wallix

WALLIX Bastion 12.1.0

Users and Approvers Guide

WALLIX PAM

Contents

1. Introduction

About this guide

This document is the Users and Approvers Guide for WALLIX Bastion 12.1.0.

This guide is intended to help you use WALLIX Bastion to connect to devices such as servers, network devices, security equipments, and administration interfaces. It also provides information on how to verify your access rights, update your preferences, or use your usual connection tools in a way that is compatible with WALLIX Bastion. This guide is also aimed at users tasked with approving access to devices.

The following documents are also provided by WALLIX:

- The Deployment Guide
- The System Operations Guide
- The Functional Administration Guide
- The Sessions Audit Guide
- The SIEM Logs Guide

1.1. General principles

What is WALLIX Bastion?

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

The role of WALLIX Bastion is to:

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

Main notions of WALLIX Bastion

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

Approval workflow

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

User profile

The user profile determines the rights and authorizations of a user in WALLIX Bastion. For example, an administrator has access to administrative configurations of WALLIX Bastion and an auditor has access to session data for auditing purposes, but the opposite is not true.

Authorization-based access

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

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

Contact your administrator if you have questions about your authorizations.

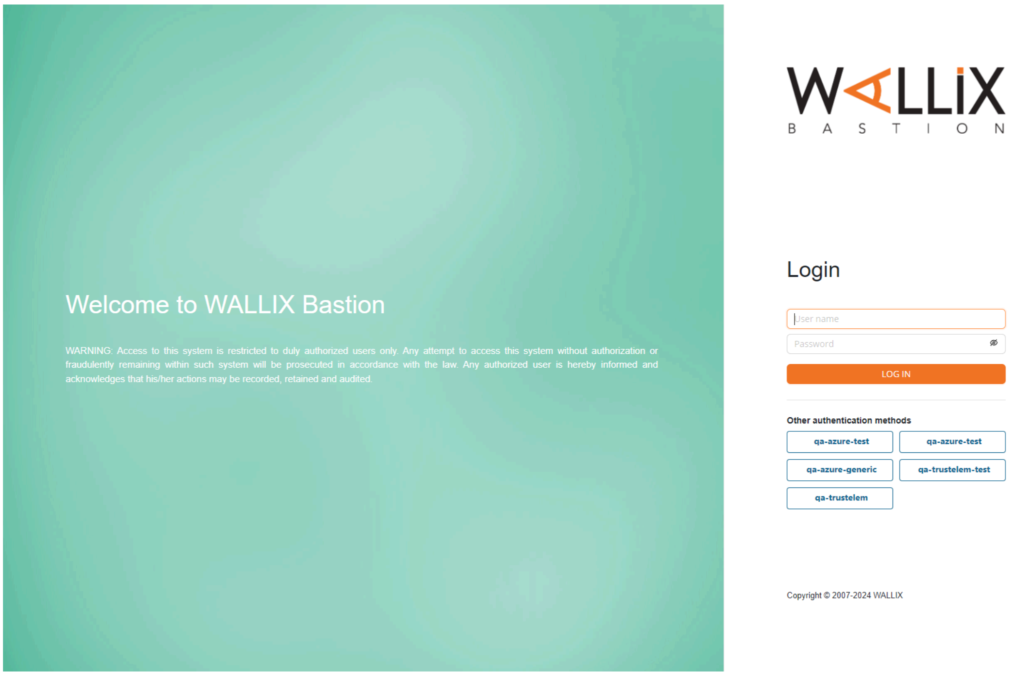
2. WALLIX Bastion authentication

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

Note:

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

Internet Explorer is not supported by the default interface.



Welcome to WALLIX Bastion

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

Copyright © 2007-2024 WALLIX

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

Attention:

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

Related information

[Authentication with a login and password *(on page 8)*](#)
[Authentication with an X.509 certificate *(on page 8)*](#)
[Authentication with an Identity Provider *(on page 8)*](#)
[Authentication with Kerberos *(on page 9)*](#)

2.1. Authentication with a login and password

Procedure

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

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

2.2. Authentication with an Identity Provider

Procedure

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

2.3. Authentication with an X.509 certificate

About this task

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

Note:

When you log in with an X.509 certificate, an alternative authentication mode is available for the sessions started directly through a client (SSH or RDP) while you remain connected. For more information, refer to Simplified authentication in X.509 mode *(on page 17)*.

Before you begin

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

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

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

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

Procedure

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

Note:

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

Results

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

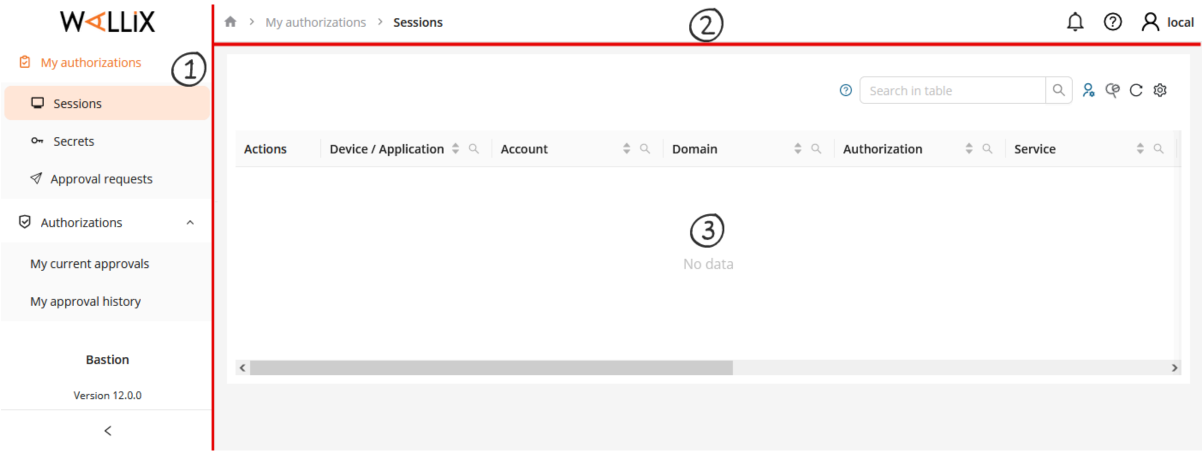
2.4. Authentication with Kerberos

Procedure

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

3. Navigating the WALLIX Bastion web interface

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



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

Logging out

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

4. Configuring your account

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

4.1. Update my e-mail

Procedure

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

4.2. Update my password

Before you begin

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

Procedure

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

Results

Your password is updated if it respects the required criteria.

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

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

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

4.3. Update my preferred language

About this task

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

Procedure

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

4.4. Define my SSH key

Note:

Depending on the configuration set by the administrator, you may not have or be allowed to change the **SSH public key**.

Procedure

1. From any page of the WALLIX Bastion web interface, click your name, and click **My preferences**.
2. On the **SSH key** page, drop or upload a public key.

   You must use the RSA, ED25519, or ECDSA algorithm.

   This key must be in the OpenSSH format. If not, an error message is displayed.
3. Click **Apply**.

4.5. Define a GPG key

The GPG key can only be used by WALLIX Bastion administrators.

4.6. Define my SSH or RDP default client

About this task

When you define a default client, you ensure that the files you download for sessions are directly in your preferred client format. However, this does not preclude the use of clients other than your default one.

Procedure

1. From any page of the WALLIX Bastion web interface, click your name, and click **My preferences**.
2. On the **My authorizations** tab, configure your preferred client:
   - **Default RDP client**: select **rdp**, **rdesktop**, **xfreerdp**, or **remmina** from the dropdown list.
   - **Default SSH client**: select **wallix-putty**, **ssh**, or **Xshell** from the dropdown list.
3. **Optional:** For the default RDP client, you can also configure the default resolution and default color depth.
4. Click **Apply**.

What to do next

Note:

The **RDP configuration file** button is used to download the RDP configuration files. The file can then be saved to establish a connection to an application in interactive mode via the RDP client selector.

This button is only displayed if you are authorized to connect to at least one application.

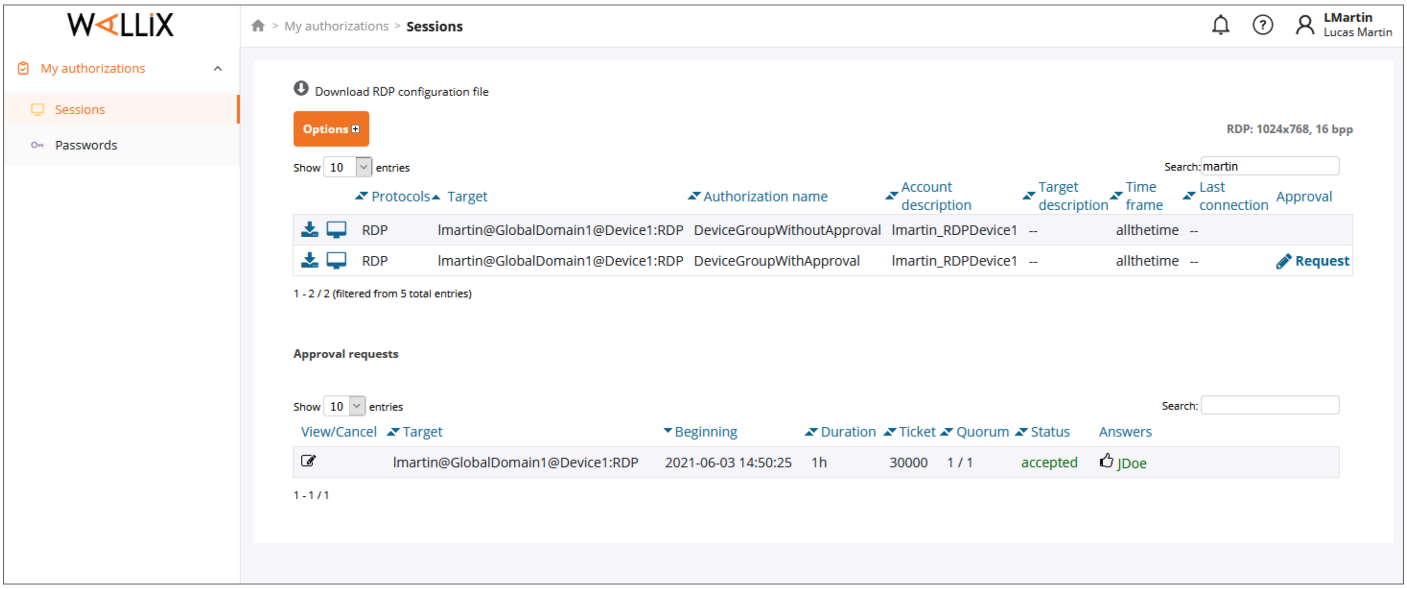
For more information on launching sessions, refer to RDP connections *(on page 18)* and SSH connections *(on page 26)*

5. Accessing target devices

5.1. Authorizations for sessions

The **My authorizations > Sessions** page lists targets you can access using a direct connection.

“My authorizations” menu - “Sessions” page



Download RDP configuration file

RDP: 1024x768, 16 bpp

Show 10 entries

Search: martin

	Protocols	Target	Authorization name	Account description	Target description	Time frame	Last connection	Approval
	RDP	lmartin@GlobalDomain1@Device1:RDP	DeviceGroupWithoutApproval	lmartin_RDPDevice1	--	allthetime	--	
	RDP	lmartin@GlobalDomain1@Device1:RDP	DeviceGroupWithApproval	lmartin_RDPDevice1	--	allthetime	--	Request

1 - 2 / 2 (filtered from 5 total entries)

Approval requests

Show 10 entries

Search:

View/Cancel	Target	Beginning	Duration	Ticket	Quorum	Status	Answers
	lmartin@GlobalDomain1@Device1:RDP	2021-06-03 14:50:25	1h	30000	1 / 1	accepted	JDoe

1 - 1 / 1

However, to connect to target sessions, you must first configure your RDP or SSH preferences. You can access your preferences by clicking the icon. For more information about setting up your preferences, refer to Configuring your account *(on page 11)*.

Session details

For each available target account, different actions can be available:

Instant access with WALLIX-PuTTY/ Download shell script (One-Time password, limited in time)

Download and open the file to immediately establish a connection using an SSH client (file suffix *.puttywab* or *.xsh* under Windows and *.xsh* under Linux).

In this case, no password is required but access is granted for a limited period of time. For SSH authentication, also refer to Target connection in interactive mode for SCP and SFTP protocols *(on page 31)*.

Instant access (One-Time password, limited in time)

Open the file to immediately establish a connection from an RDP client (filename suffix `.rdp` under Windows, and *.sh* or *.remmina* under Linux).

In this case, no password is required but the access is granted for a limited period of time. This icon is also displayed for the connection to an application.

Download RDP configuration file (password required to connect)

Download an RDP configuration file or a shell script with the SSH command (WALLIX-PuTTY on Windows or SSH on other systems) that they can save to establish a connection from an RDP or an SSH client (file suffix *.puttywab* or *.xsh* or `.rdp` under Windows and *.sh* or *.remmina* under Linux). In this case, the WALLIX Bastion password is required for the connection.

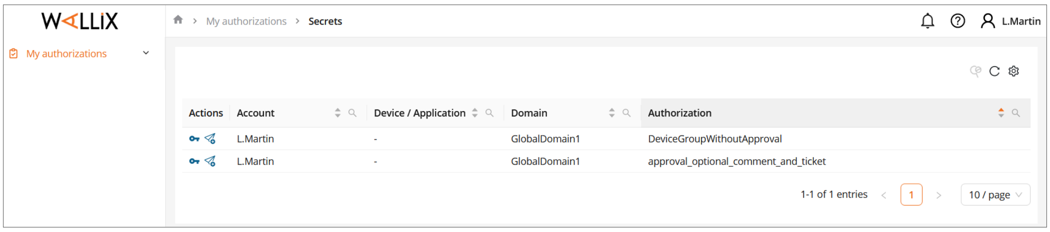
Create an approval request

Create an approval request. If an approval workflow is defined to authorize connection to the target, it is necessary to click this icon to notify the approvers and get access to the target. For more information, refer to Approval workflow *(on page 52)*.

5.2. Authorizations for secrets

The **My authorizations > Secrets** page lists all target accounts for which you are authorized to check out credentials.

“My Authorizations” menu - “Secrets” page



Actions	Account	Device / Application	Domain	Authorization
	L.Martin	-	GlobalDomain1	DeviceGroupWithoutApproval
	L.Martin	-	GlobalDomain1	approval_optional_comment_and_ticket

1-1 of 1 entries 1 10 / page

Secrets details

For each available target account, different actions can be available:

Checkout the target secrets

Check out the account and expand its information. It is then possible to view and copy the account credentials, which can be:

- the login of the account
- the password, if it is defined for the account on the local or remote instance of WALLIX Bastion
- the SSH private key, if it is defined for the account on the local or remote instance of WALLIX Bastion. This key can be downloaded in the OpenSSH, PEM/PKCS#8, PEM/PKCS#1, or PuTTY format. This key can also be encrypted with a passphrase entered in the dedicated field before being downloaded or copied. It is important to memorize this passphrase, as it must be entered each time the key is used.
- the certificate (that is, the signed SSH public key) if the account is defined on a domain associated with a Certificate Authority. This certificate can be downloaded in the OpenSSH or ssh.com format.

Create an approval request

If an approval workflow is defined to authorize connection to the target, it is necessary to click this icon to notify the approvers and get access to the secrets of the target.

For more information, refer to Approval workflow *(on page 52)*.

Important:

When a password change is in progress for a target account, it is not possible to check out and display the credentials of that target account. An error message explains that the account is temporarily unavailable for checkout.

When the lock is enabled in the checkout policy associated with this account, the account remains locked for the duration defined in this policy. The account is automatically checked in at the end of this duration. The time remaining before the check in is displayed to the right of the credentials.

The **Check out remotely** option is performed as standard checkout.

Checkout secret

When checkout a secret, more actions are available:

Copy

Copy the login or password of the target device in your clipboard.

View and Hide

Show or mask the login and password of the target device.

Extend checkout

Extend the checkout of the account's credentials.

This option is only if an administrator allowed a checkout extension in the checkout policy associated with the account. It is possible to extend the checkout duration several times, as long as the maximum duration defined by the administrator is not reached.

End checkout

Check in the account when you are done.

If the lock is enabled in the checkout policy associated with this account, this action also unlocks the account. No action can be performed until the release of the lock.

6. Connecting to and from target devices

General information

SSH, RDP, VNC, TELNET, and RLOGIN connections can be established between WALLIX Bastion and the target devices (trusted zone). However, only encrypted SSH and RDP connections are allowed between workstations and WALLIX Bastion (hostile zone).

You can use your usual tools with WALLIX Bastion such as SSH clients in text or graphic mode or RDP clients on Unix, Windows, or Mac OS X platforms. However, the command line and graphic client settings can differ to accommodate for the indirection created by WALLIX Bastion.

Target logon modes

There are two ways to log on the target:

- Auto logon mode: you automatically log on to the target account without needing to know the password.
- Manual logon mode: you manually log on to the target account and need to know the password.

Session recording

WALLIX Bastion can record user sessions (except X11 and Universal Tunneling sessions) as stated in the SSH connection and in the RDP logon prompt. Authorized WALLIX Bastion administrators can enable this feature and view the session recordings at any time. Session recordings include:

- the commands you enter from your workstation (keyboard/mouse)
- the responses from the target device you are logged on to and which are displayed on your screen

6.1. Simplified authentication in X.509 mode

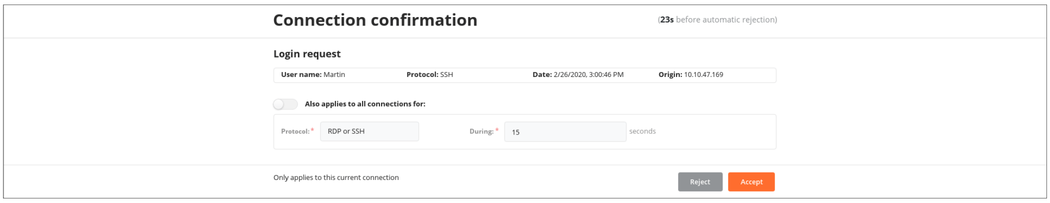
WALLIX Bastion can provide X.509 certificate authentication using the web interface, as described in Authentication with an X.509 certificate *(on page 8)*. If you use this method, a special authentication mechanism applies for sessions launched by clients logging on from the same IP address as you did.

The client waits while the browser displays a message asking whether you authorize the new connection.

If you click **Accept**, the session connection is established immediately without using keys or entering passwords.
If you click **Reject** or if you do not reply in 30 seconds, the connection to WALLIX Bastion for the desired session is closed.

You can save your preference and allow multiple automatic connections through a one-time confirmation for RDP sessions, SSH sessions, or both, for a specified validity period (expressed in seconds).

Connection confirmation window



Connection confirmation

(**23s** before automatic rejection)

Login request

User name: Martin **Protocol:** SSH **Date:** 2/26/2020, 3:00:46 PM **Origin:** 10.10.47.169

○ Also applies to all connections for:

Protocol: * RDP or SSH During: * 15 seconds

Only applies to this current connection

Attention:

For most clients, the web interface shows a message to inform you that WALLIX Bastion is awaiting your authorization. This is not true for SCP or SFTP clients which wait silently as they are not designed to display server messages.

To display this message on the web interface, both the browser and the RDP or SSH client must be operating on the same workstation (with the same IP address).

To return to normal proxy authentication, log out from the web interface.

6.2. RDP connections

Note:

Authorized and unauthorized channels are configured by the administrator.

Connection warning

Before the connection is established with a target, the system can display a series of dialog boxes or ask for a confirmation. This warns you that the session is being recorded or that your password is about to expire, or informs you of the time at which the session will be automatically disconnected.

6.2.1. RDP connections from a Linux workstation

Under Linux, you can use the RDP client rdesktop or equivalent. However, our documentation only describes the use of rdesktop.

Note:

The following is a list of some options for rdesktop:

- `-u` to enter the login
- `-g 1024x768` to select the screen resolution (you can replace 1024x768 with the desired resolution).
- `-a 24` to select the color depth (bits per pixel). The values supported are 8, 15, 16 and 24
- `-0` to connect to the remote workstation console

6.2.1.1. Start session from RDP client

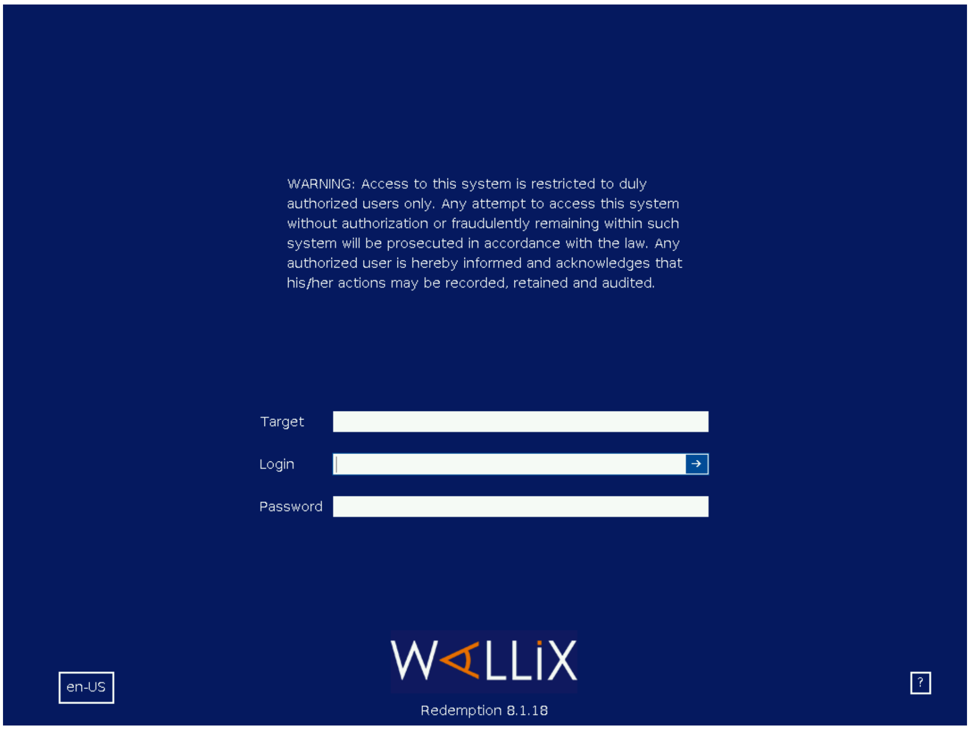
Procedure

1. Enter the following command in your local terminal, replacing `<BASTION>` with the IP address or name of your WALLIX Bastion.

   ```
   $ <RDP_CLIENT> <BASTION>
   ```

   ```
   rdesktop wab.mycorp.lan
   ```

   This opens the WALLIX Bastion login window.

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

   Target

   Login

   Password

2. Enter the information of a target declared on the Bastion. You must be authorized to access this target.

   The target must follow the `<USER>@<DEVICE>:<SERVICE>` format. For example, `Admin@WindowsServer:RemoteDesktop`. The input is case-sensitive.

   > **Tip:**
   >
   > If only one RDP or VNC service is declared on the target device, you can omit the service name. For example, enter `Admin@WindowsServer`.

3. Enter your login and password.

   The password is case-sensitive.

4. Click next or hit `Enter`.
5. **Optional:** If the access to the target is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

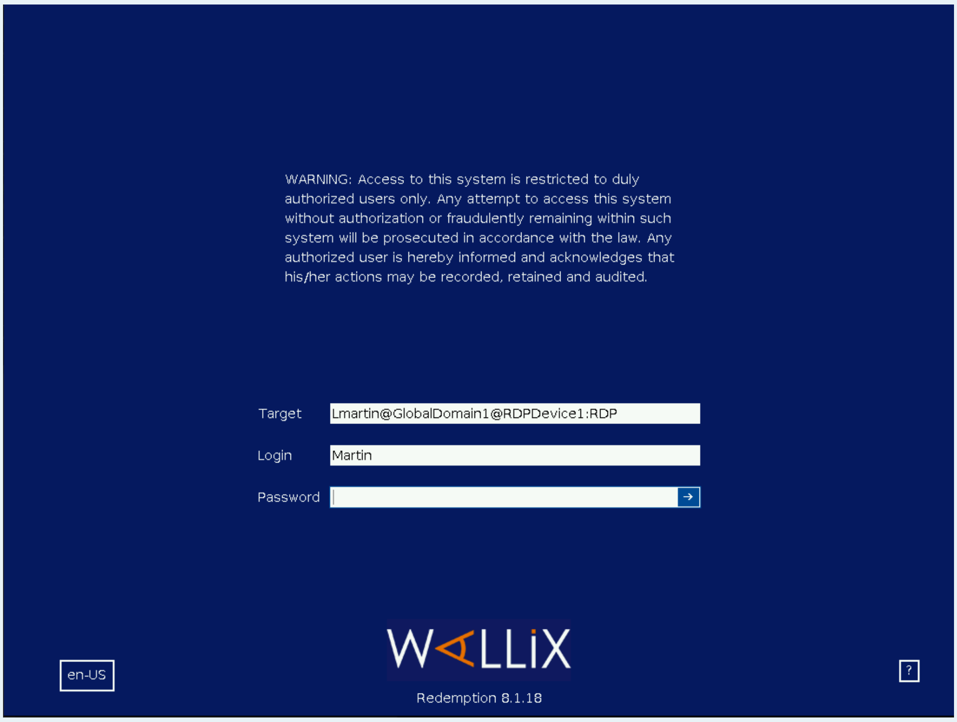
You are connected to the target.

Tip:

You can also pre-define the target information and login with the following command:

```
rdesktop -u Admin@WindowsServer:RemoteDesktop:User wab.mycorp.lan
```

It opens the login window where you must enter the password before establishing the desired target connection.



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

Target: Lmartin@GlobalDomain1@RDPDevice1:RDP

Login: Martin

Password:

6.2.1.2. Start session from RDP client without target name

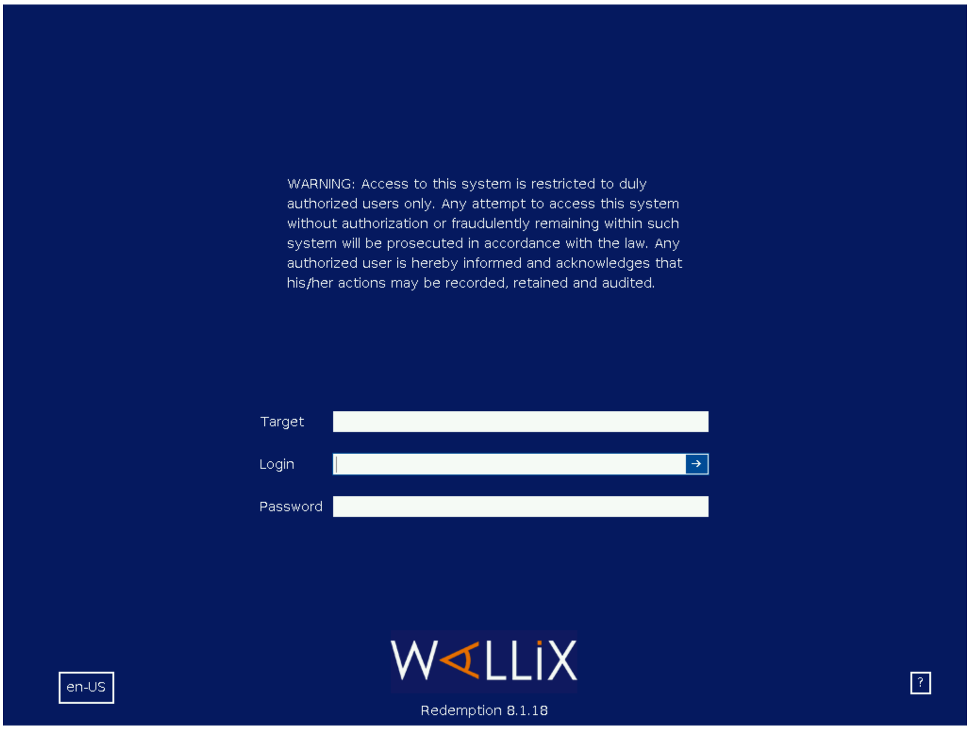
Procedure

1. Enter the following command in your local terminal, replacing `<BASTION>` with the IP address or name of your WALLIX Bastion.

```
$ <RDP_CLIENT> <BASTION>
```

```
$ rdesktop wab.mycorp.lan
```

This opens the WALLIX Bastion login window.



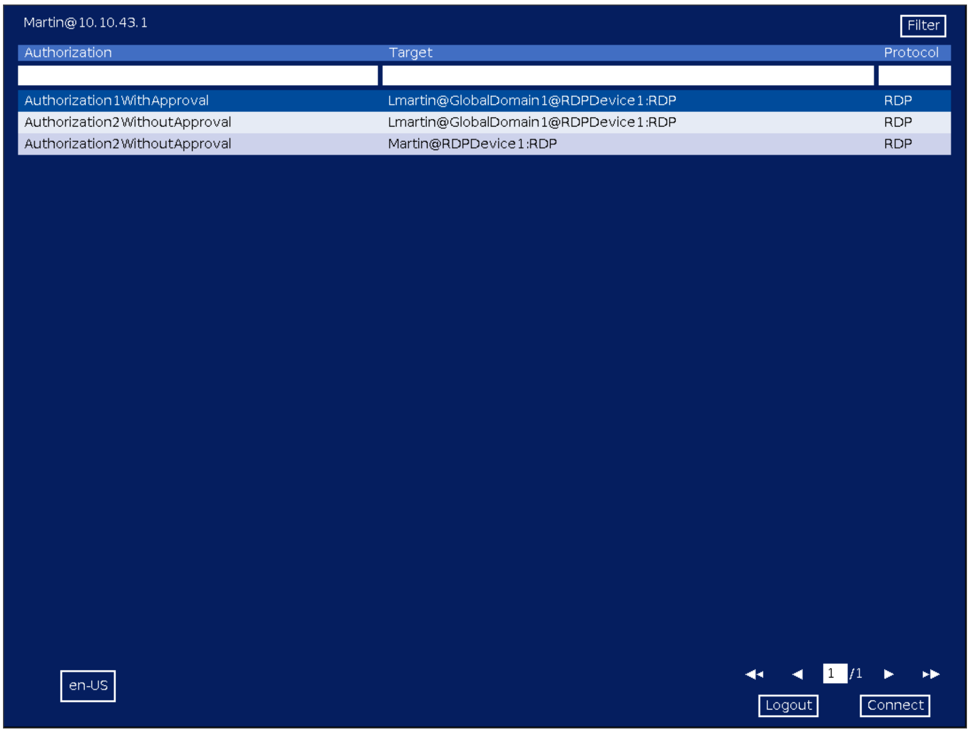
WARNING: Access to this system is restricted to duly authorized users only. Any attempt to access this system without authorization or fraudulently remaining within such system will be prosecuted in accordance with the law. Any authorized user is hereby informed and acknowledges that his/her actions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

2. Enter your login and password.

   The password is case-sensitive.

3. Click next or hit `Enter`.

   The Windows remote session appears with the list of all targets you are authorized to access.



Martin@10.10.43.1

Authorization	Target	Protocol
Authorization1WithApproval	Lmartin@GlobalDomain1@RDPDevice1:RDP	RDP
Authorization2WithoutApproval	Lmartin@GlobalDomain1@RDPDevice1:RDP	RDP
Authorization2WithoutApproval	Martin@RDPDevice1:RDP	RDP

If an accessible server belongs to different groups, several entries for the same remote resource appear in the list. You can apply a filter by group, account, or protocol when the list is long, to narrow down your search. You can also resize columns to display truncated text.

4. Select the desired server by highlighting the corresponding line.
5. Click **Connect**.
6. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

6.2.2. RDP connections from a Windows workstation

You can start an RDP session from a Windows workstation either from the web interface or directly from the Terminal Server client (“Remote Desktop Connection”).

6.2.2.1. Start session from the WALLIX Bastion interface

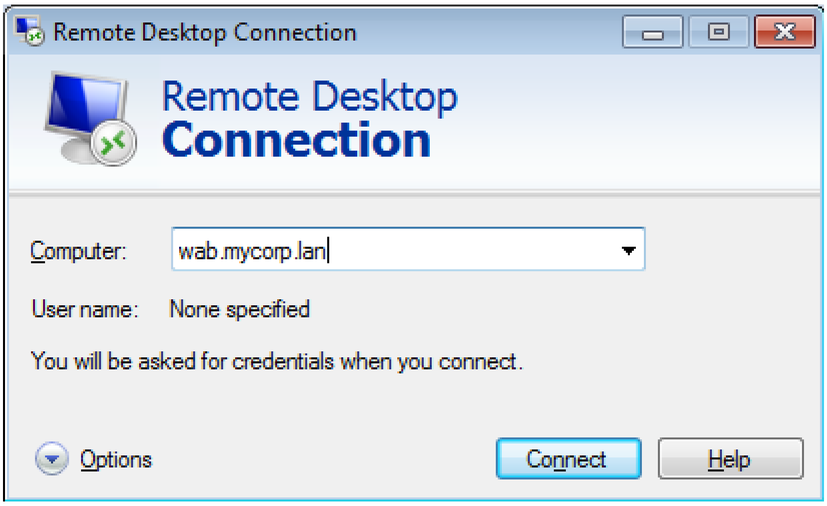
Procedure

1. Go to the **My authorizations > Sessions** page.
2. For the RDP target account you want to access, choose your preferred method:
   - Click 🖥 **Instant access** to directly open or download the file to immediately establish a connection from an RDP client and access the remote machine. In this case, no password is required but the access is granted for a limited period of time.
   - Click ⭳ **Download RDP configuration file** to download a configuration file you can save onto your workstation to establish a connection from an RDP client. In this case, the password is required for the connection.

6.2.2.2. Start session from the Terminal Server client

Procedure

1. Open your Terminal Server client. For example, open Remote Desktop Connection (MSTSC).
2. Enter the Bastion IP address or name in **Computer** and click **Connect**.

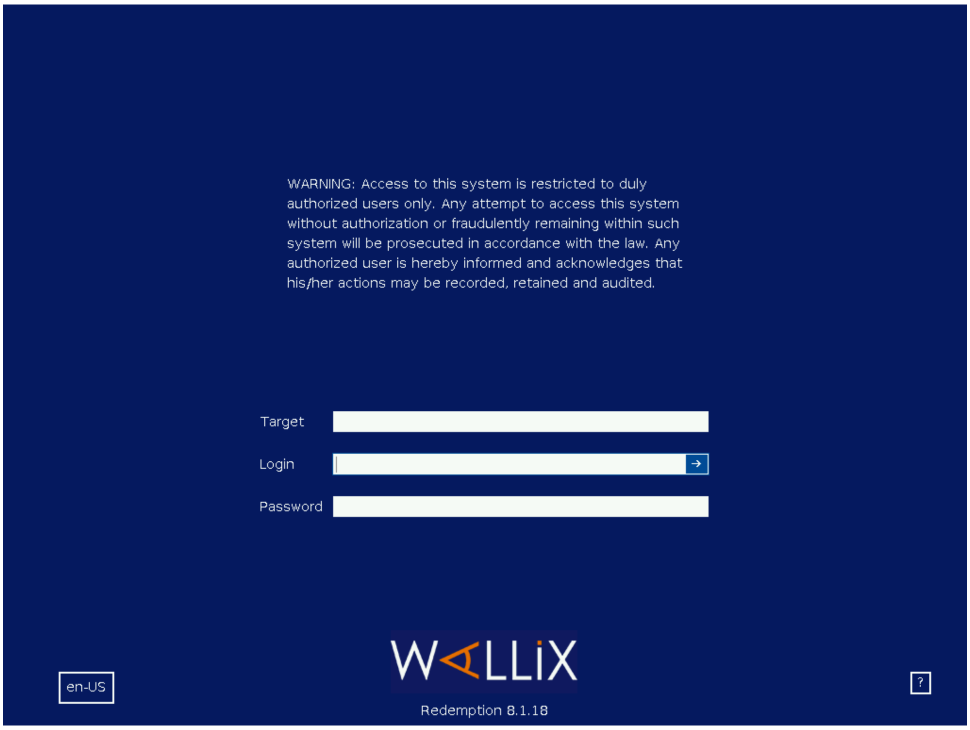


Computer: wab.mycorp.lan

User name: None specified

You will be asked for credentials when you connect.

This opens the WALLIX Bastion login window.



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

Target

Login

Password

3. Enter the information of a target declared on the Bastion. You must be authorized to access this target.

   The target must follow the `<USER>@<DEVICE>:<SERVICE>` format. For example, `Admin@WindowsServer:RemoteDesktop`. The input is case-sensitive.

   > **Tip:**
   >
   > If only one RDP or VNC service is declared on the target device, you can omit the service name. For example, enter `Admin@WindowsServer`.

4. Enter your login and password.

   The password is case-sensitive.

5. Click next or hit `Enter`.
6. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

What to do next

Note:

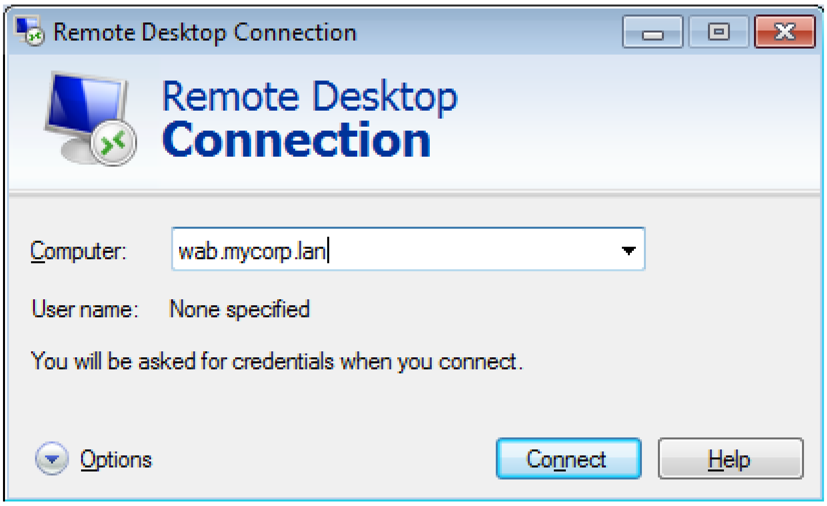
The RDP proxy embedded in WALLIX Bastion allows device redirection. That is the option of displaying the local workstation’s resources: printer, directory, notepad, etc., on the Workstation of the remote session. This feature allows you to transfer files between two Windows machines using the drag-and-drop method, even within the RDP session, or to copy and paste text from the local machine to the remote machine and vice versa.

You may need to enable the feature from the “Terminal Server Client” interface.

6.2.2.3. Start session from the Terminal Server client without target name

Procedure

1. Open the Terminal Server client.
2. Enter the Bastion IP or name in **Computer** and click **Connect**.

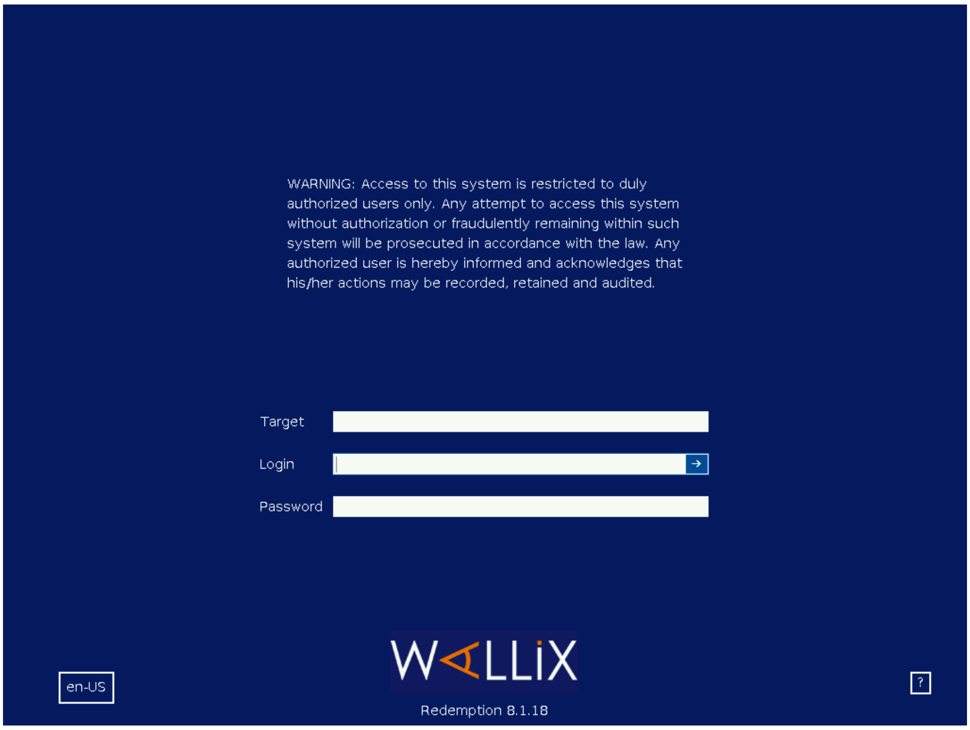


Computer: wab.mycorp.lan

User name: None specified

You will be asked for credentials when you connect.

This opens the WALLIX Bastion login window.



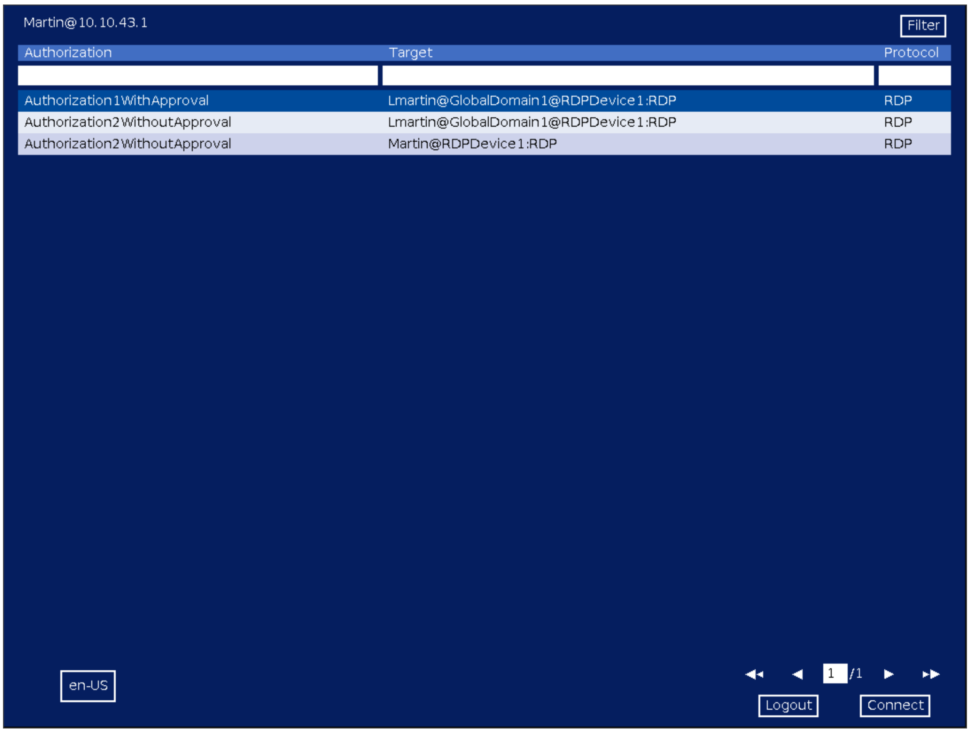
WARNING: Access to this system is restricted to duly authorized users only. Any attempt to access this system without authorization or fraudulently remaining within such system will be prosecuted in accordance with the law. Any authorized user is hereby informed and acknowledges that his/her actions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

3. Enter your login and password.

   The password is case-sensitive.

4. Click next or hit `Enter`.

   The Windows remote session appears with the list of all targets you are authorized to access.



Martin@10.10.43.1

Authorization	Target	Protocol
Authorization1WithApproval	Lmartin@GlobalDomain1@RDPDevice1:RDP	RDP
Authorization2WithoutApproval	Lmartin@GlobalDomain1@RDPDevice1:RDP	RDP
Authorization2WithoutApproval	Martin@RDPDevice1:RDP	RDP

If an accessible server belongs to different groups, several entries for the same remote resource appear on the list. You can apply a filter by group, account, or protocol to a long list to narrow down your search. You can also resize columns to display truncated text.

5. Select the desired server by highlighting the corresponding line.
6. Click **Connect**.
7. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

6.2.2.4. Start session using a smart card

About this task

WALLIX Bastion offers the possibility to authenticate to Windows targets via the RDP protocol using a smart card and the associated PIN code.

> **Important:**
>
> The smart card authentication is only possible for the connection to targets through the interactive login mechanism.

Procedure

1. Insert the smart card in the reader.
2. Connect through WALLIX Bastion to the RDP resource configured for the smart card authentication.
3. Select the `Smart card` option in the `Sign-in options` field displayed on the Windows login screen. Windows can take up to 30 seconds to display this field.
   The user's login automatically appears on the screen.
4. Enter the smart card PIN code.

6.3. SSH connections

> **Note:**
>
> Authorized and unauthorized channels are configured by the administrator.

6.3.1. SSH password or key authentication

WALLIX Bastion allows to perform a local SSH authentication using either a password or a key. The SSH public key must be provided either by your administrator or by yourself (refer to Define my SSH key *(on page 12)*).

WALLIX Bastion does not require a password for an SSH connection for key authentication. However, unless the WALLIX Bastion administrator provided a Kerberos authentication method or an X509 certificate, users must always enter their password to log on to the web interface of WALLIX Bastion and connect to target devices through RDP sessions.

The use of SSH key authentication also means that a resident agent can be used on the client workstation. As a result, the authentication parameters can be used so that users are only asked to enter their key protection password one time: when the agent starts or the first time the key is used.

The key can then be reused without having to re-enter the password each time. The agent's use is transparent with all supported clients. The authentication agent can optionally also be used to transfer the client's authentication parameters to WALLIX Bastion so that it can use them for authentication when logging on to target devices. This functionality allows WALLIX Bastion to use the client's private keys without users needing to re-enter passwords or WALLIX Bastion needing to know the private keys concerned. For this, you must usually explicitly enable the option when the clients are started, as they generally do not enable it for security reasons.

Note:

Some clients that support agent use may not support the authentication transfer option.

Format	PEM/PKCS#1	PEM/PKCS#8	OpenSSH (default value)	PuTTY
RSA	X	X	X	X
ED25519			X	X
ECDSA	X	X	X	X

6.3.1.1. Generate an encryption key with OpenSSH (Linux)

About this task

It is recommended to this key in the `.ssh` directory of your HOME directory.

Tip:

You can use the `~/.ssh/id_rsa` file, which is the default identity used by all OpenSSH commands. In this case, if the file already exists you can skip the first two steps in this section and import the file `~/.ssh/id_rsa.pub` into WALLIX Bastion (refer to Define my SSH key *(on page 12)*).

Procedure

1. Run the following terminal command to generate the public/private key pair.

   ```
   $ ssh-keygen -t rsa -f ~/.ssh/<KEY_NAME>
   Generating public/private rsa key pair.
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /home/<PATH>/.ssh/<KEY_NAME>.
   Your public key has been saved in /home/<PATH>/.ssh/<KEY_NAME>.pub.
   ```

   You can also use the parameter **-b SIZE** to change the key's size. By default, an RSA key in the current version of ssh-keygen is 2048 bits, which is a reasonable size. However, prefer a 4096-bit key if keys must be used later than 2030.

2. Import the file `~/.ssh/<KEY_NAME>.pub` into WALLIX Bastion.

   To do this, refer to Define my SSH key *(on page 12)*.

3. Proceed with the method that applies to your situation:

Authentication agent	

If you do not use an authentication agent	The `ssh`, `scp`, and `sftp` commands use the default identity key `~/.ssh/id_rsa` or the private key passed as an argument using the parameter `-i KEY`.
	For example:
	`$ ssh -t -i ~/.ssh/<KEY_NAME> -l root@machine:<USER>`
	` wab.mycorp.lan`
	`Enter passphrase for key '/home/<PATH>/.ssh/<KEY_NAME>':`

If you use an authentication agent	Import the private key whenever you restart the agent.
	`$ ssh-add ~/.ssh/<KEY_NAME>`
	`Enter passphrase for /home/<PATH>/.ssh/<KEY_NAME>:`
	`Identity added: /home/<PATH>/.ssh/wab_rsa2048`
	` (/home/<PATH>/.ssh/<KEY_NAME>)`
	You can then log on to the SSH proxy without having to re-enter the password or pass the parameter `-i` on the command line. SSH automatically tries all the identities added in the agent.

Results

You can start your SSH connection. For more information, refer to SSH connections from a Unix/Linux workstation *(on page 30)*.

6.3.1.2. Generate an encryption key with PuTTY (Windows)

About this task

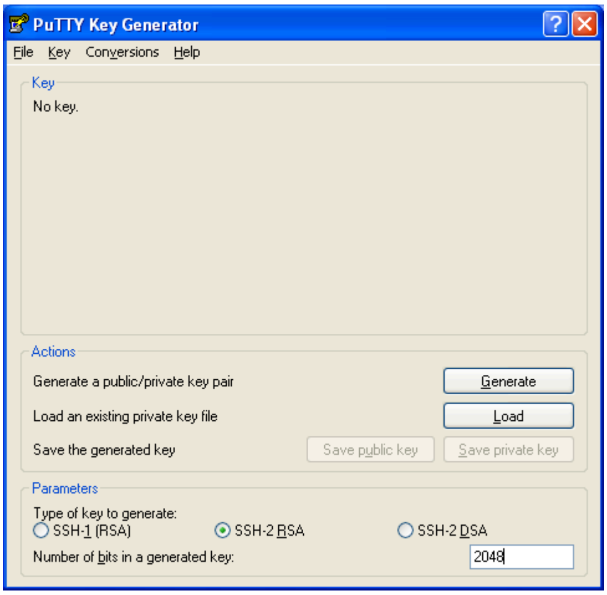
In the following procedure, the private key is named *<KEY_NAME>*, but you can use any other valid file name. Save this key in the `.ssh` directory of your HOME directory.

Procedure

1. Launch PuTTYgen to open the PuTTY Key Generator window.
2. On the **Parameters** frame, change the options as shown in the following screenshot to generate an SSH-2 RSA 2048-bit key.

> **Note:**
>
> If the keys must be used beyond 2030, a 4096-bit key is recommended.

PuTTY Key Generator window



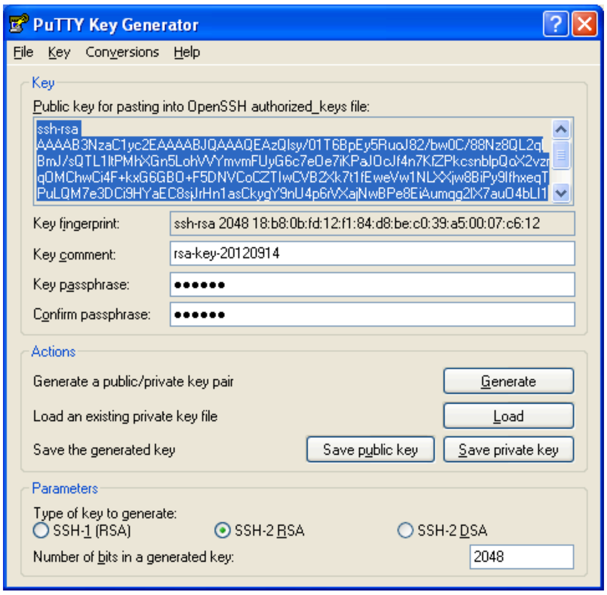
No key.

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

3. Click **Generate** and move the mouse randomly to increase entropy.
4. When PuTTY generates the key, enter the desired password in the **Key passphrase** (key password) field and confirm it in **Confirm passphrase**.
5. Click **Save private key** and save the key in your user directory, for example in `My Documents\<KEY_NAME>.ppk`.
6. Select all the text in the frame under **Public key for pasting into OpenSSH authorized_keys file** (right-click and use the contextual menu or press Ctrl+A), then copy to the clipboard (using the contextual menu or press Ctrl+C).

PuTTYgen Key Generator window with key generated



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAzQIsy/01T6BpEy5RuoJ82/bw0C/88Nz8QL2q
BmJ/sQTL1ltPMhXGn5LohVVYmvmFUyG6c7e0e7iKPaJ0cJf4n7KfZPkcsnblpQoX2vz
qOMChwCi4F+kxG6GBO+F5DNVCoCZTIwCVB2Xk7t1fEweVw1NLXXjw8BiPy9IfhxeqT
PuLQM7e3DCi9HYaEC8sjJrHn1asCkygY9nU4p6rVXajNwBPe8EiAumqg2lX7au04bLl1
```

Key fingerprint: ssh-rsa 2048 18:b8:0b:fd:12:f1:84:d8:be:c0:39:a5:00:07:c6:12

Key comment: rsa-key-20120914

Key passphrase: ●●●●●●●

Confirm passphrase: ●●●●●●●

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

7. Open Notepad to create a new text document. Paste the text in the document, using either the contextual menu or press Ctrl+V. Lastly, save this document containing the public key, for example in `My Documents\<KEY_NAME>.pub.txt`.
8. Close the PuTTY Key Generator window and Notepad.
9. Import this public key file into WALLIX Bastion. To do this, refer to Define my SSH key *(on page 12)*.
10. Import the private key into your SSH client to use it when you log on using any of the following methods:

Method	Process
Pageant authentication	a. Launch Pageant (if it is not already running) b. Double-click the Pageant icon which appears in the Windows taskbar notification area. c. In the Pageant Key List window that opens, click **Add Key** and browse the directories to select the private key file in `My Documents\<KEY_NAME>.ppk`. d. You can now log on to the SSH proxy using PuTTY, PSCP, PSFTP, FileZilla, or WinSCP (unless WinSCP is configured to prevent Pageant authentication). Alternatively, you can double-click the private key file in the File Explorer to add the key. To do this, the `.ppk` file extension must first be associated with Pageant.
PuTTY without Pageant	a. Launch PuTTY to open the PuTTY Configuration window. b. In the **Category** tree-structure, select **Connection > SSH > Auth**. c. On the “Authentication parameters” frame, click “Browse” and then select the private key file in `My Documents\<KEY_NAME>.ppk`. Remember to save the session configuration settings if you want to reuse them.

PSCP or PSFTP without Pageant	Add the `-i KEY` parameter to the command line, such as:
	`$ pscp -scp -i "C:\Documents and Settings\<PATH>\My`
	` Documents\<KEY_NAME>.ppk"`
	`myfile martin@wab.mycorp.lan:root@machine:/tmp`
	`Passphrase for key "rsa-key-20120914":`

FileZilla without Pageant	a. Launch FileZilla. b. Select the **Edit** menu command, then **Settings** and select the **SFTP** page. c. Click **Add key file** d. Select the private key file, `My Documents\<KEY_NAME>.ppk`
WinSCP without Pageant	a. Launch WinSCP. b. On the **Session** configuration category, click **...** near the **Private key file** field c. Select the file `My Documents\<KEY_NAME>.ppk`.

Results

You can start your SSH connection. For more information, refer to SSH connections from a Windows workstation *(on page 37)*.

Note:

You must launch Pageant if you want to use the SSH agent authentication transfer feature.

6.3.2. SSH connections from a Unix/Linux workstation

This section describes how to use WALLIX Bastion with OpenSSH, the most widely available client suite for Linux and the different versions of Unix. Similar tools can be available for the different variants of Unix, but they generally offer the same features as OpenSSH. In this case, refer to the corresponding manual pages to check the correct syntax to use in your suite.

The examples provided in the sections Start shell or X11 session *(on page 32)* and Start session without target name *(on page 33)* work with password or key authentication, and with or without an authentication agent.

6.3.2.1. Target connection in interactive mode for SCP and SFTP protocols

SCP and SFTP protocols do not allow a secondary interactive mode. It is necessary to add specific options during primary connection (the connection initiated between a user and WALLIX Bastion) to be prompted for target connection information. These are displayed as prompts or dialog boxes, using primary interactive keyboard (keyboard interactive). This system assumes that the client supports the interactive keyboard authentication method (“keyboard interactive”).

? (Question mark)

The question mark `?` is a forbidden character in the user name (or login). However, it can be used as a separator to specify options (on the right) requesting clearly a prompt to enter the login and/or a password to connect to the target.

The question mark `?` without any option requests the target password by default.

P (password)

The `p` option requests the target password.

L (login)

The `l` option requests the target login.

Examples of targets login

Login: `wabuser` - no additional prompt
Login: `wabuser?` - target password is prompted
Login: `wabuser?p` - target password is prompted
Login: `wabuser?l` - target login is prompted
Login: `wabuser?lp` - target login is prompted first then target password is prompted

6.3.2.2. Configure the authentication agent

About this task

If you want to use the authentication agent, you must launch it and add your authentication parameters before you use the logon commands.

> **Note:**
>
> In some graphical environments, an agent containing all of your user identities is already activated when you log on. The following commands are then unnecessary. This is generally the case with Debian or Ubuntu distributions, but not with RedHat distributions. However, this varies depending on your configuration.

Procedure

1. Launch the resident agent in your shell session by entering the following command.

   ```
   eval $(ssh-agent)
   ```

   This adds the agent’s declaration to the shell environment so that the compatible programs can automatically use it.

2. Add one or more identities to this agent by entering the following command and entering the related passphrase.

```
ssh-add <PRIVATE_KEY_PATH>
Enter passphrase for <PRIVATE_KEY_PATH>:
```

`PRIVATE_KEY_PATH` refers to the path of the desired identity's private key, which is generally stored in the `~/.ssh` directory, for example `~/.ssh/id_rsa`.

Results

You can now use one of the logon commands described in the shell sessions *(on page 32)*, Start session without target name *(on page 33)*, Transferring files using SCP *(on page 36)*, and Transferring files using SFTP *(on page 37)* procedures without having to re-enter the password. These will automatically use the agent for key-based authentication whenever it is available and declared in the shell environment.

What to do next

If you use the authentication agent, you can use the authentication transfer option if it is also activated in WALLIX Bastion for the required target account. This is only possible with shell sessions *(on page 32)* or remote command sessions *(on page 34)*, by adding the option `-A`. The SSH command line option `-A` tells WALLIX Bastion you want to start a session using the authentication transfer option. If the option is activated on the target device, the authentication parameters used for connection to WALLIX Bastion are reused to log on to the target. Refer to the dedicated documentation for more information on each session type.

Attention:

The authentication transfer option is incompatible with RSA keys more than 2048 bits long and cannot operate if the agent contains RSA and DSA identities simultaneously.

6.3.2.3. Start shell or X11 session

Procedure

1. Open your terminal and enter the following command depending on your situation.

Method	Command line

Start a basic shell session	`ssh -l <TARGET@MACHINE:SERVICE:USER> <BASTION>`
	Depending on how the administrator configured the account, machine and service, you can be asked to authenticate as `<TARGET@MACHINE:SERVICE>`
	If you use the authentication agent *(on page 31)*, you can use the authentication transfer option if it is activated in WALLIX Bastion for the required target account. To do so, add the `-A` argument to the command such as:
	`ssh -A -l <TARGET@MACHINE:SERVICE:USER> <BASTION>`

Start a basic shell session (deprecated)	`ssh -t <USER@BASTION> <TARGET@MACHINE:SERVICE>` The `-t` option allocates the pseudo terminal needed to display the session.

Method	Command line
	Additionally, if only one SSH, TELNET, or RLOGIN service is declared on the target machine, you can omit the service such as: `ssh -t <USER@BASTION> <TARGET@MACHINE>`
Start X11 session	`ssh -X -l <TARGET@MACHINE:SERVICE:USER> <BASTION>`

Start X11 session (deprecated)	`ssh -t -X <USER@BASTION> <TARGET@MACHINE:SERVICE>`
	The `-X` option tells WALLIX Bastion you want to start an **X11 Forwarding** session. The graphical applications run on the target device during the session are displayed on the workstation.
	Additionally, if only one SSH service is declared on the target machine, you can omit the service such as:
	`ssh -t -X <USER@BASTION> <TARGET@MACHINE>`

Replace the placeholders with the values that apply to your situation:

- `USER` refers to your login. It is not case-sensitive. You must be authorized to use `SSH_SHELL_SESSION` or `SSH_X11` (depending on the chosen method).
- `BASTION` refers to the name or IP address of your WALLIX Bastion.
- `TARGET` refers to the target account you want to access. It is case-sensitive.
- `MACHINE` refers to the name of the machine. It is case-sensitive.
- `SERVICE` refers to the name of the service. It is case-sensitive.

Example of a basic shell session prompt

```
ssh -l Admin@WindowsServer:OpenSSH:john wab.acme.lan
```

2. Enter your password.

   The input is case-sensitive.

3. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

6.3.2.4. Start session without target name

About this task

WALLIX Bastion allows you to list the devices to which you can access. This is done by unspecifying the target in the logon command. However, this is only possible with interactive sessions (shell or X11).

Procedure

1. Enter the following command in your local terminal, replacing `<USER>` with your login and `<BASTION>` with the IP address or name of your WALLIX Bastion.

```
ssh -t <USER>@<BASTION>
```

2. Enter your password.

The input is case-sensitive.

The list of all available targets is displayed.

3. Select the desired target by entering the corresponding number in the **ID** column.
4. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

Workflow example for a restricted target with an approved request

```
$ ssh -t jdoe@wab.mycorp.lan
jdoe's password:
| ID | Site (page 1/1)       | Authorization
|----|-----------------------|-------------------
|  0 | root@centos:ssh_2222 | auth_domain_1
|  1 | root@asterix:OpenSSH |
Enter h for help, ctrl-D to quit
> 0
Selected target: root@centos:ssh_2222
You need to ask for approval to access the target.

= Approval request =
Duration ([hours]h[mins]m): 1h
Ticket (optional): POM-780
Description (optional): Access for POM project

Your approval request is pending acceptance.

Account successfully checked out
```

6.3.2.5. Start remote command on targets session

Procedure

1. Open your terminal and enter the following command depending on your situation.

Method	Command line

Recommended	`ssh -l <TARGET@MACHINE:SERVICE:USER> <BASTION> halt`
	If you use the authentication agent *(on page 31)*, you can use the authentication transfer option if it is activated in WALLIX Bastion for the required target account. To do so, add the `-A` argument to the command such as:
	`ssh -A -l <TARGET@MACHINE:SERVICE:USER> <BASTION> halt`

Deprecated	`ssh <USER>@<BASTION> <TARGET@MACHINE:SERVICE> halt`
	Additionally, if only one SSH, TELNET, or RLOGIN service is declared on the target machine, you can omit the service such as:
	`ssh <USER>@<BASTION> <TARGET@MACHINE> halt`

Replace the placeholders with the values that apply to your situation:

    - `USER` refers to your login. It is not case-sensitive. You must be authorized to use `SSH_REMOTE_COMMAND`.
    - `BASTION` refers to the name or IP address of your WALLIX Bastion.
    - `TARGET` refers to the target account you want to access. The “Auto logon” mode must be enabled for the target account. It is case-sensitive.
    - `MACHINE` refers to the name of the machine. It is case-sensitive.
    - `SERVICE` refers to the name of the service. It is case-sensitive.

   Example with the recommended command

   ```
   ssh -l root@asterix:OpenSSH:martin wab.mycorp.lan halt
   ```

2. Enter your password.

   The input is case-sensitive.

Results

The `halt` command is run on the device without the shell being opened.

6.3.2.6. Logging on using SCP with authentication transfer

About this task

OpenSSH SCP client is not directly compatible with the authentication transfer option. However, the SCP client can be used with a wrapper script and a launcher script which pass the correct options to the underlying SSH command.

Procedure

1. In a directory in your PATH, create the launcher script file named `scp-A` containing the following lines:

   ```
   #!/bin/sh
   scp -oForwardAgent=yes -S scp-A-wrapper "$@"
   ```

2. Create the wrapper script file `scp-A-wrapper` in the same directory, containing the following lines:

   ```
   #!/usr/bin/perl
   exec '/usr/bin/ssh', map {($_ =~ /^-oForwardAgent[ =]no$/) || ($_ eq '-a') ? (
     ) : $_} @ARGV;
   ```

3. Make both files executable with the `chmod` command:

   ```
   $ chmod +x scp-A scp-A-wrapper
   ```

Results

You can use the launcher script file `scp-A` in place of the `scp` command.

```
$ scp-A myfile martin@wab.mycorp.lan:root@asterix:/tmp
```

```
$ scp-A martin@wab.mycorp.lan:root@asterix:/tmp/myfile /tmp
```

6.3.2.7. Transferring files using SCP

Procedure

1. Open your terminal and enter the following command depending on your situation.

Method	Command line
Transfer a file from the client to the target	`scp myfile <TARGET>@<DEVICE>+<SERVICE>+<USER>@<BASTION>:/tmp`

Transfer a file from the client to the target (deprecated)	`scp myfile <USER>@<BASTION>:<TARGET>@<DEVICE>:<SERVICE>:/tmp`
	Additionally, if only one SSH service is declared on the target, you can omit the service, such as:
	`scp myfile <USER>@<BASTION>:<TARGET>@<DEVICE>:/tmp`

Transfer a file from the target to the client	`scp <TARGET>@<DEVICE>+<SERVICE>+<USER>@<BASTION>:/tmp/myfile /tmp`

Transfer a file from the target to the client (deprecated)	`scp <USER>@<BASTION>:<TARGET>@<DEVICE>:<SERVICE>:/tmp/myfile /tmp`
	Additionally, if only one SSH service is declared on the target, you can omit the service, such as:
	`scp <USER>@<BASTION>:<TARGET>@<DEVICE>:/tmp/myfile /tmp`

   Replace the placeholders with the values that apply to your situation:

   - `USER`: refers to your login. It is not case-sensitive. You must be authorized to use `SSH_SCP_UP` (to the target) or `SSH_SCP_DOWN` (from the target) depending on your chosen method.
   - `BASTION` refers to the name or IP address of your WALLIX Bastion.
   - `TARGET` refers to the target account you want to access. The **auto logon** mode must be enabled. It is case-sensitive.
   - `DEVICE` refers to the name of the machine. It is case-sensitive.
   - `SERVICE` refers to the name of the service. It is case-sensitive.

   Example of a transfer of a file from the client to the target

```
scp myfile root@asterix+OpenSSH+martin@wab.mycorp.lan:/tmp
```

   Example of a transfer of a file from the target to the client

```
scp root@asterix+OpenSSH+martin@wab.mycorp.lan:/tmp/myfile /tmp
```

2. Enter your password.

   The input is case-sensitive.

6.3.2.8. Transferring files using SFTP

Procedure

1. Enter the following command in your local terminal.

   ```
   sftp <TARGET>@<DEVICE>+<SERVICE>+<USER>@<BASTION>
   ```

   Replace the placeholders with the values that apply to your situation:

   - `USER` refers to your login. It is not case-sensitive. You must be authorized to use `SFTP_SESSION`.
   - `BASTION` refers to the name or IP address of your WALLIX Bastion.
   - `TARGET` refers to the target account you want to access. The **auto logon** mode must be enabled for this account. It is case-sensitive.
   - `DEVICE` refers to the name of the machine. It is case-sensitive.
   - `SERVICE` refers to the name of the service. It is case-sensitive.

   > **Tip:**
   >
   > If only one SSH service is declared on the target device, you can omit the service.
   >
   > ```
   > sftp <TARGET>@<DEVICE>+<USER>@<BASTION>
   > ```

2. Enter your password.

   The input is case-sensitive.

3. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Workflow example

```
$ sftp root@asterix+OpenSSH+martin@wab.mycorp.lan
Connecting to wab.mycorp.lan...
martin's password:
sftp>
```

6.3.3. SSH connections from a Windows workstation

6.3.3.1. Download WALLIX-PuTTY

About this task

To use the `.puttywab` files on Windows, you must download and install the WALLIX-PuTTY application. The installation sets the file association so that the application is started automatically. The installation does not require administrative privileges. However, the installation is only operational for the logged user and not for all users of the workstation.

The download button is only displayed when the workstation is running under Windows and the user is authorized to connect to at least one SSH target.

Procedure

1. On Bastion interface, click your username, and click **My preferences**.
2. On the **My authorizations** tab, go to the **Download Wallix Client** section.
3. Select the **SSH** protocol.
   The following values are set: **client**, **operating system (OS)** and **version**.

4. Click ⤓ **Download WALLIX-PuTTY**.
5. Install the downloaded application.

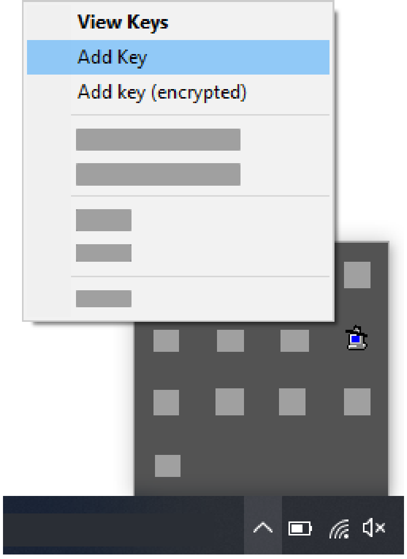
6.3.3.2. Configuring authentication agent

About this task

If you want to use the authentication agent, you must start Pageant and add your authentication parameters before using PuTTY, WinSCP, or FileZilla.

Procedure

1. Start the Pageant authentication agent.
2. Right-click the Pageant icon in the taskbar and click **Add key**.



3. Select the key from your computer.

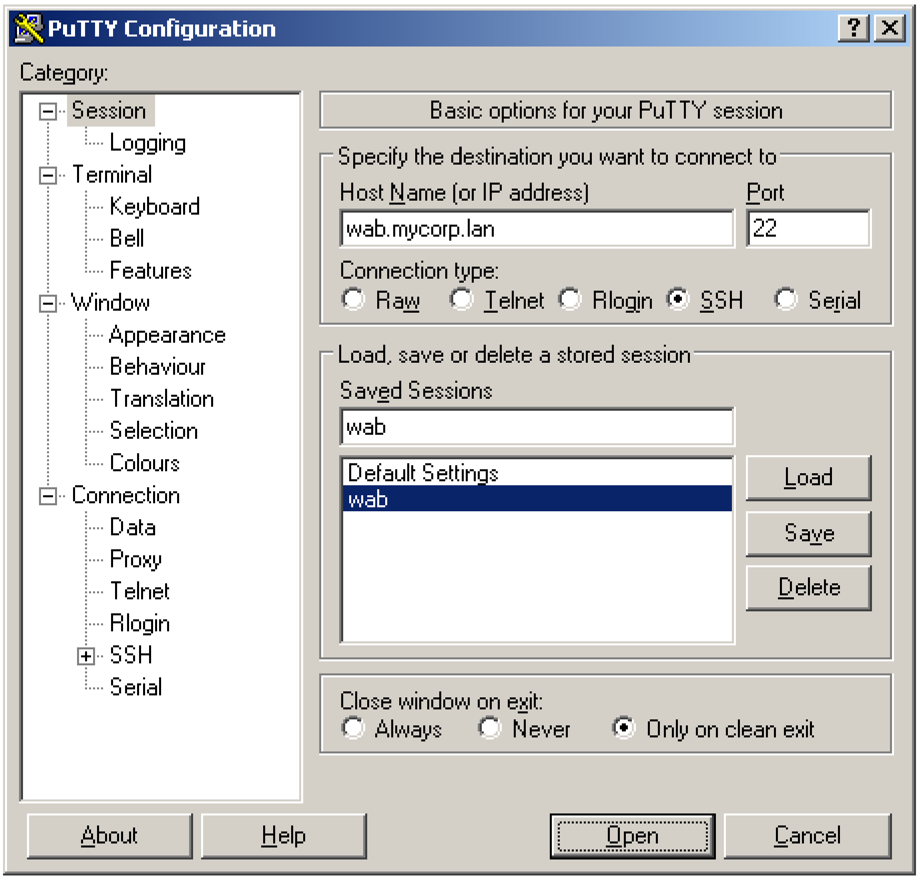
Results

You can use one of the logon commands without having to re-enter the password. These commands automatically use the agent for key-based authentication whenever it is available and declared in the shell environment.

6.3.3.3. Start shell session with PuTTY

Procedure

1. Open WALLIX-PuTTY.
2. Click **Session** and for the **Specify the destination you want to connect to** section, configure the following:
   - In **Host Name**, enter the name or IP address of your WALLIX Bastion.
   - In **Port**, enter `22`. This is the SSH proxy listening port WALLIX Bastion.



Specify the destination you want to connect to

Host Name (or IP address): wab.mycorp.lan

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: wab

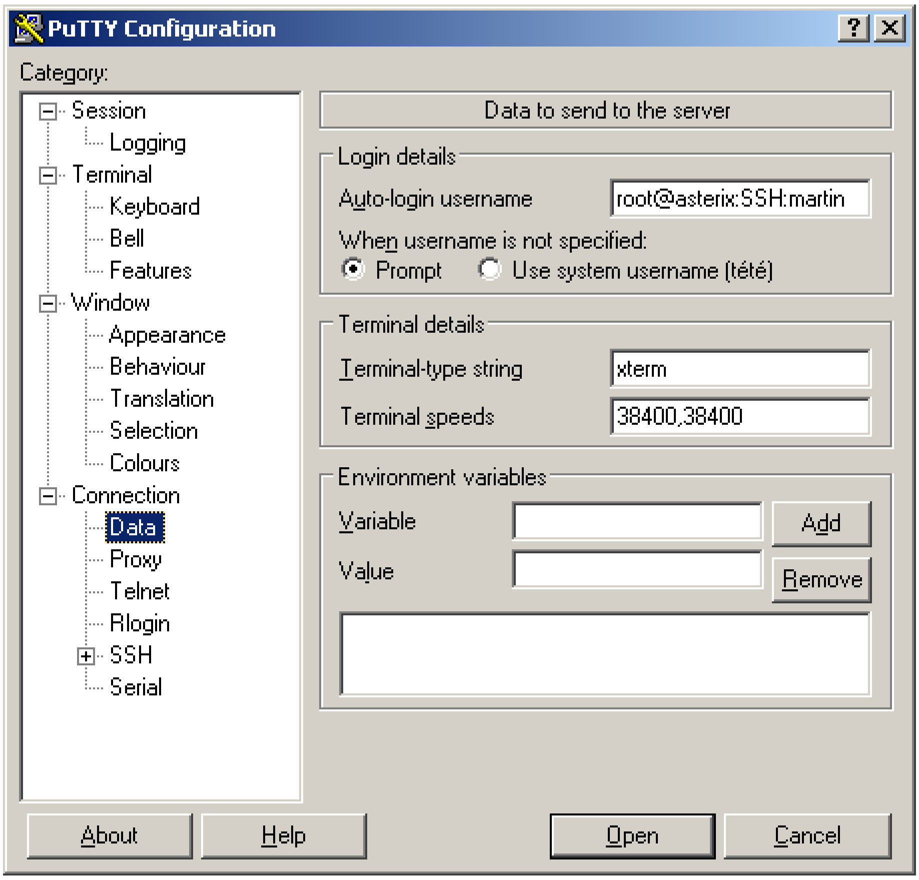
Default Settings
wab

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Click **Connection > Data** and in **Auto-login username**, configure the target access with the following format: `<TARGET@DEVICE:SERVICE:USER>`.
   Replace the placeholders with the values that apply to your situation:
   - `TARGET` refers to the target account you want to access. Case-sensitive.
   - `DEVICE` refers to the name of the machine. Case-sensitive.
   - `SERVICE` refers to the name of the service. Case-sensitive.
   - `USER`: refers to your login. Not case-sensitive.

Note:

PuTTY does not allow you to save your password. If you use this authentication method, you are asked to enter your password when you log on.



Login details

Auto-login username: root@asterix:SSH:martin

When username is not specified:

● Prompt ○ Use system username (tété)

Terminal details

Terminal-type string: xterm

Terminal speeds: 38400,38400

Environment variables

Variable:

Value:

4. **Optional:** If you want to use key-based authentication without using the authentication agent:
    a. Go to **Connection > SSH > Auth**.
    b. Enter the private key file in **Private key file for authentication**.
5. **Optional:** If you want to use the authentication agent:
    a. Follow the Configuring authentication agent *(on page 38)* procedure.
    b. In WALLIX-PuTTY, go to **Connection > SSH > Auth** and ensure that **Attempt authentication using Pageant** is enabled.
6. **Optional:** If you use the authentication agent, and if the target account allows it, you can use the authentication transfer option.

Attention:

The authentication transfer option is incompatible with RSA keys more than 2048 bits long and cannot operate if the agent contains RSA and DSA identities simultaneously.

    a. In WALLIX-PuTTY, go to **Connection > SSH > Auth**.

    b. Enable the **Allow agent forwarding** option to tell WALLIX Bastion that you want to start a session with the authentication transfer option.

    If the option is activated on the target device, the authentication parameters used for connection to WALLIX Bastion are reused to log on to the target.

7. Click **Open**.
8. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

6.3.3.4. Transferring files using PSCP

Procedure

1. Open your terminal and enter the following command:

   ```
   pscp -scp <FILENAME>
    <TARGET_ACCOUNT>@<TARGET_DEVICE>+<SERVICE>+<USER>@<BASTION>:<DIRECTORY>
   ```

   Replace the placeholders with the values that apply to your situation:
   - `<FILENAME>` refers to the name of the file you want to transfer between the local workstation and the directory.
   - `TARGET_ACCOUNT` refers to the name of the target account you want to use. The **auto logon** mode must be enabled for this account. It is case-sensitive.
   - `TARGET_DEVICE` refers to the name of the target device you want to access. It is case-sensitive.
   - `SERVICE` refers to the name of the service for the target. It is case-sensitive.
   - `USER`: refers to your login. It is not case-sensitive.
   - `BASTION` refers to the name or IP address of your WALLIX Bastion.
   - `DIRECTORY` refers to the path for the file transfer.

   ```
   pscp -scp myfile admin@asterix+OpenSSH+john@wab.mycorp.lan:/tmp
   ```

   With this command, the file called “`myfile`” is transferred from the local workstation to the `/tmp` directory using the `admin` account on `asterix`.
2. Enter your password.
3. **Optional:** If the target access is restricted, you must submit a request and wait for its approval before you can connect to the target.

Results

You are connected to the target.

Note:

The following command is deprecated but supported:

```
pscp -scp <FILENAME>
 <USER>@<BASTION>:<TARGET_ACCOUNT>@<TARGET_DEVICE>:<TARGET_SERVICE>:<DIRECTORY>
```

6.3.3.5. Transferring files using FileZilla

Before you begin

You must be authorized to use `SFTP_SESSION`.

Procedure

1. Open Site Manager.

   In FileZilla, click **File > Site Manager**.
2. On the **General** tab, configure the following information:

   a. In **Host**, enter the name or IP address of your WALLIX Bastion.

   b. In **Port**, enter `22` which is the TCP listening port of the SSH proxy.

c. InProtocol, choose **SFTP - SSH File Transfer Protocol** from the dropdown list.

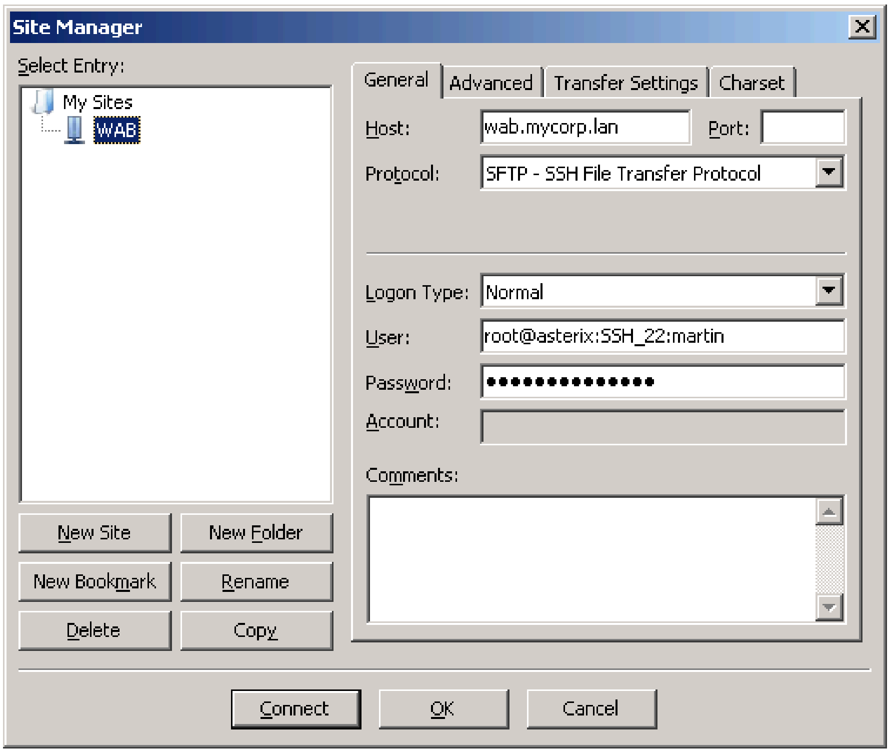
d. In **Logon type**, choose **Normal** from the dropdown list.

e. In **User**, enter the required information with the following format `<TARGET_ACCOUNT><TARGET_DEVICE>:<SERVICE>:<USER>`.
Replace the placeholders with the values that apply to your situation:

- `TARGET_ACCOUNT` refers to the target account you want to access. The **Auto logon** mode must be enabled for this account. It is case-sensitive.
- `TARGET_DEVICE` refers to the name of the machine. It is case-sensitive.
- `SERVICE` refers to the name of the service. It is case-sensitive.
- `USER` refers to your login. It is not case-sensitive.

If only one SSH service is declared on the target machine, you can omit the service name as follows: `root@asterix`.

f. In **Password**, enter your password to log in to WALLIX Bastion.



Host: wab.mycorp.lan Port:

Protocol: SFTP - SSH File Transfer Protocol

Logon Type: Normal

User: root@asterix:SSH_22:martin

Password: ••••••••••••••

Account:

Comments:

6.3.3.6. Transferring files using WinSCP

Before you begin

You must be authorized to use `SFTP_SESSION`.

Procedure

1. Open WinSCP.
2. In **Session**, configure the following information:

a. In **Host Name**, enter the name or IP address of your WALLIX Bastion.

b. In **Port**, enter `22` which is the TCP listening port of the SSH proxy.

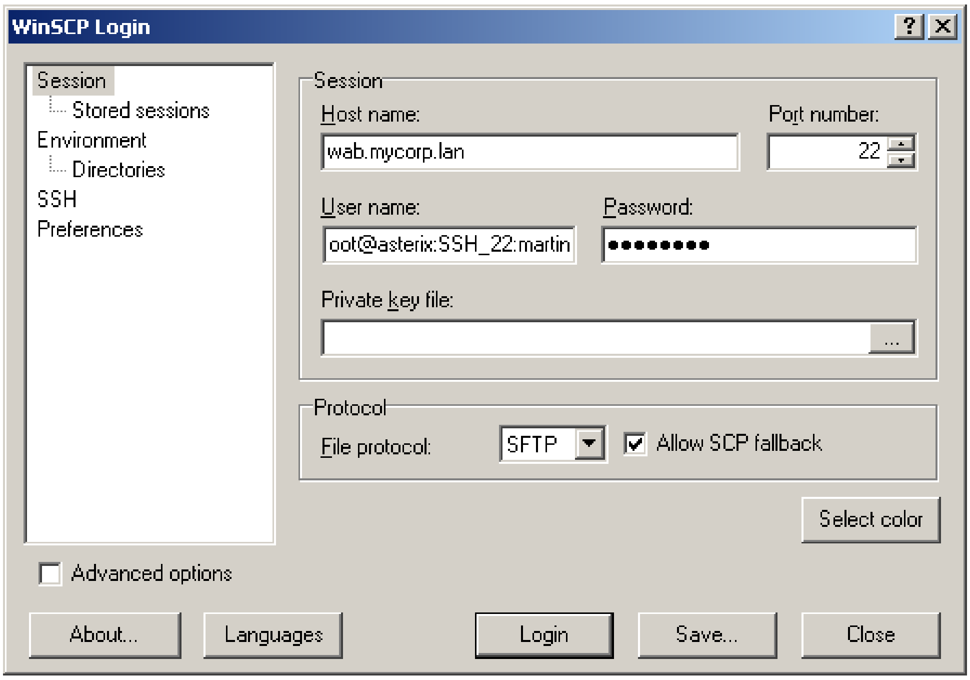
c. <in **User name**, enter the required information with the following format `<TARGET_ACCOUNT><TARGET_DEVICE>:<SERVICE>:<USER>`.
Replace the placeholders with the values that apply to your situation:

- `TARGET_ACCOUNT` refers to the target account you want to access. The **auto logon** mode must be enabled for this account. It is case-sensitive.
- `TARGET_DEVICE` refers to the name of the machine. It is case-sensitive.
- `SERVICE` refers to the name of the service. It is case-sensitive.
- `USER` refers to your login. It is not case-sensitive.

If only one SSH service is declared on the target machine, you can omit the service name as follows: `root@asterix`

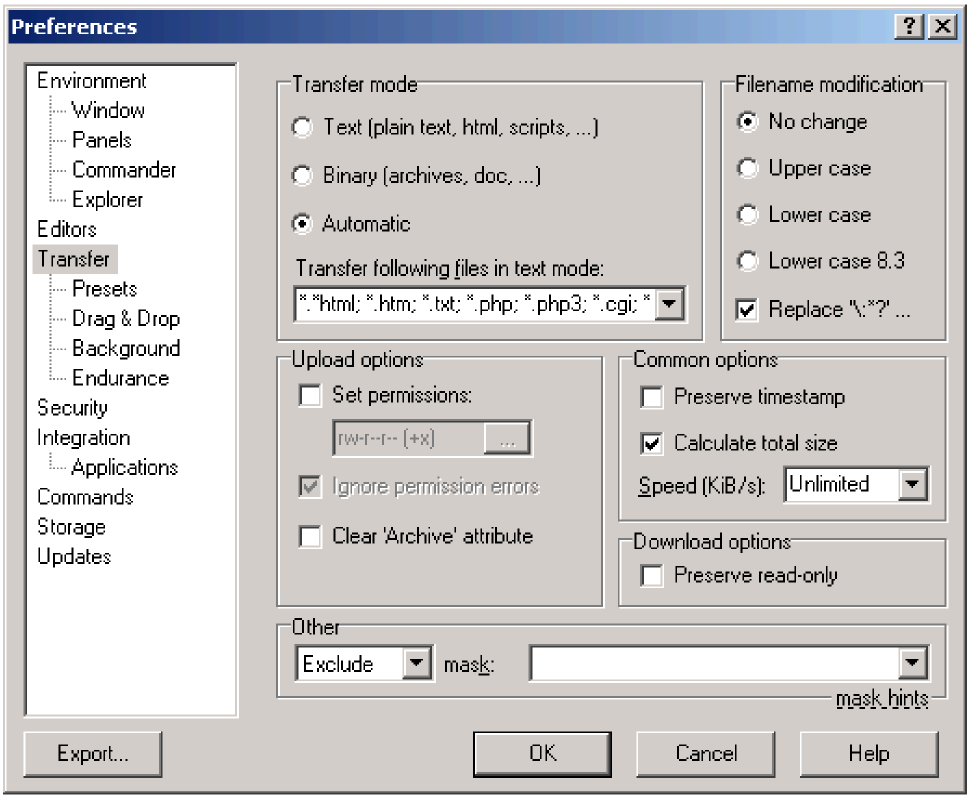
d. In **Password**, enter your password to log in to WALLIX Bastion.

e. In **Protocol**, choose **SFTP** from the dropdown list.



Host name: wab.mycorp.lan
Port number: 22
User name: oot@asterix:SSH_22:martin
Password: ●●●●●●●●●
File protocol: SFTP
☑ Allow SCP fallback
□ Advanced options

3. Click **Preferences > Transfer** enter the following information (in this exact order):
   a. Under the **Upload options** section, enable the **Ignore permission errors** option.
   b. Under the **Common options** section, deselect the **Preserve timestamp** option.



Transfer mode

○ Text (plain text, html, scripts, ...)

○ Binary (archives, doc, ...)

● Automatic

Transfer following files in text mode: *.*html; *.htm; *.txt; *.php; *.php3; *.cgi; *

Filename modification

● No change

○ Upper case

○ Lower case

○ Lower case 8.3

☑ Replace '\:*?' ...

Upload options

□ Set permissions: rw-r--r-- (+x)

☑ Ignore permission errors

□ Clear 'Archive' attribute

Common options

□ Preserve timestamp

☑ Calculate total size

Speed (KiB/s): Unlimited

Download options

□ Preserve read-only

Other

Exclude mask:

4. **Optional:** If you want to use the authentication agent:
   a. Follow the Configuring authentication agent *(on page 38)* procedure.
   b. In WinSCP, go to **Advanced... > SSH > Authentication** and ensure that **Attempt authentication using Pageant** is enabled.

6.4. Universal Tunneling connections

Universal Tunneling (UT), previously called RAW TCP/IP, allows the user to redirect TCP traffic from their workstation to the target.

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)

All application protocols based on TCP for the transport layer in the Open Systems Interconnection model (OSI model) can be managed by Universal Tunneling. An SSH tunnel is used between the user's workstation and WALLIX Bastion to encrypt and protect the data. For each Universal Tunneling session, a PCAP file can be generated to ensure traceability after the session.

Prerequisites

UT sessions are compatible with the user workstations running under:

- Windows XP, Windows 7, Windows 8, Windows 10 for the redirection to the local address mode and the redirection to a temporary interface mode
- any Linux distribution with OpenSSH, only for the redirection to the local address mode

Redirection modes

Two modes are available:

- the redirection to the local address: the fat client must be configured to redirect its traffic on the local address (`127.0.0.1`) and on an access port defined on the user workstation. The traffic will then be redirected through the SSH tunnel. This mode does not require any specific privileges from the user.
- the redirection to a temporary interface: the fat client does not need to be configured as a temporary network interface will be created on the user's workstation using the IP of the target. The traffic sent on this interface will then be redirected through the tunnel. This mode requires specific privileges from the user.

6.4.1. Universal Tunneling connections from a Windows workstation (GUI)

Before you begin

The WALLIX-PuTTY application must be downloaded and installed. For more information, refer to Download WALLIX-PuTTY *(on page 37)*.

About this task

Important:

Logging on using the configuration file only allows the redirection to a temporary interface.

Procedure

1. Go to **Sessions > My authorizations**.
2. Click the download icon (>_) for the relevant target.

Results

This downloads a configuration file to save onto your workstation to establish a connection from the WALLIX-PuTTY client.

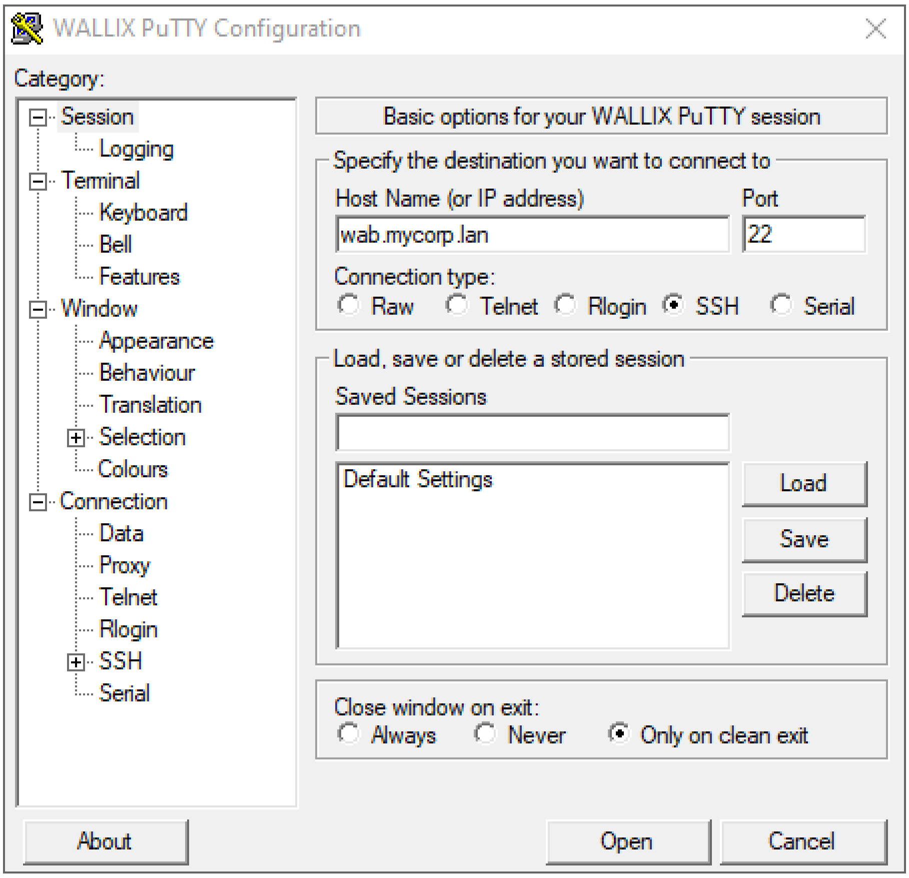
6.4.2. Universal Tunneling connections from a Windows workstation (WALLIX-PuTTY)

Before you begin

The WALLIX-PuTTY application must be downloaded and installed. For more information, refer to Download WALLIX-PuTTY *(on page 37)*.

Procedure

1. Launch WALLIX-PuTTY to open the configuration window.
2. In the **Session** category:
    a. in the **Host Name (or IP address)** field, enter the IP of the Bastion
    b. in the **Port** field (the SSH proxy listening port for WALLIX Bastion), enter `22`.



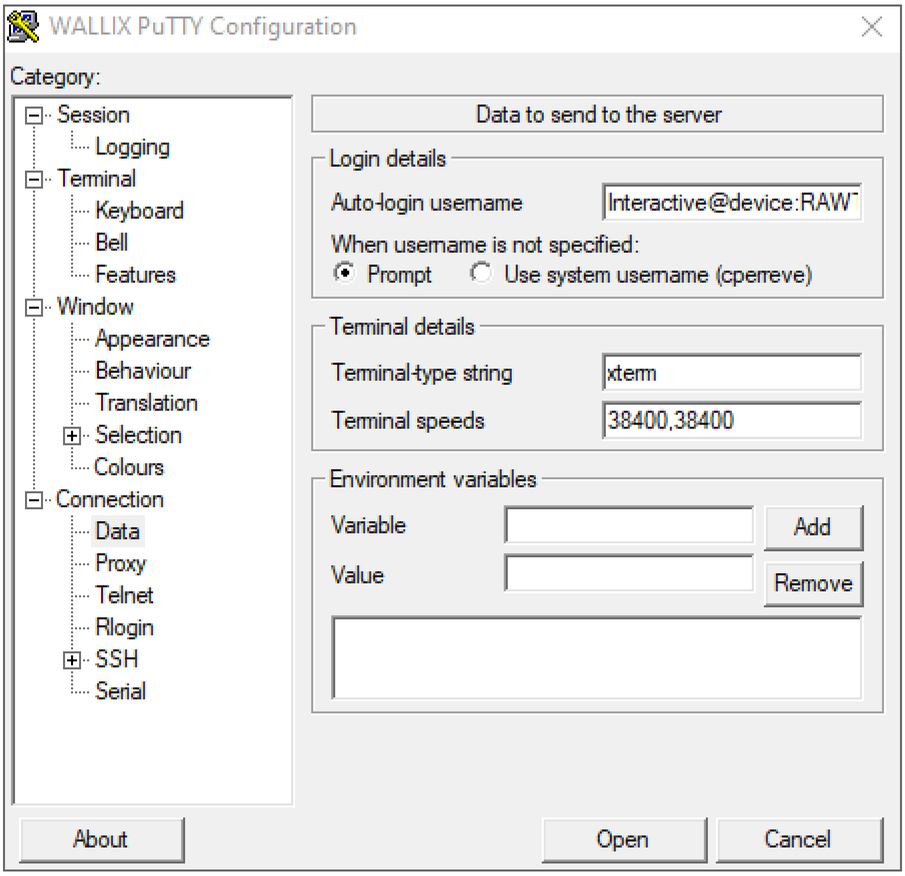
Host Name (or IP address): wab.mycorp.lan

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. In **Connection > Data**, in the **Auto-login username** field, enter `Interactive@<DEVICE>:<SERVICE>:<AUTHORIZATION>:<USER>`.



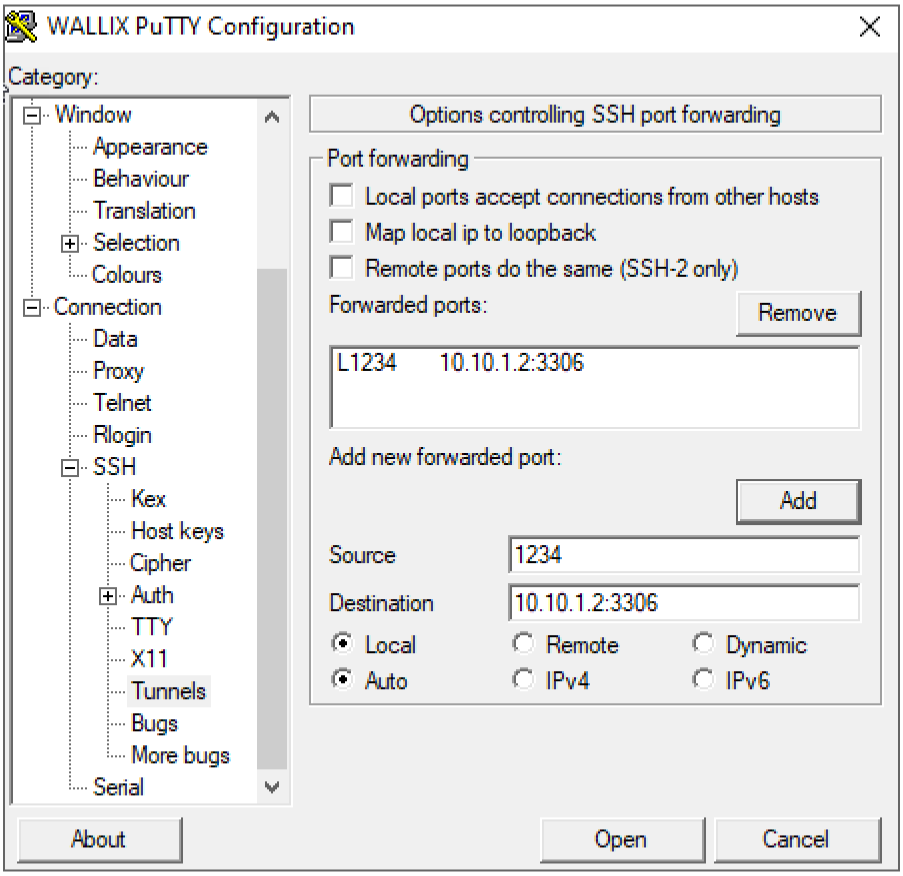
Auto-login username: Interactive@device:RAW

When username is not specified:
● Prompt ○ Use system username (cperreve)

Terminal-type string: xterm

Terminal speeds: 38400,38400

4. In **Connection > SSH > Tunnels**, for the redirection to the local address:
   a. Enable **Map local ip to loopback**.
   b. In the **Source** field, enter the local port.
   c. In the **Destination** field, enter `<TARGET_IP>:<PORT>`.
   d. Click **Add**.
   e. Select **Local** and **Auto**.



Port forwarding

□ Local ports accept connections from other hosts
□ Map local ip to loopback
□ Remote ports do the same (SSH-2 only)

Forwarded ports:

```
L1234      10.10.1.2:3306
```

Add new forwarded port:

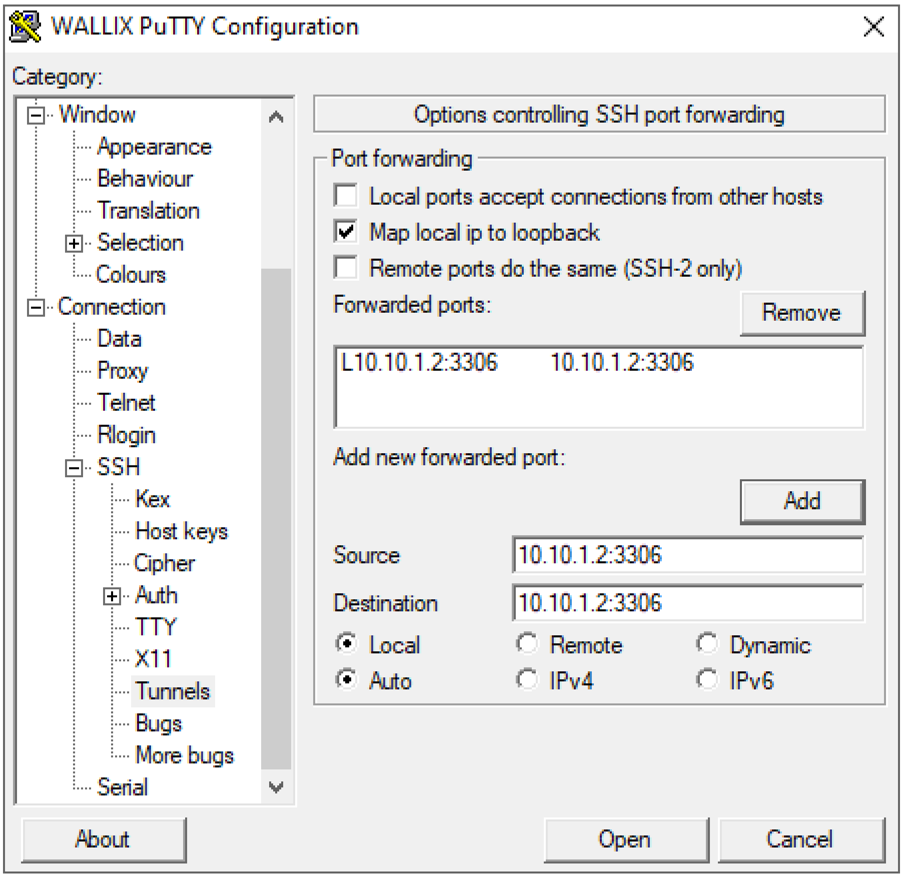
Source: 1234

Destination: 10.10.1.2:3306

● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

5. In **Connection > SSH > Tunnels**, for the redirection to a temporary interface:
    a. Enable **Map local ip to loopback**.
    b. In the **Source** field, enter `<TARGET_IP>:<PORT>`.
    c. In the **Destination** field, enter `<TARGET_IP>:<PORT>`.
    d. Click **Add**.
    e. Select **Local** and **Auto**.



Port forwarding

□ Local ports accept connections from other hosts

☑ Map local ip to loopback

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

```
L10.10.1.2:3306    10.10.1.2:3306
```

Add new forwarded port:

Source: 10.10.1.2:3306

Destination: 10.10.1.2:3306

● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

6. Click **Open**.

6.4.3. Universal Tunneling connections from a Linux workstation

About this task

Important:

Logging in from a Linux workstation only allows the redirection to the local address.

Procedure

1. Open you SSH client.
2. Enter the following command.

```
$ ssh -L <LOCAL_PORT>:<TARGET_IP:PORT> Interactive@<DEVICE:USER>@<BASTION_IP>
```

6.5. Troubleshooting

6.5.1. Troubleshooting target account login issues

A connection to a target account can fail for any of the following reasons:

- the WALLIX Bastion service is unavailable or inaccessible
- the target device is inaccessible
- the target account does not exist

- the protocol is not authorized
- the maximum number of authorized concurrent connections is reached
- you entered an invalid login or password
- you entered an invalid target account password
- you are not authorized to access the target account
- you attempt to log on outside the authorized time frame

6.5.2. Silent SSH session

On some target platforms, the characters sent by the target device are not displayed on the screen and there is no echo of the characters input on the keyboard.

This issue was mainly detected on the following targets:

- TELNET Open Solaris servers
- TELNET Solaris 8 servers

De-allocate a pseudo terminal (TTY)

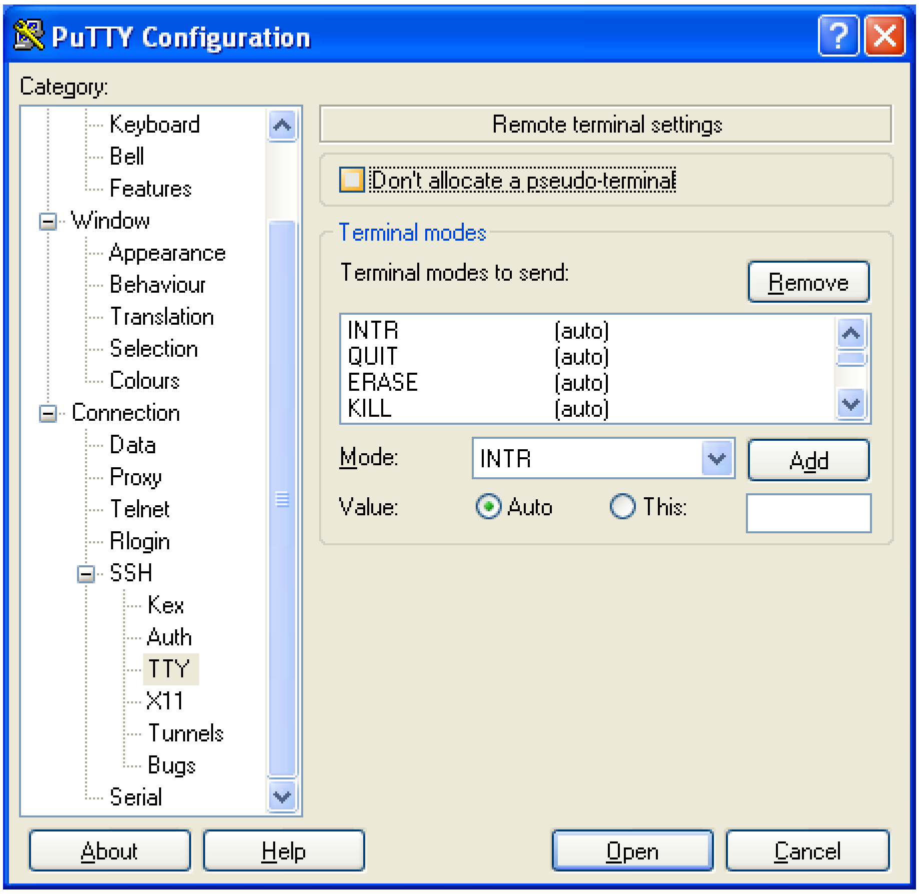
Procedure

- Under Linux/Unix, the related command is `ssh -T <Machine:Service:Username@Bastion>`.

  ```
  $ ssh -T <root@obelix:martin@wab.mycorp.lan>
  martin's password:
  ```

- Launch PuTTY to open the PuTTY Configuration window.

- Under **Category**, click **Connection > SSH > TTY** and enable the **Don't allocate a pseudo-terminal** option.



☐ Don't allocate a pseudo-terminal

Terminal modes to send:

```
INTR                 (auto)
QUIT                 (auto)
ERASE                (auto)
KILL                 (auto)
```

Mode: INTR

Value: ● Auto ○ This:

7. Approval workflow

If an approval workflow is defined to restrict connection to a target or access to target credentials, it is necessary to send a request to approvers before you can access and use targets.

Overview of a basic approval workflow

1. John Smith wants to access a restricted target.
2. John submits a request for this target and explains why access is necessary.
3. Jane Doe, who is trusted with managing access to this target, receives a notification which indicates that John submitted a request.
4. Jane reviews the request and approves it.
5. If access to the target requires only one approval, John can access the target. However, if several approvals are required, John must wait for that number of approvals to be reached.
6. If the request is approved enough times, John can access the target. If at least one approver rejects the request, then John cannot access the target.

Request statuses

A valid request (that is, its duration did not expire) can have one of the following statuses:

Accepted

The quorum (that is, the minimum number of favorable answers required for the authorization) was reached. It is then possible to access the target or target credentials from the date and time requested by the user, and for the duration validated by the approvers.

When the request is accepted by the first approver and the start date and time is 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

Rejected

An approver rejected the request. The user receives an e-mail with the reason for the rejection.

Pending

The quorum is not reached, and the request is not rejected.

Canceled

The user canceled the request, or one of the approvers canceled the request.

Closed

The request is no longer valid, and it is no longer possible for an approver to answer the request.

A request can be closed because the timeout is reached, because it was a one-time access, and it was used.

When a request is approved, it is possible to start a new session as long as the period defined by the request's duration did not expire, unless only a single connection is allowed. During this period, it is also possible to restart the session multiple times. It is then not necessary to keep open the initial connection.

If the session must start immediately (with an SSH or RDP client), the proxy offers the possibility to fill in a request form, if the selected target requires an approval.

7.1. Request access to restricted sessions

About this task

If the access to a session is protected, you must submit a request to access the session and wait for approval. For more information, refer to Approval workflow *(on page 52)*.

Procedure

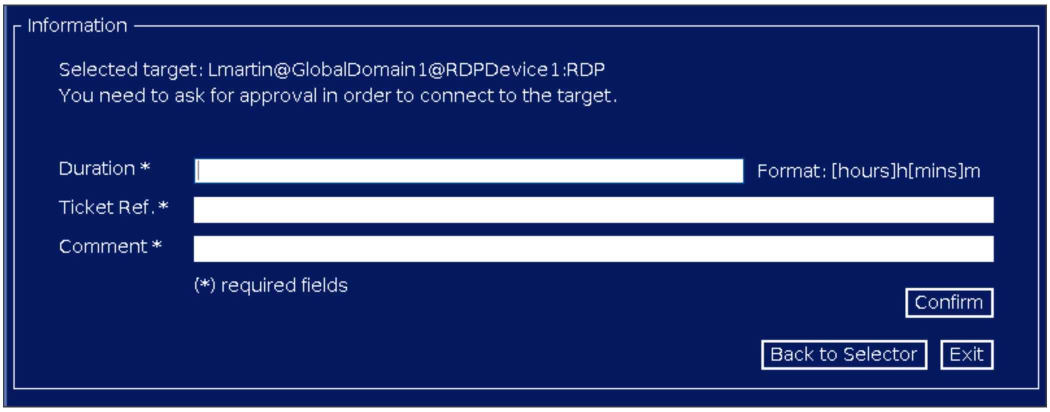
1. Go to the **My authorizations > Sessions** page.
2. Click the **Create an approval request** icon for the session you want to access.

   The approval request dialog box opens.
3. Enter the start date and time of the request.

   By default, this is the current date and time. However, you can add a later date to ensure it is approved early enough.
4. Enter the duration of the request, expressed in hours and minutes.
5. If enabled for this authorization request, enter the ticket reference associated with the request.
6. If enabled for this authorization request, add a comment to specify the reason for the approval request.
7. Click **Send request and close** if this is the only request you have, or **Request and continue** to make another request for the same session.

Results

If you are making an approval request from a proxy connection, you do not have the possibility to select a start date and time. The start date and time is the day on which you make the approval request. The following screenshot shows a RDP Proxy approval request.



Information

Selected target: Lmartin@GlobalDomain1@RDPDevice1:RDP
You need to ask for approval in order to connect to the target.

Duration * Format: [hours]h[mins]m

Ticket Ref. *

Comment *

(*) required fields

7.2. Request access to restricted secrets

About this task

If the access to the secret is protected, you must submit a request to access the secret and wait for approval. For more information, refer to Approval workflow *(on page 52)*.

Procedure

1. Go to the **My authorizations > Secrets** page.
2. Click **Create an approval request** next to the secret you want to access.

   The approval request dialog box opens.
3. Provide the start date and time of the request with the help of the calendar, and click **OK**.

   By default, this is the current date and time.
4. In **Duration**, define how long you require access to the secret (in hours and minutes).
5. **Optional:** If enabled for this authorization request, enter the ticket reference associated with the request.
6. **Optional:** If enabled for this authorization request, add a comment to specify the reason for the approval request.
7. Click **Send request and close** if this is the only request you have, or **Request and continue** to make another request for the same secret.

Results

Your request is submitted to approvers. You must wait for the approval or refusal. For more information, refer to Manage my submitted requests *(on page 54)*.

7.3. Manage my submitted requests

When you submit approval requests either for a secret or a session, you can follow and manage the request from the **My authorizations > Approval requests** page.

Requests have a status and a quorum. You can sort your requests by their status or filter the view to restrict the display to only one status.

For each request, you can:

View approval request details

View the details of the request, cancel the request (only for pending or accepted requests), and send an e-mail to all the relevant approvers.

Cancel approval request

Cancel the request for pending or accepted requests.

Notify approvers

Remind approvers who have not yet approved the request to review it by sending a new notification for active requests that are pending.

7.4. Answer an approval request

If you are a member of an approval group, you must manage approval requests from users wanting to access restricted targets.

Procedure

1. Go to the **Authorizations > My current approvals** page.
   This page lists all pending requests addressed to you.
2. Click **View details** next to the request you want to review.
   You can also click **Click here to review the approval request** for the relevant request from your notification center.
3. Review the details of the request, including information provided by the requesting user and answers from other approvers, to understand the context.

4. Add a comment to explain your decision.
   This comment is visible to the user who submitted the request and to other approvers.
5. **Optional:** Reduce the requested access duration if you consider the duration too long.
   You cannot augment the duration.
6. Set a timeout for the connection.
   For any approved request, if the requesting user did not connect to the target and the configured timeout is reached, then the request is automatically closed.
   If you do not want to configure a timeout for this request, enter `0`.
7. Decide if you authorize the access by clicking **Approve** or if you deny the access by clicking **Reject**.

Results

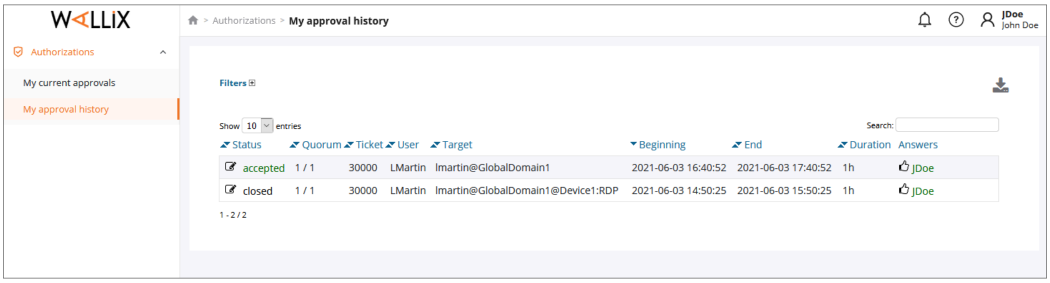
As long as the quorum is not reached, the request is not fully approved or declined. You can click **Notify approvers** to notify approvers again.

> **Note:**
>
> A session or the target credentials can be accessed as long as an accepted request is not expired, however, you can cancel this request to inhibit further access by clicking **Cancel**. For more information, refer to Cancel an approved request *(on page 55)*.

What to do next

From the **Authorizations > My approval history**, you can view all requests you already answered.

“My Approval History” page



Status	Quorum	Ticket	User	Target	Beginning	End	Duration	Answers
accepted	1 / 1	30000	LMartin	lmartin@GlobalDomain1	2021-06-03 16:40:52	2021-06-03 17:40:52	1h	JDoe
closed	1 / 1	30000	LMartin	lmartin@GlobalDomain1@Device1:RDP	2021-06-03 14:50:25	2021-06-03 15:50:25	1h	JDoe

1 - 2 / 2

7.5. Cancel an approved request

About this task

A session or the target credentials can be accessed as long as an accepted request is not expired. As an approver, you can cancel a request before its expiration to inhibit further access to the target.

Procedure

1. Go to the **Authorizations > My approval history** page.
   This page lists all the requests that you answered.
2. Click **View details** for the accepted request you want to review.
3. Add a comment to explain why you are canceling the request.
4. Click **Cancel approval request**.

8. Annex

8.1. Glossary

4 eyes

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

4 hands

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

Access control list (ACL)

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

Account

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

Account lock

Mechanism preventing the concurrent use of an account.

Account mapping

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

Appliance

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

Application cluster

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

Approval request

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

Approval workflow

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

Audit

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

Authentication agent

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

Authentication transfer

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

Authorization

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

Auto-deployment upgrade

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

Auto logon

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

Automatic credential injection

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

Backup

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

Bastion cluster

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

Break Glass

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

Check-in

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

Checkout

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

Checkout policy

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

Client

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

Connection policy

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

Connection scenario

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

Controlled deployment upgrade

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

Credential / Authentication information

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

Critical session

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

Device

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

Discovery

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

External authentication

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

Global account

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

Global domain

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

HA Database Replication

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

Interactive login

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

Local account

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

Local authentication

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

Local domain

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

Local storage

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

Login transformation rule (LTR)

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

Log

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

Major upgrade

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

Manual logon

Target connection mode allowing a manual connection using the password.

Minor upgrade

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

Multi-tunneling

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

Pattern detection

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

Permission profile

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

Primary connection

Connection initiated between a user and WALLIX Bastion.

Remote storage

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

Resident agent

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

Resource

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

Restoration

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

Scenario account

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

Seamless connection

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

Secondary connection

Connection initiated between WALLIX Bastion and a target.

Secret

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

Secret rotation plugin

Previously called "Password rotation plugin."

Extension allowing the configuration of secret rotations for targets.

Secret rotation policy

Previously called "Password rotation policy."

Rules determining the settings for password or SSH key rotations.

Secret rotation

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

Secrets vault

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

Secret vault plugin

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

Session invite

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

Session

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

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

Session probe

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

Session recording

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

Session sharing

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

Startup scenario

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

Target account

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

Target application

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

Target group

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

Transparent mode

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

Universal Tunneling (UT)

Previously called RAW TCP/IP.

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

User group

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

Vault transformation rule (VTR)

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

Index

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

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

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

About WALLIX

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

WWW.WALLIX.COM

wallix