

USER GUIDE

WALLIX Access Manager 5.0.3.0

Table of Contents

- 1. Introduction 3
 - 1.1. Preamble 3
 - 1.2. Copyright, licenses 3
 - 1.3. Legend 3
 - 1.4. About this document 3
- 2. Overview 4
- 3. Connection to the WALLIX Access Manager Web interface 5
- 4. User preferences 6
- 5. Universal Tunneling sessions (RAWTCPIP) 8
- 6. Session invite 9
- 7. Contact WALLIX Access Manager Support 11

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

This document is the property of WALLIX and may not be reproduced without its prior consent.

All the product or company names mentioned herein are the registered trademarks of their respective owners.

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 User Guide for WALLIX Access Manager 5.0.3.0.

Chapter 2. 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.

Chapter 3. Connection to the WALLIX Access Manager Web interface

To connect to WALLIX Access Manager Web interface:

1. Enter the URL provided by the administrator in the address bar of a browser.

In case of a SAML authentication, you will be redirected to the Identity Provider login page. Go directly to step 3 once the IdP login page is displayed.

2. Select the domain from the drop-down list of the  field to define the domain to authenticate to.
3. Enter or select the account credentials provided by the administrator:
 - enter and validate a login and password or
 - select and validate an X509 certificate

If an error message appears after validation, check that the username / password or certificate is correct. If the connection fails again, contact the administrator.

Chapter 4. User preferences

A user has the possibility to change his/her preferences at any time, regardless of his/her profile and the organization to which he/she belongs, by clicking on his/her name on the right 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.

In the “Application options” section

- **Language:** The interface display language. 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 by the administrator of the organization is used during approval workflows.
- **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. 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. 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 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 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. 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 will be stored in a file with the same name as the downloaded configuration file, followed by the .log extension.

Chapter 5. Universal Tunneling sessions (RAWTCPIP)

TCP traffic can be redirected from a workstation to a target using Universal Tunneling (previously called RAWTCPIP). The main use cases are the following:

- the redirection of a fat client traffic in an IT environment (such as MySQL client)
- the redirection of a fat client traffic in an OT environment (such as Siemens TIA Portal client)

A debug mode is available by enabling the Universal Tunneling - Debug Mode button on the "Preferences" page. This button must be enabled before downloading the target configuration file.

Important:

Opening multiple Universal Tunneling sessions in parallel is not recommended.

To connect to a Universal Tunneling session:

1. Download the AM Universal Tunneling client by clicking the button at the top of the page.

The Windows version of the AM Universal Tunneling client is a package containing the executable files of the AM Universal Tunneling client and IPloop. To execute the AM Universal Tunneling client, it is necessary to unzip the executable files and place them in the same directory.

2. Click the icon of the desired authorization to either:

- download the target configuration file, or
- open a target configuration pop-up window then download the target configuration file. The pop-up window requires some of the following information, depending on the version:

Local Port for Redirection to your Workstation: option to change the port opened locally on your workstation for the redirection via Universal Tunneling. This field is automatically entered with the target port for WALLIX Bastion version 10.0 or higher. Otherwise, the field is entered with a random port. To connect to a TIA Portal target, the port value 102 must be specified. Universal Tunneling only supports TIA Portal with Bastion version 10.0 or higher.

Seamless Connection: option to enable to allow the access to targets without reconfiguring the workstation.

Loopback Interface: option to select the format of the temporary network interface IP address used to redirect the traffic to an SSH tunnel.

3. Open the target configuration file. This configuration file contains the target connection information and an OTP that will be used to open a session on the target. The OTP has a limited lifetime defined by the administrator (30 seconds by default). The target configuration file must then be used immediately after the download to avoid authentication failures.

Chapter 6. Session invite

The Session invite feature allows a user (the host) connected to WALLIX Access Manager to share their RDP or VNC session with an external user (the guest) i.e., a user 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.

Note that only one external user can be invited to join an ongoing session.

Once the host is connected to a session via an authorization in which session invite has been enabled, they can invite an external user by performing the following steps:

1. Click on the **Invite** button in the header bar to display the session invite configuration window.
2. Select one of the following modes in the window:
 - **View Only**: the guest will only be able to view the session
 - **View and Control**: the guest will be able to view the session and then control it using the mouse and keyboard when the host will give them control (**Give Control** button). The actions of the guest will be observed by the host who will be able to regain control of the session at any time (**Take Control** button). Note that it is only possible to select the **View and Control** mode if it has been enabled in the authorization.
3. Click on the **Generate Invitation** button to generate a URL in the **Invitation Link** field. The **Status** and **Expiration Date** fields are updated: the invitation is pending and an expiration date and time for the invitation link is specified.
4. Click on the **Copy** icon at the end of the **Invitation Link** field to copy the URL to the clipboard.
5. Share the URL with the guest.

Once the invitation link has been shared with the guest, they must copy it into a Web browser and then validate the GDPR message in order to join the host's session before the link expires. The guest can only open one session at a time in their browser and only if they are not already logged into WALLIX Access Manager.

It is up to both users - host and guest - to find the best way to communicate during the shared session.

Note:

Once the shared session is ongoing:

- the host and the guest can only see their own cursor
- the clipboard feature cannot be used by the guest
- the resolution of the guest's session is not configurable (it is the same as the host's session).

The keyboard mapping is not synchronized between the host's session and the guest's session. Thus after changing the user controlling the session it is necessary to ensure that the keyboard mapping is correct: the keyboard layout of the session must match the keyboard layout of the system.

The host can cancel the sharing by clicking on the `Cancel Sharing` button displayed below the generated invitation link. The URL becomes invalid, the guest is disconnected from the shared session and a message is displayed.

The shared session ends as soon as the host leaves the session: the guest's session is then automatically closed and the invitation link is expired as it can only be used once.

The information displayed in the invitation configuration window can be updated by clicking on the `Synchronize` button. The content of the configuration window varies depending on the status of the invitation:

- -: no invitation link has been generated, or the previously generated link has expired, or the session has already been shared and is now closed. The host can select either `View Only` or `View and Control`, if the authorization allows to do so, and then click on the `Generate Invitation` button.
- `Pending invitation`: the host has generated an invitation link which is displayed and can be copied. The expiration date indicates how long the link is valid. The host can cancel the sharing.
- `Shared session ongoing`: the guest has joined the host's session. The host can give control of the session to the guest and take it back or he can cancel the sharing. The field containing the invitation link is now empty as the link has already been used. It is not possible to generate a new invitation while the shared session is ongoing.

Chapter 7. 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