CRL. The new CRL must be loaded in the dedicated field `CRL File` which will be displayed when this button is activated. This toggle button is only displayed during the edition of a Certificate Authority.

From the list displayed on the “Certificate Authorities” page, it is possible to:

- duplicate an existing CA by clicking on the `Duplicate` icon at the beginning of the concerned row or by right-clicking on the row to display a contextual menu with the `Duplicate` option. The CA creation window is then displayed and the form is pre-filled with the parameters of the chosen CA.
- delete an existing CA by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

Warning:

It is not recommended to delete a CA configured to be used in a domain or in an LDAP server. Deleting a CA will also delete the CA configuration on the domain and the LDAP server.

Chapter 10. Authentication domains

A domain is a way to define an authentication scheme for a subset of the users of an organization. Access Manager supports four kinds of domains:

- **local**: users are defined in Access Manager itself,
- **LDAP**: users are defined in an LDAP or Active Directory server,
- **SAML**: users are defined in an SAML identity provider (IdP),
- **BASTION**: users are defined in a bastion.

When connecting to Access Manager, the domain is provided in the URL as a parameter.

Example 10.1. Example of URL

`https://mycompany.tld/wabam/myorg?domain=mydomain`: The URL refers to the `mydomain` domain from the `myorg` organization.

It is possible to choose a default domain for an organization by editing the `Default Domain` field of the organization selected on the “Organizations” page accessible from the “Configuration” menu.

10.1. Local domains

A local domain is created for each organization. It is used to define users directly in Access Manager.

Local domains can be edited from the “Domains” page accessible from the “Configuration” menu. From the list displayed on this page, it is necessary to click on the desired local domain to display the modification window.

A local domain cannot be deleted from the organization in Access Manager.

A local domain is defined by the following attributes:

- `Name`: The name of the local domain in the system. This is a string of length between 1 and 64 characters. The name of this domain can be changed by editing the `Local Domain Name` field of the organization selected on the “Organizations” page accessible from the “Configuration” menu.
- `Default Profile`: The default profile set if there is no matching with an Access Manager profile in the directory. Access Manager searches for the user's groups and associates this user with the profiles which have the same names as his or her groups. On Active Directory, groups are searched recursively.
- `Associated Authenticators`: This expandable area allows the local domain to be associated with the available authenticators when configuring a single-factor or a multi-factor authentication. These authenticators are the LDAP, RADIUS and BASTION servers configured for the organization in Access Manager. For further information, refer to Section 10.2.2, “Configuration of the LDAP server”, Chapter 11, *RADIUS authentication* and Chapter 13, *Bastions*.

  The field `Login type` indicates the format of the login used for the authentication.

  The field `Factor` defines the order in which the authenticators are queried during the authentication. Each authenticator used for the authentication must return a positive response in the order which has been defined. The authentication succeeds when all the authenticators are validated. If an authenticator fails, then the authentication fails.

The field `Priority` defines the order in which the authenticators with the same factor are used for High-availability (HA). If the first server does not return a response, then the next one is queried until a response is returned. If no server responds, the authentication fails.

The field `Factor Used for Account Mapping` defines the authentication factor which will be used during an account mapping authentication in a multi-factor authentication.

> ***Note:***
>
> When authenticating on a local domain, the user can associate the login and the domain name in the `Login` field with the following syntax: “`local\admin`” or “`admin@local`”.

10.2. LDAP domains

> ***Warning:***
>
> IPv6 is not supported for LDAP authentications.

10.2.1. Configuration of the LDAP domain

An LDAP domain supports a set of LDAP servers. Servers can be defined for an organization in order to retrieve user definitions from an external directory. Microsoft Active Directory is considered as an LDAP server; therefore it is possible to let Windows domain users access Access Manager.

LDAP domains can be added from the “Domains” page accessible from the “Configuration” menu, by selecting LDAP from the contextual menu of the Add button. For further information, refer to Section 10.2.2, “Configuration of the LDAP server”.

An LDAP domain is defined by the following attributes:

- `Organization`: The organization to which the domain belongs.
- `Name`: The name of the LDAP domain in the system. This is a string of length between 1 and 64 characters.

  If this authentication mode is used in Access Manager together with an authentication through an LDAP domain in WALLIX Bastion, then domain names defined in both products must match.
- `Schema Type`: The type of schema of the LDAP domain, either Active Directory, NIS or X500. Default schema attributes can be overwritten by clicking on the `Pencil` icon.
- `Allow X509 Cert. Authentication`: Toggle button to tell Access Manager to allow X509 certificate authentication for the LDAP user on the login screen when connecting to the LDAP domain. This button is only available when `Active Directory` is selected as the `Schema Type`. For further information, refer to Section 10.2.4, “X509 authentication”.
- `Certificate Authorities`: Drop-down list to select one or more CAs. This list is only displayed when `Allow X509 Cert. Authentication` is enabled.

  During the user connection to the organization, the Web browser displays a window to select the appropriate client certificate if multiple client certificates are defined.
- `Default Profile`: The default profile set if there is no matching with an Access Manager profile in the directory. Access Manager searches for the user's groups and associates this user with the profiles which have the same names as his or her groups. On Active Directory, groups are searched recursively.

- `Default Language`: The default language to set if no language is found in the directory.
- `Associated Authenticators`: This expandable area allows the LDAP domain to be associated with the available authenticators when configuring a single-factor or a multi-factor authentication. These authenticators are the LDAP, RADIUS and BASTION servers configured for the organization in Access Manager. For further information, refer to Section 10.2.2, “Configuration of the LDAP server”, Chapter 11, *RADIUS authentication* and Chapter 13, *Bastions*.

  The field `Login type` indicates the format of the login used for the authentication.

  The field `Factor` defines the order in which the authenticators are queried during the authentication. Each authenticator used for the authentication must return a positive response in the order which has been defined. The authentication succeeds when all the authenticators are validated. If an authenticator fails, then the authentication fails.

  The field `Priority` defines the order in which the authenticators with the same factor are used for High-availability (HA). If the first server does not return a response, then the next one is queried until a response is returned. If no server responds, the authentication fails.

  The field `Factor Used for Account Mapping` defines the authentication factor which will be used during an account mapping authentication in a multi-factor authentication.
- `Associated Identifiers`: This expandable area allows the local domain to be associated with the available identifiers when configuring a multi-factor authentication.

  The field `Login type` indicates the format of the login used for the authentication.

  The field `Priority` defines the order in which the identifiers are queried for High-availability (HA). For load-balancing, the same priority can be set to several identifiers. In that case, for each identification, the order in which the servers are queried is random. If the first server does not return a response, then the next one is queried until a response is received. If no server responds, the identification and thus the user connection fail.

From the list displayed on the “Domains” page, it is possible to:

- duplicate an existing LDAP domain by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The domain creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new domain.
- delete an existing LDAP domain by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

> ***Note:***
>
> When authenticating on an LDAP domain, the user can associate the login and the domain name in the `Login` field with the following syntax: “`local\admin`” or “`admin@local`”.

10.2.2. Configuration of the LDAP server

LDAP servers can be added from the “LDAP Servers” page accessible from the “Configuration” menu.

An LDAP server is defined by the following `Connection` attributes which are displayed in the related tab:

- Name: The name of the server in the system. This is a string of length between 1 and 64 characters.
- Host: The hostname or the IP address of the LDAP server.
- Port: The TCP port of the LDAP server; 389 by default for No Encryption or StartTLS and 636 for SSL.
- Encryption Method: There are three different methods: No Encryption, SSL, StartTLS.
- Authentication Method: There are two different methods: No Authentication for anonymous binding and Simple Authentication. For the latter, two other attributes are required to define the binding identity: Bind DN (string of length between 1 and 228 characters) and Bind Password (string of length between 1 and 228 characters).
- Base DN: Used to restrict the queries to a sub-tree of the directory.
- Connection Timeout (s): Number of seconds to wait for an answer from the LDAP server.
- Allow LDAP user to change password: Toggle button to tell Access Manager to allow the password change for the LDAP user on the login screen when required by the LDAP server (this requires the bind user to be granted the reset password permission and the LDAP server to be reachable via an SSL connection on port 636).
- Verify LDAP Server Certificate: Toggle button to tell Access Manager to verify that the LDAP server certificate is valid and issued by the Certificate Authority loaded on the Certificate Authorities page (for further information, refer to Section 9.1, “Configuration of the X509 Certificate Authority”). This button is only available when SSL or StartTLS is selected as Encryption Method.
- Certificate Authority: Drop-down list to select the Certificate Authority which will verify the LDAP server certificate. This list is only displayed when Verify LDAP Server Certificate is enabled.
- Login Type: The format of the login used for the authentication. The three login types are the following: simple login, domain or email address.

> ***Note:***
>
> When authenticating with an email address, the Email Attribute field (accessible in the “LDAP Domain” page after clicking on the Pencil icon) must be specified with the email address which will be used to authenticate to the LDAP server.

- Domain Name: The domain the server belongs to.

  If this authentication mode is used in Access Manager together with an authentication through an LDAP domain in WALLIX Bastion, then domain names defined in both products must match.

The Test Connection button allows to test the connection to the LDAP server.

Once the LDAP server added and configured, it is necessary to go to the “Domains” page in order to associate the LDAP server with the available authenticators and identifiers. These are the other LDAP servers and RADIUS servers configured for the organization in Access Manager. For further information, refer to Section 10.2.1, “Configuration of the LDAP domain”.

From the list displayed on the “LDAP Servers” page, it is possible to:

- duplicate an existing LDAP server by clicking on the Duplicate icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the Duplicate option. The LDAP server creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new LDAP server.

- delete an existing LDAP server by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

10.2.3. Query customization

Two LDAP queries are used to retrieve the user definition. These queries are executed every time a user is logging on. The first query is used to get the user attributes and the second one is used to get the user groups. The object class used to retrieve the user from the directory is provided by the `Object Class` field.

Active Directory	NIS	X500
user	posixAccount	inetOrgPerson

Table 10.1. Default values of the Object-Class attribute

The user attributes which can be retrieved from the directory are listed in Table 10.2, “Default user attributes per schema type”.

Attribute	Active Directory	NIS	X500
Login	sAMAccountName	uid	uid
Display Name	displayName	cn	cn
Email	mail	mail	mail
Language	preferredLanguage	preferredLanguage	preferredLanguage

Table 10.2. Default user attributes per schema type

The second query retrieves the user groups. Its custom part describes how to check for user membership. A specific syntax is available to define by which attribute a user is identified in a group. The attribute name should be enclosed between `${` and `}`. The table lists the `Group Filter` value per schema type.

Schema Type	Group Filter
Active Directory	&(objectClass=group)(member:1.2.840.113556.1.4.1941:=${dn})
NIS	&(objectClass=posixGroup)(memberUid=${uid})
X500	&(objectClass=groupOfNames)(member=${dn})

Table 10.3. Group filters

10.2.4. X509 authentication

Important:

X509 authentication is not possible on the administration interface of an appliance. Consequently, it is not possible to perform X509 authentication on an appliance configured with a single network interface.

X509 authentication is not compatible with RAWTCPIP sessions.

LDAP usernames containing the special characters `" + < > #` are not supported by Access Manager.

X509 authentication can be provided to the LDAP domain user (when the `Schema Type` of the LDAP domain is `Active Directory`) together with the login/password authentication on the login screen of Access Manager when the following configuration is implemented:

- first, the following settings must be performed in the file `wabam.properties` available in the configuration directory which is, by default, `/var/wab/etc/wabam`.
  - set the parameter *`web.check.client.certificate`* to *`true`* then
  - in the parameter *`web.client.certificate.subhostname`*, specify the value of the second element of the fully qualified domain name (FQDN) of the host.

    In the following example: `hello.X509.nono.net`,

    - “*`X509`*” corresponds to this second element and must then be specified as the parameter value.
    - the element that precedes the subhostname, “*`hello`*”, must correspond to the organization name used in Access Manager.
- next, restart the service Access Manager.
- if necessary, set also the following parameters for the needed organization to manage certificate revocation in the `Web` expandable section from the “Application” tab on the “Application Settings” page, accessible from the “Settings” menu:
  - *`web.cert.enable.crldp`*: enable CRLDP revocation check,
  - *`web.cert.ocsp.responder.url`*: specify the URL to the OCSP responder.
- in the “Certificate Authorities” page, add one or more CA certificates and the CRL file, if needed, in PEM format, for the appropriate organization. For further information on the configuration of CA certificates, refer to Section 9.1, “Configuration of the X509 Certificate Authority”.
- lastly, on the LDAP domain window accessible from the “Domains” page of the “Configuration” menu, allow X509 certificate authentication for the users on the LDAP domain via the `Allow X509 Cert. Authentication` toggle button, then by selecting one or more CAs in the `Certificate Authorities` drop-down list.

During the user connection:

- the Web browser displays a window to choose the appropriate client certificate when multiple client certificates are defined.
- data of the client certificate is verified against data of the Active Directory to retrieve the user data (language, profiles, etc.).

10.3. SAML domains

> ***Warning:***
>
> IPv6 is not supported for SAML authentications.

Security Assertion Markup Language (**SAML**) is an XML-based data format for exchanging authentication and authorization data between two parties, in particular, between an identity provider and a service provider.

Authentication to Access Manager can be delegated to Identity Providers through SAML 2.0 standard protocol. Access Manager acts as a Service Provider (SP) and supports HTTP redirect and HTTP POST bindings.

Delegating authentication to a SAML Identity Provider (IdP) requires:

- a SAML domain with attribute mapping
- a SAML Identity Provider linked to the SAML domain.

A SAML domain supports a set of SAML Identity Providers. Within a domain, each server is considered equivalent to the others. Thus Access Manager uses indifferently any server in the domain to provide high-availability capabilities.

Access Manager supports both IdP-initiated and SP-initiated connection modes.

10.3.1. Configuration of the SAML domain

SAML domains can be added from the “Domains” page accessible from the “Configuration” menu, by selecting `SAML` from the contextual menu of the `Add` button. They can also be added on the `Domain` tab from the “SAML Identity Providers” page accessible from the “Configuration” menu. For further information, refer to Section 10.3.2, “Configuration of the SAML identity provider (IdP)”.

A SAML domain is defined by the following attributes:

- `Name`: Name of the SAML domain in the system. This is a string with a length between 1 and 64 characters.

> ***Important:***
>
> To use the SAML authentication with WALLIX Bastion, this domain name must be the same as the one entered in the `Server domain name` field of the related `Authentication domain` in the Bastion configuration.

- `Attributes`: Mapped attributes of the SAML response sent by the identity provider. They can be edited by clicking on the `Pencil` icon. A mapping can be set for the following user attributes:
  - `Login`: Login of the user
  - `Display Name Attribute`: Name that will be displayed in the top banner of Access Manager. If empty, the name displayed will be `login@domain`.
  - `Email Attribute`: Email of the user
  - `Language Attribute`: 2-letter country code (e.g.: “en”, “fr”)
  - `Profile Attribute`: Profile of the user
- `Default Profile`: Default profile if no matching Access Manager profile can be retrieved from the SAML response sent by the identity provider. Access Manager matches profiles by searching the organization's profile names. Access Manager associates a profile with the user when the Access Manager profile name matches the value in the `Profile Attribute` field.
- `Default Language`: Default language if no supported language is found in the SAML response sent by the identity provider.

From the list displayed on the “Domains” page, it is possible to:

- duplicate an existing SAML domain by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The domain creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new domain.
- delete an existing SAML domain by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

10.3.2. Configuration of the SAML identity provider (IdP)

SAML IdPs can be added from the “SAML Identity Providers” page accessible from the “Configuration” menu.

The identity provider of Access Manager is identified by the following attribute:

- `Name`: Name of the IdP in the system. This is a string with a length between 1 and 128 characters.

The `Service Provider` (i.e. Access Manager) is defined by the following attributes which are displayed in the related tab:

- `WALLIX-AM Entity Id`: Name used to refer to Access Manager in the exchanges with the identity provider. It corresponds to the `entityId` field in the service provider metadata file (`sp-metadata.xml`).
- `Sign Messages`: Toggle button to tell Access Manager to sign the requests sent to the identity provider.
- `Signing Key & Certificate`: Signing key-certificate configuration status and generation button.

  The `Pencil` icon opens a panel to edit the following attributes:

  - `Signing Key`: Private key used to sign the authentication request sent to the IdP. It can be set either by using the dedicated field in the user interface or by clicking on the `Generate` button. The generated private key cannot be displayed by the user interface. If a specific private key is to be used instead of a generated key, then it is possible to paste it here. It must be in PEM format, without the headers and footers.
  - `Signature Validation Certificate`: Certificate used to validate the signature of the data sent to the IdP. It can be set either by using the dedicated field in the user interface or by clicking on the `Generate` button. It corresponds to the certificate in the `<KeyDescriptor>` section with the `use="signing"` attribute in the service provider metadata file (`sp-metadata.xml`). It must be in PEM format, without the headers and footers.
- `Encrypt Messages`: Toggle button to tell Access Manager to check for encrypted data. If the IdP did not use encryption, the authentication process fails.

> ***Important:***
>
> When configuring SAML to authenticate to WALLIX Bastion via WALLIX Access Manager, it is required to disabled the encryption of messages.

- `Encryption Key & Certificate`: Encryption key-certificate configuration status and generation button.

  The `Pencil` icon opens a panel to edit the following attributes:

  - `Decryption Key`: Private key used to decrypt the IdP answer. It can be set either by using the dedicated field in the user interface or by clicking on the `Generate` button. The generated private key cannot be displayed by the user interface. It must be in PEM format, without the headers and footers.
  - `Encryption Certificate`: Certificate sent to the IdP to encrypt the answer. It can be set either by using the dedicated field in the user interface or by clicking on the `Generate` button. It corresponds to the certificate in the `<KeyDescriptor>` section with the `use="encryption"` attribute in the service provider metadata file (`sp-metadata.xml`). It must be in PEM format, without the headers and footers.

- `Signed Response`: Toggle button to tell Access Manager to require signed responses from the IdP.
- `Signed Assertion`: Toggle button to tell Access Manager to require signed assertions from the IdP.
- `Force Authent.`: Toggle button to tell Access Manager to force the user to re-authenticate to the IdP even if an SSO session is active for this user.
- `Authent. Expir. Delay`: Validity delay before the expiration of the authentication (in minutes).

> ***Warning:***
>
> By disabling the attributes `Signed Response` and `Signed Assertion`, any user will be able to connect to Access Manager as an administrator.

Once the SAML identity provider configuration is saved, the service provider metadata file can be downloaded by clicking on the `Download` button below the `Metadata File` field. This file is supported by some Identity Providers such as Microsoft ADFS and Shibboleth to define Access Manager as a trusted party. This button is only displayed when editing a SAML identity provider.

The `Identity Provider` is defined by the following attributes which are displayed in the related tab:

An IdP metadata file can be imported to fill in the form by clicking on the “Import” icon on the upper right corner of the tab.

- `Identity Provider Entity Identifier`: Identifier of the IdP during the SAML process. It corresponds to the `entityId` attribute of the `EntityDescriptor` element in the IdP metadata file (`idp-metadata.xml`).
- `SSO Binding Type`: List to select the authentication method.
- `Redirect Binding Uri`: Uri to which Access Manager redirects the user for authentication. It corresponds to the `Location` attribute of the `SingleSignOnService` element for the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect` binding. This field is displayed when `Redirect` has been selected in the list of the `SSO Binding Type` field.
- `Redirect Logout Uri`: Uri to which Access Manager sends logout requests to the IdP. This field is displayed when `Redirect` has been selected in the list of the `SSO Binding Type` field.
- `POST Binding Uri`: Uri to which Access Manager redirects the user when using the POST method. This field is displayed when `POST` has been selected in the list of the `SSO Binding Type` field.
- `POST Logout Uri`: Uri to which Access Manager sends logout requests to the IdP when using the POST method. This field is displayed when `POST` has been selected in the list of the `SSO Binding Type` field.
- `Identity Provider Validation Certificate`: Certificate used to validate the signed data received from the IdP. It corresponds to the certificate in the `KeyDescriptor` section with the `use="signing"` attribute in the `IDPSSODescriptor` element in the IdP metadata file (`idp-metadata.xml`). The `Pencil` icon opens a panel to paste the certificate. It must be in PEM format, without the headers and footers.

The related domain and its attributes are defined as follows in the `Domain` tab:

- `Domain Name`: Domain to which the service provider belongs. This is a string of length between 1 and 64 characters. If SAML domains have already been created for the organization, it is possible to select one of them by clicking on the `Pencil` icon.

> ***Important:***
>
> To use the SAML authentication with WALLIX Bastion, this domain name must be the same as the one entered in the `Server domain name` field of the related `Authentication domain` in the Bastion configuration.

- `Attributes`: Mapped attributes of the SAML response sent by the identity provider can be edited by clicking on the `Pencil` icon. A mapping can be set for the following user attributes:
  - `Login`: Login of the user
  - `Display Name Attribute`: Name that will be displayed in the top banner of Access Manager. If empty, the label displayed will be `login@domain`.
  - `Email Attribute`: Email of the user
  - `Language Attribute`: 2-letter country code (e.g.: “en”, “fr”)
  - `Profile Attribute`: Profile of the user
- `Default Profile`: Default profile if no matching Access Manager profile can be retrieved from the SAML response sent by the identity provider. Access Manager matches profiles by searching the organization's profile names. Access Manager associates a profile with the user when the Access Manager profile name matches the value in the `Profile Attribute` field.
- `Default Language`: Default language if no supported language is found in the SAML response sent by the identity provider.

> ***Important:***
>
> When configuring SAML to authenticate to WALLIX Bastion via WALLIX Access Manager, make sure to disable the `Strip Domain` parameter in the Bastion of the organization, in order to keep the domain part in the user login (i.e. `@domain`). Thus WALLIX Bastion users declared in external authentication mode can be mapped with external Access Manager users in order to retrieve their corresponding authorizations.

From the list displayed on the “SAML Identity Providers” page, it is possible to:

- duplicate an existing SAML IdP by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The SAML IdP creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new SAML IdP.
- delete an existing SAML IdP by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

10.4. Bastion domains

10.4.1. Configuration of the bastion domain

A bastion domain allows you to configure a bastion as an authenticator and identifier in order to allow the local users from this bastion to access Access Manager.

Bastion domains can be added from the “Domains” page accessible from the “Configuration” menu, by selecting `BASTION` from the contextual menu of the `Add` button. For further information, refer to Section 10.4.2, “Configuration of the bastion”.

A bastion domain is defined by the following attributes:

- `Name`: The name of the bastion domain in the system. This is a string of length between 1 and 64 characters.
- `Profile Attribute`: The mapped attributes between Access Manager and the bastion. The administrator must ensure that the profile names defined in Access Manager and the profile and group names defined in the bastion are the same. A mapping can be defined for the following user attributes:
  - `Profile`: mapping on the user profile defined in the bastion.
  - `Group`: mapping on the user groups defined in the bastion.
- `Default Profile`: The default profile set if there is no matching between an Access Manager profile and a bastion profile or bastion groups.
- `Default Language`: The default language to set if no language is retrieved from the bastion.
- `Associated Authenticators`: This expandable area allows the bastion domain to be associated with the available authenticators when configuring a single-factor or a multi-factor authentication. These authenticators are the LDAP, RADIUS and BASTION servers configured for the organization in Access Manager. For further information, refer to Section 10.2.2, “Configuration of the LDAP server”, Chapter 11, *RADIUS authentication* and Chapter 13, *Bastions*.

  The field `Login type` indicates the format of the login used for the authentication. Only the “Simple login” type is allowed for a bastion domain.

  The field `Factor` defines the order in which the authenticators are queried during the authentication. Each authenticator used for the authentication must return a positive response in the order which has been defined. The authentication succeeds when all the authenticators are validated. If an authenticator fails, then the authentication fails.

  The field `Priority` defines the order in which the authenticators with the same factor are used for High-availability (HA). If the first server does not return a response, then the next one is queried until a response is returned. If no server responds, the authentication fails.

  The field `Factor Used for Account Mapping` defines the authentication factor which will be used during an account mapping authentication in a multi-factor authentication.
- `Associated Identifiers`: This expandable area allows the bastion domain to be associated with the available identifiers when configuring a multi-factor authentication.

  The field `Login type` indicates the format of the login used for the authentication. Only the “Simple login” type is allowed for a bastion domain.

  The field `Priority` defines the order in which the identifiers are queried for High-availability (HA). For load-balancing, the same priority can be set to several identifiers. In that case, for each identification, the order in which the servers are queried is random. If the first server does not return a response, then the next one is queried until a response is received. If no server responds, the identification and thus the user connection fail.

From the list displayed on the “Domains” page, it is possible to:

- duplicate an existing bastion domain by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The domain creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new domain.
- delete an existing bastion domain by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

> ***Note:***
>
> When authenticating on a bastion domain, the user can associate the login and the domain name in the `Login` field with the following syntax: “`local\admin`” or “`admin@local`”.

10.4.2. Configuration of the bastion

The bastion which will be used as an authenticator and identifier can be added from the “Bastions” page accessible from the “Configuration” menu. For further information on the configuration of bastions, refer to Chapter 13, *Bastions*.

The attributes to be defined to declare a bastion as an authenticator and identifier are the following:

- `Use as an authenticator/identifier`: Toggle button to tell Access Manager to use the bastion as an authenticator and identifier.
- `Name`: List to select the name of the bastion domain created on the “Domain” page. This field is displayed when the attribute `Use as an authenticator/identifier` is enabled. For further information, refer to Section 10.4.1, “Configuration of the bastion domain”.
- `Login type`: List to select the login type used for the authentication on the bastion domain. Only the “Simple login” type is allowed for a bastion domain. This field is displayed when the attribute `Use as an authenticator/identifier` is enabled.

Chapter 11. RADIUS authentication

> **Warning:**
>
> IPv6 is not supported for RADIUS authentications.

RADIUS servers can be defined for an organization in Access Manager to provide users with RADIUS authentication. This authentication is based on PAP or CHAP protocols.

For RADIUS authentications, Access Manager supports the challenge-response mechanism.

RADIUS authentication servers can be added from the “RADIUS Servers” page accessible from the “Configuration” menu.

A RADIUS authentication server is defined by the following attributes:

- `Name`: The name of the server in the system. This is a string of length between 1 and 128 characters.
- `Host`: The hostname or the IP address of the RADIUS server.
- `Protocol`: There are three different values for authentication protocols: `AUTO`, `PAP` and `CHAP`. When `AUTO` is selected, the server tries first CHAP protocol and then switch to PAP protocol if the first one fails. `AUTO` is selected by default.
- `Authentication Port`: The port of the RADIUS server for authentication; 1812 by default.
- `Connection Timeout (s)`: Number of seconds to wait for an answer from the RADIUS server.
- `Login type`: The format of the login used for the authentication. The three login types are the following: simple login, domain or email address.
- `Change Shared Secret`: Toggle button to change the secret used to cypher transactions between the RADIUS client and the RADIUS server. Enter the new secret in the dedicated field which will be displayed when switching on this button. This field is only displayed during the modification of a RADIUS server.
- `Shared Secret`: The secret to cypher transactions between the RADIUS client and the RADIUS server. This field is only displayed during the creation of a RADIUS server.
- `NAS Identifier`: The Network Access Server (NAS) identifier to identify the RADIUS authentication requests on the RADIUS server.

The `Test Connection` button allows to test the connection to the RADIUS authentication server.

When editing the RADIUS authentication server, the expandable area `Domains using this server as authenticator` is displayed at the bottom of the page. This area lists the names of the local or LDAP domains configured in Access Manager using this server in their authentication process. For further information, refer to Chapter 10, *Authentication domains*.

From the list displayed on the “RADIUS Authentication Servers” page, it is possible to:

- duplicate an existing RADIUS authentication server by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The RADIUS authentication server creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new RADIUS server.

- delete an existing RADIUS authentication server by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

Chapter 12. Users

Users can be defined either locally in Access Manager or in an external directory. Users should also be known by the same login by the bastions holding their authorizations.

12.1. Profiles

A user can have one or several profiles. A profile is a set of rights. Rights control the ability for a user to perform actions such as the user creation for example, with the right `Create User`. In order to be able to open a session on a target, the user profile must be associated with the `Target Access` right.

Profiles can be added from the “Profiles” page which can be accessed from the “Configuration” menu.

A profile is defined by the following attributes:

- `Name`: Name of the profile.
- `Rights`: List to select the right(s) for the profile.

The profile `Global Administrator` is linked by default to the global organization. This profile provides all the permissions.

The `Administrator`, `Approver`, `Auditor` and `User`profiles are linked by default to a non-global organization (such as the **`default`** organization). They provide specific rights.

From the list displayed on the “Profiles” page, it is possible to:

- duplicate an existing profile by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The profile creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new profile.
- delete an existing profile by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

12.2. Local users

A local user is a user defined directly in Access Manager.

Local users can be added from the “Users” page which can be accessed from the “Configuration” menu.

The user identity is defined in the `Identity` tab by the following attributes:

- `Organization`: The organization the user belongs to. Only users in the global organization can create users outside their own organizations.
- `Login`: The value that the user provides to identify himself or herself. This is a string of length between 1 and 128 characters. It should not contain either the `@` or the `\` characters, which are reserved as domain separators. This login should match the WALLIX Bastion user login in order to properly retrieve user's authorizations.
- `Name`: The value displayed to the screen. This is a string of length between 1 and 128 characters.

- `Email`: The email address of the user. This address must respect the format `myuser@mydomain.ltd`.
- `Language`: The language in which the interface and the messages are displayed to the user.
- `Approval Time Zone`: The time zone selected by the user in his/her profile. It enables the optimal synchronization of the steps of the approval workflow when WALLIX Access Manager and WALLIX Bastion are running in different time zones. If this parameter is not defined, then the default time zone set in the file `wabam.properties` is used during approval workflows.

  This default time zone can be changed by editing the parameter *`approval.time.zone`* in the file `wabam.properties` which is available in the configuration directory: `/var/wab/etc/wabam`.

  > ***Warning:***
  >
  > The parameter *`approval.time.zone`* must be configured with the time zone of the server in order to ensure proper synchronization of the approvals. If the parameter *`approval.time.zone`* does not exist in the file `wabam.properties` or if no default time zone is entered for this parameter, then WALLIX Access Manager uses the time zone of the server on which it is running.
  >
  > The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

- `Change Password`: A toggle button to change the password used to authenticate the user. Enter and confirm the new password in the dedicated fields. It must comply with the password policy requirements defined for the organization. For further information, refer to Section 8.3, “Password policies”.
- `Force Password Change`: A toggle button to force the password change. At next logon, a warning message will be displayed to the user and he or she will be forced to change his or her password.
- `Unlock User`: A button to release the lock of the user account as the number of login failures allowed has been exceeded. This number is set in the password policy for the organization. For further information, refer to Section 8.3, “Password policies”.
- `Description`: Optional character string (up to 1024 characters) for providing a user description.

The user rights are defined in the `Rights` tab by the following attributes:

- `Profiles`: A list of profiles defining the user rights. For further information, refer to Section 12.1, “Profiles”.
- `Restricted Source IPs`: A list of IP addresses or subnets using the CIDR notation (<network address>/<number of mask bits>), from which the user or the administrator from the global organization is authorized to connect. An empty list means that the user or the administrator from the global organization can connect from any host.

  > ***Important:***
  >
  > Access Manager supports IPv4 and IPv6 address formats.

From the list displayed on the “Users” page, it is possible to:

- duplicate an existing user by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The user creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new user.

- delete an existing user by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

12.3. Non-local users

A non-local user is defined in Access Manager from an SAML identity provider (IdP) or from an LDAP or Active Directory server.

From the list displayed on the “Users” page, which can be accessed from the “Configuration” menu, it is possible to:

- identify non-local users: a dedicated icon is displayed in the `Login` field for users defined from an SAML identity provider or from an LDAP or Active Directory server.
- delete an existing non-local user by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

Chapter 13. Bastions

> ***Important:***
>
> The IP addresses which can be set on Access Manager support both IPv4 and IPv6 formats.

Bastions represent the WALLIX Bastion appliances deployed by the organization.

Bastions can be added on the “Bastions” page, which can be accessed from the “Configuration” menu.

A bastion is defined by the following attributes:

- `Name`: Name of the bastion in Access Manager. This is a string of length between 1 and 128 characters.
- `Host`: Hostname or IP address of the bastion. It must be the IP address used for the user service of WALLIX Bastion. In the case of a multi-interface deployment, WALLIX Bastion can have different interfaces and IP addresses for the user and the administration services. This is a string of length between 1 and 228 characters.
- `API Key`: A WALLIX Bastion REST API key generated from the Web interface of WALLIX Bastion (from the “Configuration” menu). This field is only displayed during the creation of a bastion.
- `Change API Key`: Toggle button to provide a new API key. Enter the data in the `API Key` field which appears below.
- `Reset Bastion Certificate`: Toggle button to reset the bastion certificate. It will be replaced by the next connection to the bastion. This action is required when the certificate is updated on the bastion.
- `Reset SSH Fingerprint`: Toggle button to reset the bastion SSH fingerprint. It will be set by the next SSH session.
- `Reset RDP Fingerprint`: Toggle button to reset the bastion RDP fingerprint. It will be set by the next RDP session.
- `Cluster`: Add the bastion to a cluster. Clusters are used for load-balancing the sessions among multiple bastions using the same configuration. The administrator should ensure that the configuration of the authorizations with the same names must match within all the cluster's bastions. The load-balancing is performed by selecting the bastion hosting the lowest number of opened sessions within the Access Manager farm. For further information, refer to Chapter 20, *Scalability and High-availability*. When a bastion is part of a cluster, its authorizations are no longer listed under its name, but under the cluster name. Clusters are not compatible with the feature allowing the display of the target passwords. However it can be used with an external vault.

  A + button is provided to add a new cluster and a `Pencil` icon is provided to rename an existing cluster.
- `Strip Domain`: Toggle button to strip the domain part (i.e. `@domain`) from the user login for non-local Access Manager users to be authenticated on the bastion. Thus local WALLIX Bastion users declared in external authentication mode can be mapped with external Access Manager users to retrieve their corresponding authorizations.
- `Approval Time Zone`: List to select the time zone of the bastion. It enables the optimal synchronization of the steps of the approval workflow when WALLIX Access Manager and WALLIX Bastion are running in different time zones. If the version of the Bastion is 8.1 or higher, the time zone is automatically updated with the bastion's time zone when the connection is tested via

the `Test Connection` button or when saving this configuration. If the version of the Bastion is earlier than 8.1 and no default time zone is selected then the default time zone set in the file `wabam.properties` is used during approval workflows.

The default time zone can be changed by editing the parameter *`approval.time.zone`* in the file `wabam.properties` which is available in the configuration directory: `/var/wab/etc/wabam`.

> ***Warning:***
>
> The parameter *`approval.time.zone`* must be configured with the time zone of the server in order to ensure proper synchronization of the approvals. If the parameter *`approval.time.zone`* does not exist in the file `wabam.properties` or if no default time zone is entered for this parameter, then WALLIX Access Manager uses the time zone of the server on which it is running.
>
> The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

- `API Version`: Access Manager automatically detects the API version compatible with this bastion. This detection may be done when the connection is tested via the `Test Connection` button.
- `Allow Session Search`: Toggle button to enable session audit data retrieval on the “Session Audit” page accessible from the “Audit” menu. For further information, refer to Chapter 19, *Session audit data*.
- `Search Start Date`: This field is displayed when the session audit data retrieval is enabled via the `Allow Session Search` field. The start date from which the sessions can be retrieved must be entered. A calendar is available by clicking into the frame.
- `Login`: This field is displayed when the session audit data retrieval is enabled via the `Allow Session Search` field. The login of the bastion's user allowed to retrieve session audit data must be entered. This user is linked to the `Auditor` profile.
- `Use as an authenticator/identifier`: Toggle button to tell Access Manager to use the bastion as an authenticator and identifier. For further information, refer to Section 10.4, “Bastion domains ”.
- `Name`: List to select the name of the bastion domain created on the “Domain” page. This field is displayed when the attribute `Use as an authenticator/identifier` is enabled.
- `Login Type`: List to select the login type used for the authentication on the bastion domain. Only the “Simple login” type is allowed for a bastion domain. This field is displayed when the attribute `Use as an authenticator/identifier` is enabled.
- `Active Bastion`: Toggle button to activate or deactivate a bastion configured in Access Manager. A deactivated bastion is not deleted, it remains in the Access Manager database and is displayed on the interface. However, authorizations, current approvals, approval history, or session audit are not available for a deactivated bastion. Note that to disable a bastion used as an authenticator and identifier, it is necessary to first set the bastion as “Unused” in the `Factor` field, “Domains” page > `Associated Authenticators` area (for further information, refer to Section 10.4.1, “Configuration of the bastion domain”).

The `Test Connection` button allows to test the connection to the bastion for the current user or another user.

From the list displayed on the “Bastions” page, it is possible to:

- duplicate an existing bastion by clicking on the `Duplicate` icon at the beginning of the concerned row or right-clicking on the row to display a contextual menu with the `Duplicate` option. The bastion creation window is then displayed and the form is pre-filled with the parameters of the chosen one. The required field(s) must be specified for the new bastion.

- delete an existing bastion by right-clicking on the concerned row: a contextual menu is displayed and the `Delete` option must be selected. Access Manager displays a dialogue box requesting a confirmation before permanently deleting the row.

Chapter 14. User authorizations

The available authorizations are displayed on the “Authorizations” menu. These are the ones of the WALLIX Bastion user using the same login as the one of the Access Manager connected user.

User's authorizations are gathered from the bastions of the organization at each login.

Authorizations on sessions can be accessed from the “Sessions” page and are only available to users whose profile is associated with the `Target Access` right.

Authorizations on passwords can be accessed from the “Passwords” page and are only available to users whose profile is associated with the `Target Password Access` right.

14.1. Authorizations and folders

On the “Sessions” and “Passwords” pages, authorizations are placed by default into folders corresponding to their target group name.

> ***Note:***
>
> In case of synchronization failure of the bastion or incorrect configuration of Access Manager, the previously synchronized authorizations are not deleted to ensure minimum service.

On the `Explorer` tab:

- When a given folder is selected on the tree structure, the user can filter the corresponding authorizations displayed in the table by entering data in the upper area so as to restrict the display to the relevant rows. When searching for authorizations via tags, the user must use the following syntax: “`tag:key:value`”. Note that the syntax is case sensitive.
- The user can manage filing for his or her authorizations by using the dedicated icons to create, edit or delete folders into which authorizations can be filed. The folders displayed on the tree structure are private to a user. An empty folder is characterized by a transparent folder icon. Note that the same folder related to a given target group may contain authorizations for sessions but may be empty for password authorizations and vice versa.
- The user can move the authorizations from the table to any folder on the tree structure by performing a drag-and-drop operation with the cursor at the beginning of the concerned row. In order to restore the authorizations to their initial location, the user can click on the `Return Authorizations to Default Folder` icon.
- The `Synchronize` icon allows to refresh and retrieve up-to-date authorizations without modifying the customized folder layout.

On the `Search` tab:

- The user can retrieve the relevant authorizations regarding sessions or passwords by entering data in the dedicated area. When searching for authorizations via tags, the user must use the following syntax: “`tag:key:value`”. Note that the syntax is case sensitive. A simple direct click on the `Search` button without entering the search area retrieves all the existing authorizations.
- The user can manage filing for the retrieved authorizations. To do so, he or she must select the relevant rows and click on `Move to a folder`. On the window displayed, the user can then select on the tree structure the folder into which the authorizations can be filed. The icons on the window can be clicked to create, edit or delete folders. The folders displayed on the tree structure

are private to a user. An empty folder is characterized by a transparent folder icon. Note that the same folder related to a given target group may contain authorizations for sessions but may be empty for password authorizations and vice versa.

On the `Tag Explorer` tab:

- The user can filter the authorizations displayed in the table by entering data in the upper area so as to restrict the display to the relevant rows. When searching for authorizations via tags, the user must use the following syntax: “`tag:key:value`”. Note that the syntax is case sensitive.
- The user can sort in ascending or descending order the tags in the “Information” column of the table in order to display the relevant information more efficiently. To do so, he or she must click on the desired tag to define the sort order, symbolized by an arrow.
- The `Expand All` and `Collapse All` icons allow the user to expand or collapse all the folders of the tree structure.
- The `Synchronize` icon allows the user to refresh and retrieve up-to-date authorizations without modifying the customized folder layout.

14.2. User authorizations on sessions

> ***Important:***
>
> Access Manager supports IPv4 and IPv6 address formats.
>
> X509 authentication is not compatible with Universal Tunneling (RAWTCPIP) sessions.

Authorizations on sessions can be accessed from the “Sessions” page and are only available to users whose profile is associated with the `Target Access` right.

From the “Sessions” page, the user can connect to the target using the SSH, RDP or Universal Tunneling (previously called RAWTCPIP) client tools bundle in the application.

To do so:

1. Select the appropriate authorization folder from the tree structure on the `Explorer` or `Tag Explorer` tabs.
2. Click the icon at the beginning of the desired authorization row.

For Universal Tunneling sessions, the AM Universal Tunneling client which must be downloaded to the user's workstation connects to the Access Manager server using TLS and checks the validity of the server certificate to allow the connection to the target. To do this, some prerequisites are required:

- The Certificate Authority which issued the server certificate must be saved in the trust store of the workstation's operating system.
- The HTTPS certificate used by the Access Manager server must have at least one `Subject Alternative Name` field specified with the DNS used to connect to the Access Manager server.

Universal Tunneling allows simultaneous access to up to 50 interfaces in the same session.

> ***Note:***
>
> The user can open an RDP session or an application as an administrator if the `rdp.option.admin.enabled` parameter has been enabled in the `RDP` expandable section on the “Settings” page. In this case, he or she must click on the small orange icon appearing on the corner of the icon at the beginning of the authorization row.

> The user can copy-paste text and files between multiple RDP sessions. They can also drag and drop files between their workstation and the target. These actions are possible if the `rdp.shared.clipboard` parameter has been enabled in the `RDP` expandable section on the “Settings” page. When this parameter is enabled, the `Clipboard` menu is not displayed in the session. Please note that Mozilla Firefox does not allow text to be copied and pasted directly from the user's workstation to the RDP session.
>
> It is only possible to copy-paste and to drag-and-drop one set of files at a time via the clipboard.

If an approval workflow has been defined in WALLIX Bastion to be allowed to connect to the target, the user must send an approval request on the `Approval Request` window and notify approvers to be granted access. For further information, refer to Section 14.4, “Approval request management for the user”.

14.3. User authorizations on passwords

Authorizations on passwords can be accessed from the “Passwords” page and are only available to users whose profile is associated with the `Target Password Access` right.

From the “Passwords” page, the user can view the account's credentials (login, password and SSH key) on a dedicated window. To do so, he or she must select the appropriate authorization file from the tree structure on the `Explorer` or `Tag Explorer` tabs, then click on the padlock icon at the beginning of the desired authorization row.

On the `Password` window:

- The user can click on the red eye icon on the right of the `Password` field (if displayed) and choose a duration to display the password. The password becomes unreadable when the duration has elapsed.
- The user can copy the account credentials into the clipboard by clicking on the `Copy` icon in front of each field.
- If the lock has been enabled at the level of the checkout policy associated with this target account in WALLIX Bastion, the user must click on the `Check-in` button on the window to release the account before the end of checkout duration. Nonetheless, the account will be automatically checked-in at the end of the checkout duration. The checkout duration has been defined at the level of the checkout policy in WALLIX Bastion.
- The user can download the file containing the private key (if any defined) for SSH connection. A toggle button allows the selection of the OpenSSH or Putty format before clicking on the `Download` icon on the right of the `SSH Private Key` field.

If an approval workflow has been defined in WALLIX Bastion to be allowed to access the target's password, the user must send an approval request on the `Approval Request` window and notify approvers to be able to view the password. For further information, refer to Section 14.4, “Approval request management for the user”.

14.4. Approval request management for the user

If an approval workflow has been defined in WALLIX Bastion to be allowed to connect to the target or to access the target's credentials, the user logged on WALLIX Access Manager must send an approval request and notify approvers to be granted access.

Only users whose profile is associated with the rights `View Approval Request`, `Create Approval Request` and `Update Approval Request` can request approval from their authorizations and view the request status on the “Approval Requests” page accessible from the “Approval” menu.

14.4.1. Approval request on sessions

If an approval workflow has been defined in WALLIX Bastion to be allowed to connect to the target, the user must send an approval request and notify approvers to be granted access.

When connecting to an RDP, SSH or RAWTCPIP target from an authorization on the “Sessions” page, Access Manager displays the `Approval Request` window to send the request. This approval request is defined by the following attributes:

- `Start Date`: Start date and time from which the access is requested. By default, this is the current date and time. A calendar is available to modify the data by clicking into the frame.
- `Hours` | `Minutes`: Duration during which the access is requested. By default, this duration is set to 1 hour. However, the fields are available for update.
- `Ticket Reference`: Ticket reference to specify for the approval request. This field is displayed/hidden and, if displayed, required/optional according to the authorization definition in WALLIX Bastion.
- `Comment`: Comment to specify the reason for the approval request. This field is displayed/hidden and, if displayed, required/optional according to the authorization definition in WALLIX Bastion.

Once the approval request has been sent, Access Manager displays a confirmation message: the user can refresh the page and possibly send another request by clicking on `Re-open a session`.

The user can then view the status of the approval request on the “Approval Requests” page accessible from the “Approval” menu. For further information, refer to Section 14.4.3, “View of the approval request status”.

Once a request is approved, it is possible to access the target as long as the period defined by the request is still valid.

14.4.2. Approval request on passwords

If an approval workflow has been defined in WALLIX Bastion to be allowed to access the target's password, the user must send an approval request and notify approvers to be able to view the password.

When viewing the target's credentials from an authorization on the “Passwords” page, Access Manager displays the `Approval Request` window to send the request. This approval request is defined by the following attributes:

- `Start Date`: Start date and time from which the access is requested. By default, this is the current date and time. A calendar is available to modify the data by clicking into the frame.
- `Hours` | `Minutes`: Duration during which the access is requested. By default, this duration is set to 1 hour. However, the fields are available for update.
- `Ticket Reference`: Ticket reference to specify for the approval request. This field is displayed/hidden and, if displayed, required/optional according to the authorization definition in WALLIX Bastion.
- `Comment`: Comment to specify the reason for the approval request. This field is displayed/hidden and, if displayed, required/optional according to the authorization definition in WALLIX Bastion.

The user can then view the status of the approval request on the “Approval Requests” page accessible from the “Approval” menu. For further information, refer to Section 14.4.3, “View of the approval request status”.

Once a request is approved, it is possible to access the target's password as long as the period defined by the request is still valid.

14.4.3. View of the approval request status

On the “Approval Requests” page, accessible from the “Approval” menu, the user can view the status of the requests sent for approval as long as their duration has not expired.

Access Manager always updates data when this page opens. If needed, the `Synchronize` button on the right upper part of the page allows to refresh and retrieve up-to-date approval requests.

On the search area in the upper part of the page, the user can specify criteria or enter keywords to retrieve the relevant approval requests. Data is displayed on chronological order on the lower part of the page by clicking on the `Search` button.

The user can only view on this page valid requests, i.e. whose duration has not expired. The request can be in either one of the following status:

- “Pending”: the quorum representing the minimum number of positive answers required for the authorization has not been reached.
- “Accepted”: the quorum has been reached for approval. The user is notified by email and is then allowed to connect to the target or view the target's password from the authorization as long as the request duration has not expired.
- “Rejected”: the approval request has been rejected and is thus invalid. The user is then notified by email of the reason for the rejection.
- “Cancelled”: the accepted approval request has been cancelled by the approver before its expiration. The target access is not granted anymore.

Each line provides the following information:

- the status of the request
- the current quorum
- the ticket reference associated with the request
- the demanding user
- the target for which a request is demanded
- the request start date and time
- the request end date and time
- the request duration
- the comment associated with the request

By clicking on the information icon at the beginning of the line, the user can get a detailed view of the answers provided for the request on the `Approval details` window. When the request is “Pending” for approval, the user can click on the `Cancel Approval` button to cancel it.

14.5. Approval request management for the approver

When a user issues an approval request from a given authorization, a group of approvers is notified by email and can decide to allow or reject the connection to a target or the access to the target's credentials from WALLIX Access Manager.

The group of approvers is set during the approval workflow definition on a given authorization in WALLIX Bastion.

Only users whose profile is associated with the rights for the `Approver` profile: `View Approval` and `Update Approval` can manage answers to the approval requests issued by users and also view the approval history from the “Approval” menu.

14.5.1. Answer to the approval request

On the “Current Approvals” page, accessible from the “Approval” menu, the approver can view all the requests pending for approvals sent from users to access targets or target's credentials and to which s/he must provide an answer.

Access Manager always updates data when this page opens. If needed, the `Synchronize` button on the right upper part of the page allows to refresh and retrieve up-to-date approval requests.

On the search area in the upper part of the page, the approver can specify criteria or enter keywords to retrieve the relevant approval requests. Data is displayed on chronological order on the lower part of the page by clicking on the `Search` button.

The approver can only view on this page valid requests, i.e. whose duration has not expired. The request can be in either one of the following status:

- “Pending”: the quorum representing the minimum number of positive answers required for the authorization has not been reached.

> ***Note:***
>
> When the first approver accepts the request and the start date and time have been reached:
>
> – the start date and time of the request are then updated with the start date and time of this action
>
> – the end date and time are then extended for the request duration from this action

- “Accepted”: the quorum has been reached for approval. The user is then allowed to connect to the target or view the target's password from the authorization as long as the request duration has not expired. However, the approver can cancel the accepted approval request before its expiration to prevent the user from accessing the target again.

Each line provides the following information:

- the Bastion instance for which a request is demanded,
- the status of the request
- the current quorum
- the ticket reference associated with the request
- the demanding user
- the target for which a request is demanded
- the request start date and time
- the request end date and time
- the request duration
- the comment associated with the request

By clicking on the information icon at the beginning of the line, the approver can get a detailed view of the answers provided for the request by other approvers on the `Approval details` window. The approver can also either accept or reject or cancel the approval request from this window by clicking on the relevant buttons: Access Manager displays the `Answer to an approval request` window described below.

On the “Current Approvals” page, the approver can provide an answer to the request by clicking on the corresponding status: Access Manager displays the `Answer to an approval request` window. The approver can then:

- enter a required comment to specify the reason of the approval/rejection/cancellation regarding the request
- if needed, reduce the request duration by changing the value in the fields
- if needed, reduce the timeout set for the connection by changing the value in the field. If the user has not connected to the target and this timeout has been reached, then the “Accepted” request is automatically “Closed”.
- click on the `Cancel` button to cancel the “Accepted” request before its expiration in order to prevent the user from accessing the target again
- click on the `Accept` button to approve the “Pending” request and then grant access to the user once the quorum has been reached
- click on the `Reject` button to reject the “Pending” request and then deny access to the user

14.5.2. View of the approval history

On the “Approval History” page, accessible from the “Approval” menu, the approver can view all the requests which are no longer valid. It is thus no longer possible to answer to these requests.

Each line provides the following information:

- the Bastion instance for which a request is demanded,
- the status of the request
- the quorum reached for the request
- the ticket reference associated with the request
- the demanding user
- the target for which a request is demanded
- the request start date and time
- the request end date and time
- the request duration
- the comment associated with the request

By clicking on the information icon at the beginning of the line, the approver can get a detailed view of the answers provided for the request on the `Approval details` window.

14.6. Session invite feature

The Session invite feature allows a privileged user (the host) to share their current RDP or VNC session with an external user (the guest), who does not have an associated user account in WALLIX Access Manager or WALLIX Bastion.

> ***Important:***
>
> The Session invite feature is not supported by WALLIX Bastion4Cloud Edition.
>
> Session invite is not available for SSH sessions as well as application targets.
>
> Session invite is not compatible with tablets and smartphones.

The right to invite an external user to a session is granted by a WALLIX Bastion administrator through an authorization. Only one external user can be invited to join a current session.

Once the host is connected (via WALLIX Access Manager) to a session which is eligible for the Session invite feature, they can generate an invitation link. This link needs to be shared by the host with their guest before it expires.

> ***Important:***
>
> Invitation links are generated based on the host name used by the host users to access WALLIX Access Manager. The host name used by the host users must therefore be accessible by their guest users so that they can join the session.

The guest's actions in the shared session are limited by two options:

- `View only`: the guest can only view the current session
- `View and Control`: the guest can view the current session and then control it using the mouse and keyboard when the host gives them control. The guest's actions are observed by the host, who can regain control of the session at any time.

The guest's session is linked to the host's session. Thus, when the host closes their session, the guest's session closes automatically. The host also has the possibility to cancel the sharing: the invitation link becomes invalid and the connected guest is disconnected from the shared session.

The host and guest actions are recorded in the logs of WALLIX Bastion.

For further information on the Session invite workflow, refer to the “Session invite” chapter in the *User guide*.

Chapter 15. Application settings

The application settings can be managed from the “Settings” menu and are only available to users whose profile is associated with the `Update Settings` right.

15.1. Settings

From the “Application” tab on the “Settings” page, it is possible to view and edit the application parameters. These parameters may have a different value depending on the organization.

The display of a parameter depends on the organization type: for example, the expandable section `Bastion` is not displayed on the global organization.

The “Baseline Organization” contains all the parameters for the application and can be used as a reference value.

An administrator from the global organization can edit the parameters of another organization as well as those of the baseline organization. A list of values is available in the upper part of the page to select the desired organization. The user can filter the parameters of a given organization by entering data in the area above the table so as to restrict the display to the relevant rows.

A user from the global organization can view and edit the parameters of any organization and those of the baseline organization. A list of values is available in the upper part of the page to select the desired organization. The user can filter the parameters of a given organization by entering data in the area above the table so as to restrict the display to the relevant rows.

A user from a non-global organization (such as the **`default`** organization) has only access to the parameters of his or her organization. The user can filter the parameters of the organization by entering data in the area above the table so as to restrict the display to the relevant rows.

A toggle button at the level of each parameter in the expandable sections allows the user to edit the corresponding value.

All the parameters within a given organization can be reset to the baseline organization values by clicking on the button `Restore baseline organization values` at the bottom of the page.

All the parameters of the baseline organization can be reset to their default values by clicking on the button `Restore built-in values` at the bottom of the page.

Each modification of a parameter from the application settings can be viewed in the audit logs.

15.1.1. Specific application settings

This section describes some specific application parameters available from the “Application” tab in “Settings” > “Application Settings”.

15.1.1.1. `Bastion` section

The `bastion.connection.timeout` parameter allows the administrator to configure the connection timeout to a bastion. The default value of this timeout is 10 seconds. It is recommended to set this value as low as possible:

- to reduce the waiting time when a bastion in a cluster is unreachable
- to prevent failed session openings

15.1.1.2. Language section

The parameters in the expandable `Language` section cannot be accessed in order not to affect the proper functioning of Access Manager.

15.1.1.3. RDP section

The `rdp.clipboard.size` parameter allows the administrator to specify the maximum number of characters in the clipboard buffer when copying and pasting from a local computer to an RDP session.

> ***Note:***
>
> The total number of characters that can be shared at once from a local computer to an RDP session via the clipboard corresponds to the `rdp.clipboard.size` parameter multiplied by 10. If the number of characters in the text to be copied is greater than this value, then the text will be truncated.

The `rdp.download.maxFileNumber` parameter allows the administrator to specify the maximum number of files which can be downloaded at one time.

The `rdp.download.maxFileSize` parameter allows the administrator to specify the maximum size not to be exceeded when downloading a set of files.

The `rdp.shared.clipboard` parameter allows the user to share text and files between multiple RDP sessions, as well as to drag and drop files between the user's workstation and the target. When this parameter is enabled, the `Clipboard` menu is no longer displayed in the session. In conjunction with `session.legacy.copyPaste`, text and files can only be copied between RDP sessions.

> ***Note:***
>
> Mozilla Firefox does not allow text to be copied and pasted directly from the user's workstation to the RDP session.

15.1.1.4. REST API section

The `restapi.connection.timeout` parameter allows the administrator to configure the connection timeout to a bastion REST API. The default value of this timeout is 10 seconds. It is recommended to set this value as low as possible:

- to reduce the waiting time when a bastion in a cluster is unreachable
- to prevent failed session openings

The `restapi.request.paging.limit` parameter allows the administrator to page the number of items to be retrieved from a bastion REST API in case of latency issues when loading screens of Access Manager. The default value -1 means that all items are retrieved at once when the REST API is called. Note that this parameter does not include session audit.

15.1.1.5. Session section

The `session.keepAlive` parameter allows the administrator to enable or disable the KeepAlive function. This function uses the ping mechanism of the WebSocket protocol (for further information, refer to https://datatracker.ietf.org/doc/html/rfc6455) to keep the RDP, SSH, SFTP and RAWTCPIP session open when there is no network traffic between Access Manager and the client. To enable the KeepAlive function, a time interval (in seconds) between two KeepAlive messages must be set. By default, the parameter is disabled (value set to “0”) and it allows a maximum value of 3600 seconds. When the session is closed, KeepAlive automatically stops sending messages.

> ***Warning:***
>
> The Access Manager service must be restarted after changing the value of the `session.keepAlive` parameter .
>
> Enabling the KeepAlive function has no impact on the `session.maxInactiveInterval` parameter .

The `session.legacy.copyPaste` parameter allows the administrator to prevent the automatic synchronization of the clipboard between the user workstation and the target, in order to protect against potential security risks. By enabling this parameter, the use of the `Clipboard` menu becomes mandatory. This parameter is disabled by default.

> ***Note:***
>
> Mozilla Firefox does not allow text to be copied and pasted directly from the user's workstation to the RDP session.

The edition of the `session.maxInactiveInterval` parameter in the expandable `Session` section requires a logout from the session for the changes to be taken into account.

The `session.short.title.mode` parameter allows the administrator to shorten the title of the browser tab for the RDP, SSH and SFTP sessions. By enabling this parameter, the format of the title will be “login@target name” instead of the full name of the authorization.

15.1.1.6. Tag section

The `tag.target.passwordTreePath` parameter allows the administrator to define the hierarchy of the folders for the authorizations on the passwords, on the “Tag Explorer” tab. If the connected user has defined a hierarchy of folders in his or her preferences, then the hierarchy defined by this user will be applied by default.

The `tag.target.sessionTreePath` parameter allows the administrator to define the hierarchy of the folders for the authorizations on the sessions, on the “Tag Explorer” tab. If the connected user has defined a hierarchy of folders in his or her preferences, then the hierarchy defined by this user will be applied by default.

15.1.1.7. `Universal Tunneling` section

The `ut.otp.ipsource.verification` parameter allows the administrator to enable the source IP verification when connecting with an OTP (one-time password).

The `ut.otp.lifetime` parameter allows the administrator to define the lifetime (in seconds) of the OTP.

The `ut.otp.purge.period` parameter allows the administrator to define a period (in minutes) for performing purges of expired and unused OTPs.

The `ut.port.range` parameter applies to the connection between the Access Manager and the Bastion. It allows the administrator to define a range of ports available on the Access Manager server for port forwarding when establishing a RAWTCPIP session.

The `ut.sshtunnel.buffer.size` parameter allows the administrator to define the buffer size used for SSH port forwarding. This parameter should ONLY be changed upon instructions from WALLIX Support Team.

The `ut.sshtunnel.network.interface` parameter allows the administrator to define the network interface used on the Access Manager server to open a local port for SSH port forwarding. This parameter can be edited to switch between the IPv4 or IPv6 loopback address.

The `ut.websocket.buffer.size` parameter allows the administrator to define the buffer size used for WebSocket port forwarding. This parameter should ONLY be changed upon instructions from WALLIX Support Team.

The `ut.websocket.deactivate.compression` parameter allows the administrator to deactivate the WebSocket compression.

15.1.1.8. Web section

The “list” icon of the `web.remoteCmd.cipherSuite` parameter in the expandable `Web` section allows to display the list of the allowed cipher suites within the application.

This parameter allows to specify the list of cipher suites which are allowed and/or forbidden by the server, using the syntax of the OpenSSL "ciphers" command.

15.2. Logs

Only an administrator from the global organization can access and edit the “Logs” tab on the “Settings” page.

From this tab, it is possible to customize the various log levels for specific events triggered in relation to the application, configuration, target access or third-party clients. This tab should be used under the guidance of the product Support Team as it may be useful for troubleshooting.

The user can filter the log levels by entering data in the area above the table so as to restrict the display to the relevant rows.

The log levels can be set:

- individually for each module: a toggle button is provided to enable the configuration at the end of each row.

  When configuring the log levels individually, an orange warning icon (“Verbose Module”) is displayed on the rows for which an important data volume is generated.
- globally: the `Default` frame in the upper part of the page allows the selection of a log level which will be applied to all the modules within the page. In this case, it remains possible to switch the toggle button on a given row to select a different log level value. However, the toggle button must not be switched again before saving the selection as the default value would be automatically set back.

The access log file (i.e. “access.log”) gathering connections from external clients to the Access Manager server and the technical log files (i.e. “error.log” and “tech.log”) can be downloaded as archive by clicking on `Download Logs Archive (ZIP)` at the bottom of the page.

The access log file (i.e. “access.log”) is also available in the following directory: `/var/log/wallix/wabam`. This log is similar to the access log of the Apache server. For further information, refer to `https://httpd.apache.org/docs/2.4/logs.html#accesslog`. The generation of this log file can be set in section `Access log configuration` within the file `wabam.properties`. This file is under the configuration directory : `/var/wab/etc/wabam`.

> ***Warning:***
>
> The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

15.3. Database backup and restore

It is recommended to backup the database and the file `wabam.properties` periodically. Many solutions are available for achieving database backups. The chapter describes only one of them. Check with your database administrator what is the best solution for your own deployment. The file `wabam.properties` is available in the configuration directory which is, by default, `/var/wab/etc/wabam`.

15.3.1. Database backup and restore from the Web interface

From the “Database” tab on the “Settings” page, it is possible to back up and restore the database. This tab is only available to users whose profile is associated with the `Restore organization` right.

Only an administrator from the global organization can choose to back up or restore the whole database as he or she can view and manage all organizations.

A user from a non-global organization (such as the **`default`** organization) can only back up or restore the database related to his or her organization.

> ***Note:***
>
> The size of a backup file cannot exceed 10 megabytes. If the size of the file exceeds 10 megabytes, we recommend to perform the backup and restore from the command line tool. For further information, please refer to Section 15.3.2, “Database backup and restore from the command line tool”.

15.3.1.1. Database backup from the Web interface

To back up the database, a password or a key must be provided on the `Encryption Key` area in the upper part of the page to encrypt sensitive data (such as the API keys for the bastions). From this area, it is possible to:

- click on the red eye icon on the right to display the data entered
- click on the `Copy` icon on the left to copy the password or the key entered into the clipboard

On the `Save Database` section:

- the administrator from the global organization can select the desired organization from the list of values. The administrator can then choose to back up the whole database by selecting `All Organizations` or a single database by selecting the desired organization from this list.

  This list is not available for the user from a non-global organization (such as the **`default`** organization): the name of his or her organization is directly displayed.

- once the appropriate data has been selected from the list of values, it is possible to click on the `Export` button on the right to download the back up of the database as a ZIP archive.

15.3.1.2. Database restore from the Web interface

> ***Note:***
>
> The database restore operation can only be performed on an Access Manager instance whose database schema version is the same.

To restore the database, the password or the key entered on the `Encryption Key` area for the database backup must be provided again. It is possible to click on the red eye icon on the right to display the data entered.

On the `Restore Database` section:

- the parameters related to the database must be dropped or uploaded as a ZIP archive on the dedicated area.

> ***Caution:***
>
> Access Manager performs an integrity check on the files during the database restore. Therefore, the restore operation fails if any of the files have been modified.

- once the ZIP archive has been uploaded, the administrator from the global organization can then choose to restore a new database including new organizations by clicking on the `Create` button or restore an existing database by clicking on the `Reset` button.

> ***Caution:***
>
> Only an administrator from the global organization can view the `Create` button. When the administrator restores a database with new organizations, all existing data will be overwritten.

15.3.2. Database backup and restore from the command line tool

15.3.2.1. Database backup from the command line

The database data, key store and the file `wabam.properties` can be backed up from the command line tool, using the following command:

```
wabam-backup -d <backup_directory> -n <backup_filename> -p <backup_password>
```

Where:

- *backup_directory* corresponds to the directory where the backup file is stored
- *backup_filename* corresponds to the name to use for the backup file (the created file will have exactly the given name. No file extension is forced in this case). If this parameter is omitted, the backup file name will have the following format: `backup_yyyyMMdd-hhmmss.wambk`.
- *backup_password* corresponds to the password used to encrypt the backup file. If *<backup_password>* is omitted, the user will be prompted to enter a password.

> **_Note:_**
>
> The generated backup file is a .zip file, which can be opened with any zip tool that supports 256-bits AES encryption (e.g.: 7zip).

The option **-h** shows the help message listing the arguments which can be used to perform this action:

```
wabam-backup -h

The available options are:
        --backupDir-d value: directory where the backup archive is created.
        [--backupName-n value]: name of the archive to generate.
        [--backupPassword-p value]: password used to protect the backup archive.
 If omitted, the user is prompted to enter the password to use.
        --configfile-f value: name and path of the configuration file to use -
 already included in the executable.
        [--help-h]: list of the arguments that can be used to backup wabam data.
        [--skipCertificate-k]: skip certificate export[--skipConfig-c]: skip
 configuration export
```

> **_Warning:_**
>
> The commands used when installing the Access Manager appliance are only supported for MySQL Community Server and MariaDB Server databases. Therefore, it is not possible to run these commands if an Oracle Database Server is declared as the database type in the file `wabam.properties`.

15.3.2.2. Database restore from the command line

> **_Warning:_**
>
> Before performing the restore, make sure that the service WALLIX Access Manager is not running.

A backup can be restored from the command line tool, using the following command:

```
wabam-restore -b <backup_file> -p <backup_password>
```

Where:

- *backup_file* corresponds to the backup file to restore
- *backup_password* corresponds to the password used to decrypt the backup file

The option **-h** shows the help message listing the arguments which can be used to perform this action:

```
wabam-restore -h

The available options are:
        [--adminDbPassword-a value]: admin DB password.
        [--adminDbPasswordFile-P value]: path to the configuration file
 containing the admin DB password - The file must contain a property
 privileged_user_password.
```

```
        --adminDbUser-u value: login of admin DB user this account is used for
database initialization.
        --backupFile-b value: backup file.
        --backupPassword-p value: password used to protect the backup archive.
        --configfile-f value: name and path of the configuration file to use -
already included in the executable.
        [--help-h] : list of the arguments that can be used to backup wabam
data.
        [--skipCertificate-k]: skip certificate import.
        [--skipChecksumResult-i]: ignore the checksum result and restore even if
it is failed.
        [--skipConfig-c]: skip configuration import.
```

> ***Warning:***
>
> The commands used when installing the Access Manager appliance are only supported for MySQL Community Server and MariaDB Server databases. Therefore, it is not possible to run these commands if an Oracle Database Server is declared as the database type in the file `wabam.properties`.

Chapter 16. Session audit settings

> ***Warning:***
>
> IPv6 is not supported for session audits.

Access Manager embeds an audit session repository. The session audit data can be displayed on the “Session Audit” page accessible from the “Audit” menu. For further information, refer to Chapter 19, *Session audit data*.

The settings to retrieve session audit data can be managed from the “Settings” menu. Only an administrator from the global organization can access the “Session Audit Settings” submenu.

Data on this page is displayed as read-only for the global administrator but it can be edited by clicking on the “Edit” button.

These settings are defined by the following attributes:

- `Session Repository Access Mode`: The connection mode used to access the session audit repository
  - `Localhost only`: When this mode is selected, then the session audit repository is accessed locally on the current Access Manager instance. In this case, the Web browser and the Access Manager instance must be both running on the same workstation.
  - `IP and localhost`: When this mode is selected, then the session audit repository can be accessed and receives queries from an external Web browser (in particular when assistance is required from the Support Team).
  - `Clustered`: When this mode is selected, then several Access Manager instances can interact with each other and share the access to their own session audit repository between them. In this case, there is a master instance and there are slave ones.
- `HTTPS Login`, `HTTPS Password`: The login and the password to provide for querying the session audit repository. These fields should be defined to ensure secure access to the repository. For the `Clustered` mode, the values entered or edited on an Access Manager instance will apply to all the other cluster members.
- `Repository Hostname`: The IP address or the DNS name of the local Access Manager instance to be defined for the `IP and localhost` or `Clustered` connection mode.
- `Other Cluster Member IPs`: The IP address(es) of the other Access Manager instance(s) when the `Clustered` mode is selected as the connection mode. To add a node, first enter the IP in this field then click on the + icon.

> ***Note:***
>
> Information retrieval is more robust between three Access Manager instances at least.

- `Repository Port`: The access port configured for the local Access Manager instance
- `Cluster Name`: The name of the local Access Manager instance. When the `Clustered` mode is selected as the connection mode, the name entered in this field must be the same for all the configured Access Manager instances.
- `Cluster Master`: Toggle button to specify whether the instance is the master or the slave node, when the `Clustered` mode is selected as the connection mode.
- `SSL Certificate Management`: This area can be expanded and allows to define certificates to secure access to the audit session repositories.

On the left part, it is possible to drop or upload the SSL certificate of the Web server by providing a PKCS#12 file. If needed, a password can also be provided for the certificate on the `Certificate Password` field. By default, a self-signed certificate is generated during the installation.

On the right part, it is possible add the certificates related to the other cluster members (i.e. Access Manager instances), when the `Clustered` mode is selected as the connection mode. To do so, it is necessary to click on the Add button to display the `New Trusted Certificate` window and enter the relevant data. It will then be displayed below the `Trusted Certificates` area.

> ***Warning:***
>
> Each Access Manager instance must add the trusted certificate related to the other instances to allow communication between all the session audit repositories. At this stage, the master node and the slave ones must be specified via the `Cluster Master` toggle button.

The button `Show Repository Certificate` allows to display the certificate for the current Access Manager instance.

The `Test Configuration` button allows to test the connection for the current instance configuration.

> ***Important:***
>
> The following parameters are available for configuration in the expandable section `Session Audit` from the “Application” tab on the “Settings” page (accessible from the menu “Settings” > “Application Settings”):
>
> - `sa.live.update.frequency`: allows the administrator to specify how often audit data is updated for the current sessions. This value is expressed in seconds.
> - `sa.session.reader.groupsize`: allows the administrator to specify the number of sessions read each time the REST API is queried.
> - `sa.session.retention.days`: allows the administrator to specify the number of days for which the audit date is kept. This parameter is set to 30 days by default.
> - `sa.session.user.filter`: when set to “Yes”, the users whose profile defined in the bastion allows viewing the session audits can access the session details and videos. The default value of this parameter is “No” i.e., the auditors of Access Manager have access to the details and videos of the sessions of their organization regardless of the configuration made in the bastion.
> - `sa.session.user.prefilter`: when set to “Yes”, the buttons giving access to the session details and videos are removed if the user does not have the right to access this information in his/her profile defined in the bastion. The default value for this parameter is “Yes”. This parameter is used only when the parameter `sa.session.user.filter` is enabled.
> - `sa.update.frequency`: allows the administrator to specify how often audit data is updated. This value is expressed in seconds.

Chapter 17. Database settings

> **Important:**
>
> The IP addresses which can be set on Access Manager support both IPv4 and IPv6 formats.

During the initial installation, Access Manager will create a fresh database (i.e. a schema) and a database user for connecting to it. This database is created in the server instance provided with the Access Manager appliance.

> **Note:**
>
> The configuration of the database settings can be done using the `wabam-config-database` command.

The database settings can be displayed on the “Database Settings” page accessible from the “Settings” menu.

These settings are displayed as read-only data for the global administrator and are defined by the following attributes:

- `Database Type`, `Host`, `Port`: These fields define the server instance. For a database, the `SID` field is also provided.
- `Database Name`: The name of the database. For the latter, the database is created implicitly with the user and has the same name.
- `Database User`, `Database User Password`: The database user is created with the minimal rights. Access Manager will use this user during normal operations. The name and the password to be used for this user are specified in these fields.
- `Privileged User`, `Privileged User Password`: In order to create the database, a privileged database user should be provided. These fields define this privileged user. For a database, this account should be able to log as `sysdba`. When installing newer versions of the software, the Access Manager administrator will have to provide again the privileged database user if the database schema has to be modified for the upgrade.
- `Pool Size`: The minimum and maximum values for the database connection pool size.
- `Secure`: Toggle button enabled by default to secure the connection to the MySQL database. This attribute is required for any version of MySQL using the *caching_sha2_password* authentication plugin as an SSL connection is required to connect to the database.
- `Azure Database`: Toggle button that allows Access Manager to determine the connection method to use when the database is hosted on Azure Cloud platform.

The `Test Connection` button allows to test the connection to the database.

During the initial installation, if the name specified on the `Database User` field already exists on the database, a warning message is displayed when saving the database parameters. It is then required to choose an action regarding this user among the suggestions by clicking on the dedicated button.

Chapter 18. Audit log

Access Manager records all user actions.

Only users whose profile is associated with the `View Audit` right can browse the actions related to their organization on the “Log” page accessible from the “Audit” menu.

A record contains the action (e.g.: "Login"), the organization concerned, the type of the object affected by the operation, the name of the object, the name of the user performing the action, the timestamp and the status of the action. Moreover, by clicking on the icon at the beginning of the row, details related to the action are displayed.

Chapter 19. Session audit data

The session audit data can be displayed on the “Session Audit” page accessible from the “Audit” menu. This page is only available to users with the `Auditor` profile, as well as users whose profile defined in the bastion is associated with the right to view the session audits.

> ***Note:***
>
> A delay necessary for the display of the audit data on the page may occur while a session is running.

On the search area in the upper part of the page, the user can enter keywords to retrieve the relevant sessions. This search may concern current or closed sessions. It is possible to refine the search using the wildcard symbol “*”: a click on the information icon will provide the possible syntaxes. Data is displayed on the lower part of the page by pressing the `Enter` key or by clicking on the magnifier icon on the right of the area.

On the advanced search form, the user can specify criteria to retrieve the corresponding sessions then click on the `Search Sessions` button to display the data on the lower part of the page.

The sessions corresponding to the search are listed by date in the lower part of the page. The following information is provided for each line:

- the date, start/end time and duration for the closed session or
- the date and start time for the current session
- the name of the bastion
- the user name
- the target protocol
- the name of the target device
- the name of the target account
- the status of the session

For each session, it is possible to:

- click on one of these elements' attribute to restrict the search to the related criterion
- display detailed information by clicking on `View session detail`. The information can then be viewed on the `Session Detail` window.
- view the current session in a popup window or in a dedicated web browser tab by clicking on `View session`: a viewer allows then to go through the session video in real-time.

  > ***Note:***
  >
  > The option `View session` is only available for the current sessions.

- view the session recording in a popup window or in a dedicated web browser tab by clicking on `Replay session`: a viewer allows then to go through the session video. The latter can be downloaded by clicking on `Download video` below the viewer.

  > ***Note:***
  >
  > The option `Replay session` is only available for the recorded sessions.

- view the session recording for a given action at a given time by clicking on the session's chronological entries. These entries are displayed if the session log redirection is enabled for the bastion's sessions in WALLIX Bastion. A viewer allows to go through the video of the selected sequence on the `Session Audit` web browser tab.

Chapter 20. Scalability and High-availability

The following sections outline the implementation of load-balancing with the deployment of several Access Manager instances or a cluster of Bastions within a single Access Manager instance.

20.1. Deploying several Access Manager instances

In order to implement load-balancing, it is possible to deploy several Access Manager instances. Such a deployment will also provide high-availability by preventing Access Manager to be a single point of failure. The load-balancing itself should be implemented in front of the instances.

The first instance has to be installed normally. However the following ones require to manually edit their file `wabam.properties`. This file is under the configuration directory : `/var/wab/etc/wabam`. The installation encryption key (`crypto.install.key`), the database settings (all properties with a name starting with `db.connections`) and the installation administrator credentials (values starting by `user.admin`) should be copied from the first installation.

> ***Note:***
>
> If the databases of the two appliances are replicated, there is no need to duplicate the `db.connections` parameters.

If the administrator credentials have to be changed later, they have to be changed on the first instance and copied to the other ones.

> ***Warning:***
>
> The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

20.2. Deploying a cluster of bastions within a single Access Manager instance

Setting up a cluster of bastions within the same Access Manager instance makes it possible to identify the authorizations which are common to several bastions in the cluster, in order to distribute the load when accessing targets. So, when connecting to a target via an authorization common to several bastions, the call will be made to the bastion with the fewest sessions in progress.

When the bastions in the cluster are *identical*, i.e. they share the same configuration (notably the same proxy certificates) and the same authorizations, it is recommended to enable the `bastion.cluster.identical.mode` parameter in the `Bastion` expandable section from the “Application” tab on the “Settings” page (accessible from the menu “Settings” > “Application Settings”).

Enabling this parameter provides a significant performance improvement, as only information from one of the bastions in the cluster is stored and synchronized.

Chapter 21. Parameters for the global configuration

21.1. RDP client name customization

By default, the RDP client name corresponds to the hostname of the Access Manager server.

The `rdp.clientName` parameter can be configured to define a new RDP client name which will be used during RDP sessions. In a cluster, this parameter also allows you to set a different RDP client name for each WALLIX Access Manager.

This parameter does not exist by default in the `wabam.properties` file.

To add or change it, go to the configuration directory: `/var/wab/etc/wabam`.

> ***Warning:***
>
> The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

21.2. Java Virtual Machine options

The heap size, one of the memory areas of the Java Virtual Machine (JVM), is a parameter that indicates the maximum amount of memory the server can use.

The default heap size is 2373MB for the appliance and 60% of the total physical memory installed on the server during installation for the Linux and Windows applications.

If more memory is required or the appliance memory is increased, the heap size can be changed by editing the *-Xmx* option in the `wabam.vmoptions` file, which is located by default in:

- `/var/wab/etc/wabam/wabam.vmoptions` on WALLIX Appliance
- `C:\ProgramData\Wallix\wabam\conf\wabam.vmoptions` on Windows
- `/etc/opt/wallix/wabam/wabam.vmoptions` on Linux

> ***Important:***
>
> Backup the `wabam.vmoptions` file before making any changes. This backup can be used in case of syntax errors, line deletions, etc. introduced during the file modification.

Use this syntax to specify the maximum amount of memory to use:

```
# Enter one VM parameter per line
-Xmx<value><unit>
```

Where:

- `<value>` is an integer representing the maximum amount of memory
- `<unit>` can be “m” for MB or “g” for GB

Note:

Access Manager must be restarted after modifying the `wabam.vmoptions` file.

The change of the heap size can be verified after restarting the Access Manager by consulting the “tech.log” logs. A log containing “JVM arguments” displays the new value for the maximum Java heap size. For example:

```
2023-12-13 18:18:14;[INFO];cat=Node;Node(299);JVM arguments [-
Dfile.encoding=UTF-8, -Xmx3780m, -XX:MaxDirectMemorySize=256M, -
Djava.library.path=/opt/wallix/wabam/native]
```

21.3. Disclosure of IP addresses in HTTP headers

In order to protect Access Manager from vulnerabilities related to IP address disclosure when the HTTP protocol version is downgraded from 1.1 to 1.0, it is necessary to configure the `web.host.header.https` parameter before changing the version.

This parameter allows you to configure the value to be displayed in the headers for the HTTP 1.0 requests. If the parameter is not set, then the IP address will be displayed in the header. The default value of this parameter is the hostname.

This parameter can be manually changed in the file `wabam.properties`. This file is available in the configuration directory: `/var/wab/etc/wabam`.

Warning:

The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

21.4. DoS filter

A DoS filter is available to protect Access Manager against security vulnerabilities and in particular against denial of service attacks (DoS attacks).

The DoS filter parameters can be manually changed in the file `wabam.properties`. This file is available in the configuration directory: `/var/wab/etc/wabam`.

Warning:

The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

The parameters to specify to secure Access Manager are the following:

- `web.max.requests.perSec`: allows you to specify the maximum number of requests per second which can be accepted by the server. Requests which excess this number are first delayed, then ignored. By default, this parameter is set to 60.
- `web.delays.overrate.limit`: allows you to specify the delay (in milliseconds) imposed on all requests which are over the rate limit before they are ignored. By default, this parameter is set to 100.

- `web.availabilityTimeout`: allows you to specify the delay (in milliseconds) imposed before a request fails. By default, this parameter is set to 0 (deactivated) to allow a large volume transfer during the RDP session.
- `web.rate.usingSession`: when set to *`true`*, this parameter allows you to specify that the usage rate is tracked by session. The default value is *`true`*.
- `web.rate.withRemotePort`: when set to *`true`* and when `web.rate.usingSession` is set to *`false`*, this parameter allows you to specify that the usage rate is tracked by IP and port. The default value is *`false`*.
- `web.rate.ipWhitelist`: allows you to specify a comma-separated list of IP addresses that will not be limited by the usage rate.

- `web.max.connection`: allows you to specify the maximum number of concurrent connections to the server. By default, this parameter is set to 0: this number is then unlimited.
- `web.max.acceptedRate.connection`: allows you to limit the number of concurrent connections that can be accepted during a certain time. By default, this parameter is set to 0: this number is then unlimited.
- `web.max.acceptedRate.time`: allows you to specify the time (in milliseconds) during which the number of accepted concurrent connections is limited. By default, this parameter is set to 0: this number is then unlimited.

When many tunnels are used in Universal Tunneling sessions, the number of requests received by Access Manager may exceed the limit set by the DoS filter. In this case, the DoS filter parameters can be adjusted to accommodate the use of Universal Tunneling by:

- increasing the value of the `web.max.requests.perSec` parameter, or
- adding IP addresses to the `web.rate.ipWhitelist` parameter

21.5. Proxy server management

When a proxy server is placed in front of Access Manager, the information contained in the audit logs is that of the proxy and not that of the user who made the HTTP request.

Parameters to identify the information of the original client are available and can be changed manually in the file `wabam.properties`. This file is available in the configuration directory: `/var/wab/etc/wabam`.

> ***Warning:***
>
> The service Access Manager must be restarted after changing the parameters in the `wabam.properties` file.

Specifying these parameters also helps to avoid connection difficulties and to protect against security vulnerabilities caused by denial of service attacks (DoS attacks).

> ***Note:***
>
> The default value of the parameters corresponds to the standard proxy configuration.

The parameters to specify are the following:

- `web.proxy.activated`: when set to *`true`* (default value), this parameter helps you to specify that an HTTP proxy server is activated.

- `web.proxy.header.forwarded-for`: this parameter helps you to identify the IP address of the client. The default value for this parameter is *`X-Forwarded-For`*.
- `web.proxy.header.forwarded-server`: this parameter helps you to identify the hostname of the proxy server. The default value for this parameter is `X-Forwarded-Server`.
- `web.proxy.header.forwarded-host`: this parameter helps you to identify the original hostname requested by the client. The default value for this parameter is `X-Forwarded-Host`.
- `web.proxy.header.forwarded-port`: this parameter helps you to identify the destination port used by the client. The default value for this parameter is `X-Forwarded-Port`.
- `web.proxy.header.forwarded-proto`: this parameter helps you to identify the protocol (HTTP or HTTPS) used by the client. The default value for this parameter is *`X-Forwarded-Proto`*.
- `web.proxy.header.ssl-sessionid`: this parameter helps you to identify the SSL session ID of the client. The default value for this parameter is *`Proxy-ssl-id`*.
- `web.proxy.header.proxied-https`: this parameter helps you to identify the HTTPS status indicator. The default value for this parameter is `X-Proxied-Https`.
- `web.proxy.header.forward.useRFC7239only`: when set to `true`, this parameter only supports the RFC7239 and therefore only accepts the `Forwarded` header with all the expected information for the HTTP request.

21.6. User data retention policy

In the process of compliance with the GDPR requirements, Access Manager allows the administrator to purge user audit data.

> ***Warning:***
>
> Only audit data generated by Access Manager will be deleted.

User audit data can be purged from the interface of Access Manager, in the expandable `Automatic Audit Purge` section from the “Application” tab on the “Settings” page (accessible from the menu “Settings” > “Application Settings”):

- `purge.audit.active`: allows the administrator to enable the automatic purge of the user audit data. This parameter is disabled by default.
- `purge.audit.hourOfDayToExec`: allows the administrator to specify the time at which the automatic purge is launched each day. By default, this parameter is set to 3, i.e. 3 a.m. This parameter allows values between 0 and 23.
- `purge.audit.purgeOlderThanInDays`: allows the administrator to specify the retention duration (in days) of the audit data. Thus, all audit data older than this value is purged. By default, this parameter is set to 270 days.

The parameters for the automatic purge can also be changed manually in the file `wabam.properties`. This file is available in the configuration directory: `/var/wab/etc/wabam`.

> ***Warning:***
>
> The service Access Manager must be restarted after modifying the parameters in the `wabam.properties` file.

The parameters to specify are the following:

- `purge.audit.active`: when set to *`true`*, it allows the administrator to specify that the automatic purge is activated. The default value for this parameter is *`false`*.

> ***Warning:***
>
> When several Access Manager instances are deployed, the `purge.audit.active` parameter must be enabled only on one of the cluster nodes.

- `purge.audit.hourOfDayToExec`: allows the administrator to specify the time at which the automatic purge is launched each day. By default, this parameter is set to 3, i.e. 3 a.m. This parameter allows values between 0 and 23.
- `purge.audit.purgeOlderThanInDays`: allows administrator to specify the retention duration (in days) for audit data. Thus, all audit data older than this value is purged. By default, this parameter is set to 270 days.

It is also possible to manually purge the audit data of a user by running the following command: `wabam-purge-audit`.

The `[--help -h]` option displays the help message listing the arguments that can be used to purge the audit data of the user.

The `[--logins -l value]` option is mandatory. It allows the administrator to specify the logins of the user whose audit data must be purged. The following syntax rules must be respected:

- the logins must be separated by spaces
- if a login contains a space such as “John Doe”, then it must be entered as “John\ Doe”
- if a login contains a “\” symbol such as “John\Doe”, then it must be entered as “John\\Doe”

The `[--org -o value]` option is mandatory. It allows the administrator to specify the name of the organization on which the audit data of the user must be purged.

The `[--after -a /(\d{2}|\d{4})-\d{2}-\d{2}/]` option allows the administrator to purge the audit data newer than the date entered. The format is as follows: YYYY-MM-DD or YY-MM-DD. If this option is not set, all audit data of the user is deleted.

The `[--before -b /(\d{2}|\d{4})-\d{2}-\d{2}/]` option allows the administrator to purge the audit data older than the date entered. The format is as follows: YYYY-MM-DD or YY-MM-DD. If this option is not set, all audit data of the user is deleted.

The `[--deleted -d]` option allows the administrator to specify inactive users or organizations, i.e. users or organizations who have been deleted, in order to purge their audit data. By default, this option is set to *`false`*.

21.7. Visibility in Web searches

The indexing of Access Manager in search engines is restricted with the X-Robots tag set in the HTTP headers of the Access Manager pages.

To do so, it is necessary to specify the `web.xrobot.header.value` parameter in the expandable section `Web` from the “Application” tab on the “Settings” page (accessible from the menu “Settings” > “Application Settings”).

By default, the `web.xrobot.header.value` parameter is entered with the following values:

- `none`: allows to prevent the indexing of Access Manager and the tracking of the links contained in the Access Manager pages

- `noimageindex`: allows to prevent the indexing of the images from the Access Manager pages

Chapter 22. Troubleshooting

22.1. Resetting password of the baseline organization global administrator

It is possible to reset of the following parameters linked to the authentication and rights of the baseline organization global administrator:

- the password
- the profile and
- the restricted source IPs.

The default administration profile (including all the rights and which can neither be modified nor deleted) is then granted to the global administrator.

> ***Warning:***
>
> Before performing the reset, make sure that the service Access Manager is not running. If the reset is done during an upgrade, it is then necessary to perform the reset a second time at the end of the upgrade.

This reset can be launched as follows:

- under Linux, enter the following command in the command line tool:

```
/opt/wab/sbin/wabam-restore-admin -f <configuration_file_path>
```

  The `[-f]` option is used to set the path to the configuration file. If the option is not set, the path to the `wabam.properties` file is the default path.

- under Windows, run the executable file in: `C:\Program Files\Wallix\wabam\bin\wabam-restore-admin.exe`

The administrator is then requested to enter and confirm the new password in the command line window. Under Windows, it is necessary to press again the `Enter` key to exit the window.

> ***Note:***
>
> A short delay may occur after running the command or the executable file.

Chapter 23. Contact WALLIX Access Manager Support

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

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

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