



WALLIX Bastion 12.1.0

Functional Administration Guide

Copyright © 2007 – 2025 WALLIX

WALLIX PAM



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

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

WALLIX Bastion is subject to the WALLIX software license contract.

WALLIX Bastion is based on free software. The list and source code of GPL and LGPL licensed software used by WALLIX Bastion are available from WALLIX upon request.

The Third-Party Components document lists all packages modified by WALLIX and the information related to the license agreement terms.

Contents

1. Introduction.....	10
1.1. Additional features.....	10
1.2. Warning.....	11
2. WALLIX Bastion authentication.....	12
2.1. Authentication with a login and password.....	13
2.2. Authentication with an Identity Provider.....	13
2.3. Authentication with an X.509 certificate.....	13
2.4. Authentication with Kerberos.....	14
3. Navigating the WALLIX Bastion web interface.....	15
4. Configuring your account.....	16
4.1. Update my e-mail.....	16
4.2. Update my password.....	16
4.3. Update my preferred language.....	16
4.4. Define my SSH key.....	17
4.5. Define a GPG key.....	17
4.6. Define my SSH or RDP default client.....	18
5. Getting started with WALLIX Bastion administration.....	19
5.1. About WALLIX Bastion.....	19
5.2. WALLIX Bastion in the network infrastructure.....	19
5.3. WALLIX Bastion ACLs.....	20
5.4. WALLIX Bastion user base roll-out.....	21
6. Rights and access control for user accounts.....	22
6.1. Permission profiles.....	22
6.1.1. Permission profile overview.....	23
6.1.2. Default permission profiles.....	34
6.1.3. Create a custom permission profile.....	37
6.1.4. Export custom permission profiles.....	38
6.1.5. Import custom permission profiles.....	38
6.1.6. Edit a custom permission profile.....	42
6.1.7. Delete a permission profile.....	43
6.2. User groups.....	43
6.2.1. Add a user group.....	43
6.2.2. Import user groups.....	44
6.2.3. Edit a user group configuration.....	45
6.2.4. Manage members of a user group.....	46
6.2.5. Delete user groups.....	46
6.3. Control Local and LDAP/AD users access.....	47
7. User accounts management.....	48

7.1. General information.....	48
7.1.1. Overview of authentication protocols.....	48
7.1.2. Overview of authorization protocols.....	50
7.1.3. Overview of Multi-Factor Authentication.....	50
7.1.4. Setup recommendations.....	50
7.2. Directory Services users.....	52
7.2.1. Connect to an Active Directory server.....	53
7.2.2. Connect to an LDAP server.....	57
7.2.3. Import users from an LDAP or AD server.....	62
7.2.4. Authentication protocols for LDAP/AD users.....	63
7.3. Federated Identity users.....	71
7.3.1. SAML 2.0.....	71
7.3.2. Generic OpenID Connect (OIDC).....	77
7.4. Local users.....	80
7.4.1. Create local user accounts.....	81
7.4.2. Import local user accounts.....	82
7.4.3. Authentication protocols for local users.....	85
7.4.4. Unlock local user accounts.....	90
7.4.5. Edit local user accounts.....	90
7.4.6. Export local user accounts.....	91
7.4.7. Delete local user accounts.....	91
7.5. External sources management.....	91
7.5.1. Import authentication domains.....	92
7.5.2. Import user group mappings.....	96
7.5.3. Edit an external authentication.....	98
7.5.4. Edit an authentication domain.....	98
7.5.5. Disable and unset X.509 certificate authentication.....	98
7.5.6. Delete an external authentication.....	99
7.5.7. Delete an authentication domain.....	99
8. User communication.....	100
8.1. System notifications.....	100
8.1.1. Add connection messages for users.....	100
8.1.2. Add a banner message.....	100
8.2. E-mail notifications.....	101
8.2.1. List of default e-mail notifications.....	101
8.2.2. Custom notification templates.....	105
8.2.3. Change sender for e-mail notifications.....	108
8.2.4. Configure e-mail sending for event notifications.....	108
8.2.5. Edit e-mail sending for event notifications.....	109
8.2.6. Disable missing GPG key e-mail notification.....	109
8.2.7. Delete an e-mail notification trigger.....	109

9. Devices.....	110
9.1. Create a new device.....	110
9.2. Manage services for a device.....	110
9.3. Manage local domains associated with a device.....	111
9.4. Manage local accounts on the device.....	111
9.5. Manage the target groups associated with the device.....	113
9.6. Import devices.....	113
9.7. Edit a device.....	116
9.8. Use tags to organize devices.....	116
9.8.1. Manage the tags for a device.....	117
9.8.2. Add tags to multiple devices.....	117
9.8.3. Remove tags from multiple devices.....	117
9.9. View and delete certificates or keys on the device.....	118
9.10. Change target servers identification.....	118
9.11. Delete a device.....	118
10. Applications.....	119
10.1. Add a standard application.....	119
10.2. Add an account to a standard application.....	120
10.3. Manage the resource associations with a standard application.....	120
10.4. Import applications.....	121
10.5. Edit a standard application.....	122
10.6. Delete a standard application.....	122
10.7. Configure the jump server.....	122
10.8. Configure the application launch using RemoteApp mode.....	124
10.9. Automate connections to an application using Autolt scripts.....	125
10.10. Automate connections to a web app using WALLIX Application Driver.....	126
10.10.1. WALLIX Application Driver parameters for web app launch.....	127
10.10.2. Using WALLIX Application Driver without specific deployment.....	130
10.10.3. Using WALLIX Application Driver through a manual deployment.....	132
10.10.4. Using the browser extension with WALLIX Application Drive.....	133
11. Connection policies.....	134
11.1. Add a connection policy.....	134
11.2. Edit a connection policy.....	135
11.3. Transformation rules.....	135
11.3.1. Get a login for secondary connection.....	135
11.3.2. Retrieve account credentials in WALLIX Bastion vault.....	136
11.4. TELNET/RLOGIN connection scenario on a target device.....	137
11.5. Session probe mode.....	138
11.5.1. Launch the session probe from a specific directory.....	145
11.5.2. About outbound connection monitoring rules.....	145
11.6. Authentication mechanisms for RDP target connections.....	146

11.7. Force screen resolution on RDP targets.....	148
11.8. Startup scenario on a target device.....	149
11.8.1. Startup scenario options.....	149
11.9. Connect to a VNC session over an SSH tunnel.....	151
11.10. Log all keyboard input.....	152
11.11. Dynamic virtual channels for RDP protocol.....	153
11.12. Antivirus software or a DLP solution with ICAP.....	153
11.12.1. Configuration of connection to ICAP servers.....	154
11.12.2. Enabling file verification.....	154
11.12.3. Blocking file transfer on invalid verification.....	155
11.12.4. Enabling file storage on invalid verification.....	155
11.13. Configuration of cryptographic algorithms supported on target devices.....	156
11.13.1. SSH cryptographic settings on target devices.....	156
11.13.2. RDP cryptographic settings on target devices.....	156
11.14. Delete a connection policy.....	157
12. Targets.....	158
12.1. Target accounts.....	158
12.1.1. Add a target account to a global domain.....	159
12.1.2. Add a target account to a device.....	160
12.1.3. Add a target account to an application.....	160
12.1.4. Define SSH private key for global or device account.....	161
12.1.5. Define references for service account management.....	162
12.1.6. Associate global domain accounts to a group.....	162
12.1.7. Associate device or application accounts to a group.....	163
12.1.8. Import target accounts.....	164
12.1.9. Edit a target account.....	167
12.1.10. Delete a target account.....	167
12.2. Target groups.....	167
12.2.1. Create a target group.....	167
12.2.2. Import target groups.....	171
12.2.3. Edit a target group.....	172
12.2.4. Delete a target group.....	172
12.3. Domains.....	173
12.3.1. Add a global domain with a local vault.....	173
12.3.2. Add a global domain with an external vault.....	174
12.3.3. Import global domains.....	175
12.3.4. Import local domains.....	177
12.3.5. Add an account to the global or a local domain.....	179
12.3.6. Edit a global or a local domain.....	180
12.3.7. Change the passwords for all the accounts on a global domain.....	181
12.3.8. Change the passwords for all the accounts on a local domain.....	181

12.3.9. Associate the domain with an SSH Certificate Authority.....	182
12.3.10. Revoke the signed certificate for the accounts on the domain associated with a Certificate Authority.....	182
12.3.11. Delete a domain.....	183
12.4. Checkout policies.....	183
12.4.1. Add a checkout policy.....	184
12.4.2. Delete accounts using a checkout policy.....	184
12.4.3. Edit a checkout policy.....	184
12.4.4. Delete a checkout policy.....	185
12.5. Protected Users group.....	185
12.5.1. Target account configured as account mapping.....	186
12.5.2. Target account in WALLIX Bastion Vault.....	186
12.6. Setting up an AD authentication silo.....	186
12.7. Enabling smart card authentication on targets for RDP protocol.....	187
13. Authorizations.....	189
13.1. Create an authorization.....	189
13.2. Approval workflow.....	190
13.2.1. Approval workflow configuration.....	191
13.3. Edit an authorization.....	192
13.4. Import authorizations.....	192
13.5. Delete authorizations.....	196
14. Assets Discovery.....	197
14.1. Configure a network scan for device discovery.....	197
14.2. Configure a network scan for account discovery.....	198
14.3. Configure an Active Directory scan for device discovery.....	199
14.4. Configure an Active Directory scan for local account discovery.....	200
14.5. Configure an Active Directory scan for global account discovery.....	201
14.6. Configure a MS Azure Active Directory scan for device discovery.....	201
14.7. Configure a MS Azure Active Directory scan for local account discovery.....	202
14.8. Launch a scan manually.....	204
14.9. Set a periodic scan launch.....	204
14.10. Scan job information.....	204
14.10.1. Get general information about a scan.....	205
14.10.2. View the raw results of a scan.....	205
14.11. Cancel a running scan job.....	206
14.12. Onboard discovered resources in WALLIX Bastion.....	206
14.12.1. Onboard discovered devices or local accounts.....	207
14.12.2. Onboard discovered global accounts.....	208
15. Secrets rotation.....	209
15.1. Password change policies.....	209
15.1.1. Add a password change policy.....	210

15.1.2. Edit a password change policy.....	212
15.1.3. Schedule secret rotation for target accounts on a domain.....	212
15.1.4. Modify the maximum number of parallel secret rotations.....	212
15.1.5. Delete a password change policy.....	213
15.2. Password change plugins.....	213
15.2.1. Check Point Gaia plugin.....	215
15.2.2. Cisco plugin.....	216
15.2.3. Cisco Nexus plugin.....	216
15.2.4. Citrix ADC plugin.....	217
15.2.5. Dell iDRAC plugin.....	217
15.2.6. F5 BIG IP plugin.....	218
15.2.7. Fortinet FortiGate plugin.....	218
15.2.8. HP ILO plugin.....	219
15.2.9. IBM 3270 plugin.....	220
15.2.10. IBM AIX plugin.....	222
15.2.11. Juniper SRX plugin.....	223
15.2.12. LDAP plugin.....	223
15.2.13. MySQL plugin.....	224
15.2.14. Oracle plugin.....	225
15.2.15. Palo Alto PANOS plugin.....	225
15.2.16. Ultra VNC plugin.....	226
15.2.17. Unix plugin.....	227
15.2.18. VMWare ESX plugin.....	228
15.2.19. Windows plugin.....	228
15.2.20. WindowsService plugin.....	231
15.3. External password vault plugins.....	235
15.3.1. Bastion plugin.....	236
15.3.2. CyberArk Enterprise Password Vault plugin.....	237
15.3.3. HashiCorp Vault plugin.....	238
15.3.4. Thycotic Secret Server plugin.....	240
15.4. Configure automatic secret rotation for a domain.....	243
15.5. Configure automatic secret rotation for a target account at check-in.....	244
15.6. Manually trigger secret rotation for a target account (with user-generated secrets).....	244
15.7. Manually trigger secret rotation for one or more target accounts (with auto-generated secrets).....	245
15.8. Automatically trigger secret rotation for one or more target accounts (with auto-generated secrets).....	245
15.9. Trigger secret rotation for all target accounts using a same password change policy (CLI).....	246
15.10. "Break Glass" mechanism.....	246
15.10.1. Standard "Break Glass" mechanism.....	246

15.10.2. Alternative "Break Glass" mechanism.....	247
16. Sessions configuration.....	248
16.1. Restrict sessions use.....	248
16.1.1. User authorizations on sessions.....	248
16.1.2. External ticketing system script for approval workflow.....	250
16.1.3. Time frames for target access.....	251
16.1.4. RDP options.....	252
16.1.5. Restrictions for RDP pattern detection.....	253
16.1.6. SSH options.....	254
16.1.7. Restrictions for SSH pattern detection.....	256
16.1.8. Import restrictions for target groups and user groups	260
16.2. Session invite.....	262
16.2.1. Customize expiry for session invite.....	263
16.3. Transparent mode configuration for RDP and SSH proxies.....	263
16.4. KeepAlive function for the proxies.....	264
16.4.1. Enabling KeepAlive function for connection between the RDP proxy and the RDP client.....	264
16.4.2. Enabling KeepAlive function for connection between the SSH proxy and the SSH client.....	265
16.4.3. Enabling KeepAlive function for connection between the SSH proxy and the SSH target server.....	265
16.5. Session probe mode with the WALLIX BestSafe agent.....	266
16.5.1. Enabling the interaction with the WALLIX BestSafe agent.....	266
17. Infrastructure strategy.....	268
17.1. Clusters.....	268
17.1.1. Add a cluster.....	268
17.1.2. Import clusters.....	268
17.1.3. Edit a cluster.....	269
17.1.4. Delete clusters.....	270
17.2. Load balancing with Remote Desktop Connection Broker.....	270
18. Universal Tunneling (RAW TCP/IP).....	272
18.1. Seamless connection.....	273
18.2. Multi-tunneling.....	273
18.3. NAT	274
18.4. Configuration to access an IT or OT target.....	274
19. Monitor WALLIX Bastion activity.....	276
20. Annex.....	279
20.1. Glossary.....	279
21. Index.....	I



1. Introduction

About this guide

This document is the Administration Guide for WALLIX Bastion 12.1.0. It is aimed at resource administrator who manage day-to-day administration of users, targets, and all surrounding areas.

Use it to configure WALLIX Bastion before roll-out, and also for its day-to-day administration.

The following documents are also provided by WALLIX:

- The Deployment Guide
- The System Operations Guide
- The Users and Approvers Guide
- The Sessions Audit Guide
- The SIEM Logs Guide

1.1. Additional features

WALLIX Session Manager

This specific feature of WALLIX Bastion is available according to the software license contract signed by your company. This feature allows you to:

- identify the users who are connected to specific devices and monitor their activity. Sessions can be viewed in real-time through the WALLIX Bastion web administration interface or downloaded to be viewed locally on a local workstation
- review video-recorded activity from a privileged user session
- get a direct resource access using native clients such as PuTTY, WinSCP, MSTC, or OpenSSH
- define and configure connection policies through mechanisms available for RDP, VNC, SSH, TELNET, RLOGIN, and RAW TCP/IP protocols

For more information, refer to [Sessions configuration \(on page 248\)](#).



Attention:

The **Session management** menu and the **Sessions** entry in the **My authorizations** menu can only be managed if the WALLIX Session Manager feature is associated with your license key.

WALLIX Password Manager

This specific feature of WALLIX Bastion is available according to the software license contract signed by your company. This feature allows you to:

- secure target account passwords and SSH keys
- manage checkout and check-in actions for target account credentials
- change or generate target account passwords
- define a password change policy which can be selected during the creation/modification of a global domain
- select a password change plugin among the list configured in WALLIX Bastion during the creation/modification of a global or local domain



For more information, refer to [Secrets rotation \(on page 209\)](#).



Attention:

The **Password management** menu and the **Secrets** entry in the **My authorizations** menu can only be managed if the WALLIX Password Manager feature is associated with the license key.

1.2. Warning

The installation of external components such as Endpoint Detection and Response (EDR), backup, or monitoring agents is forbidden.

Any changes to the WALLIX Bastion system other than those available in the GUI or in the CLI commands are in violation of the WALLIX terms and conditions.

The person carrying out the operations is accountable for any variation from the information and procedures provided in the product documentation. These variations may diverge from secure guidelines or fall outside of the allowed scope.

2. WALLIX Bastion authentication

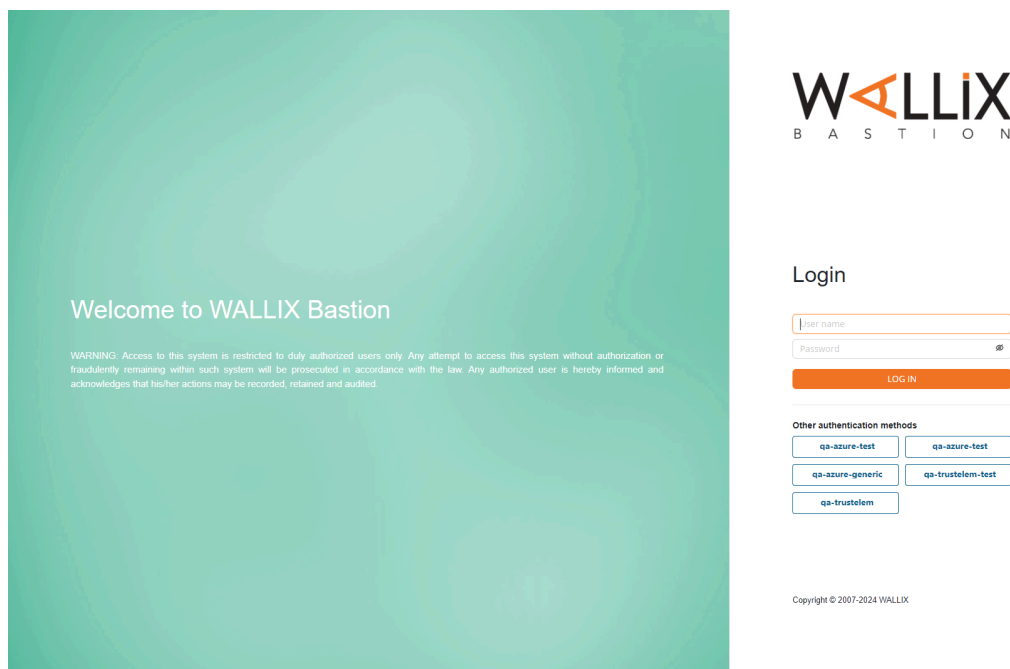
You can access WALLIX Bastion from the `https://<bastion_name>/ui` address. The login page is displayed according to your browser's language preferences. After the authentication, you can select a different preferred language for WALLIX Bastion.



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.



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 \(on page 13\)](#)

[Authentication with an X.509 certificate \(on page 13\)](#)

[Authentication with an Identity Provider \(on page 13\)](#)

[Authentication with Kerberos \(on page 14\)](#)



2.1. Authentication with a login and password

Procedure

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

The password is case-sensitive.

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

2.2. Authentication with an Identity Provider

Procedure

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

2.3. Authentication with an X.509 certificate

About this task

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

Before you begin

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

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

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



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

Procedure

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



Note:

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

Results

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

2.4. Authentication with Kerberos

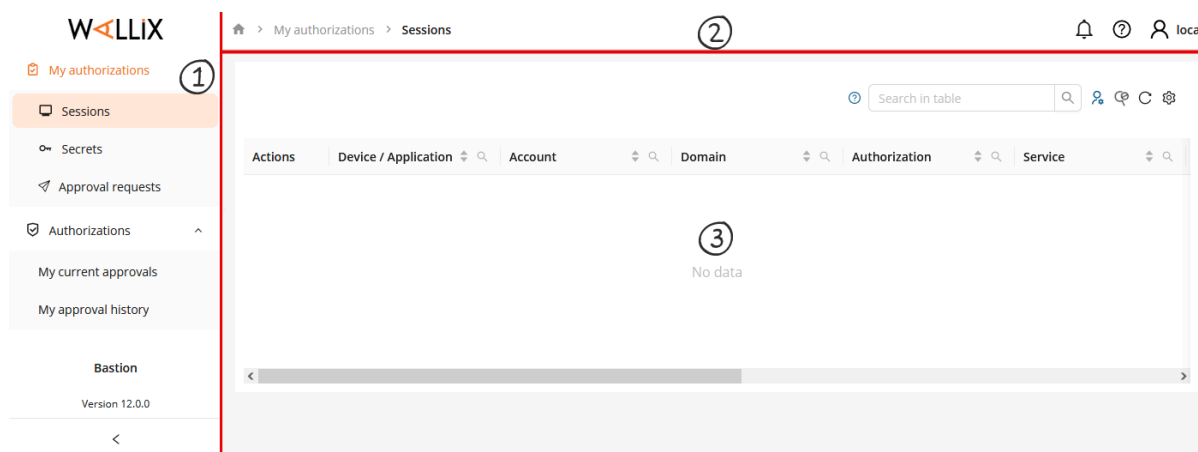
Procedure

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



3. Navigating the WALLIX Bastion web interface

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



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

Logging out

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



4. Configuring your account

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

4.1. Update my e-mail

Procedure

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

4.2. Update my password

Before you begin



Attention:

The **Password** tab is only available if the user was declared locally with a **local_password** authentication. Only this type of users can update their password from this tab.

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

The **SSH public key** tab is only available if the user was declared locally with a **local_sshkey** authentication. Only this type of users can update their password from this tab.



Attention:

It is not possible to provide a SSH Key if no algorithm is allowed for the SSH key on the **Configuration > Local Password Policy** page. For more information, refer to [Local password policy \(on page 85\)](#).



Note:

If PuTTYgen is used to generate the key, the public key displayed in the OpenSSH format during the generation must be saved in a text file. As an example, this key is labeled as follows: `ssh-rsa AAAAB3NzaC1yc2EAAAABJQ6[ . . . . ]c3xu9p/xNjw== rsa-key-20151204`. This key can then be uploaded.

If a key already exists, a private key can be uploaded. PuTTYgen must be used to generate the corresponding public key in the appropriate format.

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



Attention:

By default, users who must provide a GPG key receive a daily warning e-mail if they do not do have one. Administrators can modify this default behavior.



Important:

In HA Database Replication Master/Master mode, you must upload the GPG key to both master nodes, even if the second node displays the fingerprint after uploading the GPG key to the first node.



Procedure

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

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.



5. Getting started with WALLIX Bastion administration

5.1. About WALLIX Bastion

WALLIX Bastion was developed for the technical teams who administer IT infrastructure (servers, network, and security devices, etc.). This solution was designed to meet the access control and traceability needs of system administrators.

WALLIX Bastion includes access control lists (ACLs) and traceability features. It constitutes a security buffer for administrators who want to log on to devices by:

- checking the authentication detail provided by the user
- checking their access rights for the concerned resource
- managing passwords of the target accounts

WALLIX Bastion also allows you to automate logons to target devices to enhance the security of the information system by preventing disclosure of server authentication detail.

The following protocols are supported:

- SSH (and its sub-systems)
- TELNET, RLOGIN
- RDP and VNC
- RAW TCP/IP. This protocol allows to forward local TCP/IP connections on the client station to a target server using local TCP/IP port forwarding. The SSH proxy acts as an SSH server whose function is only to provide local TCP/IP port forwarding. If a shell session channel is opened at the beginning, it will then monitor the forwarding actions performed.

WALLIX Bastion offers a web interface (also called "GUI"), compatible with Internet Explorer, Chrome, and Firefox to monitor activity and connections and also configure its components.

5.2. WALLIX Bastion in the network infrastructure

WALLIX Bastion is positioned between a low trust domain and a high trust domain.

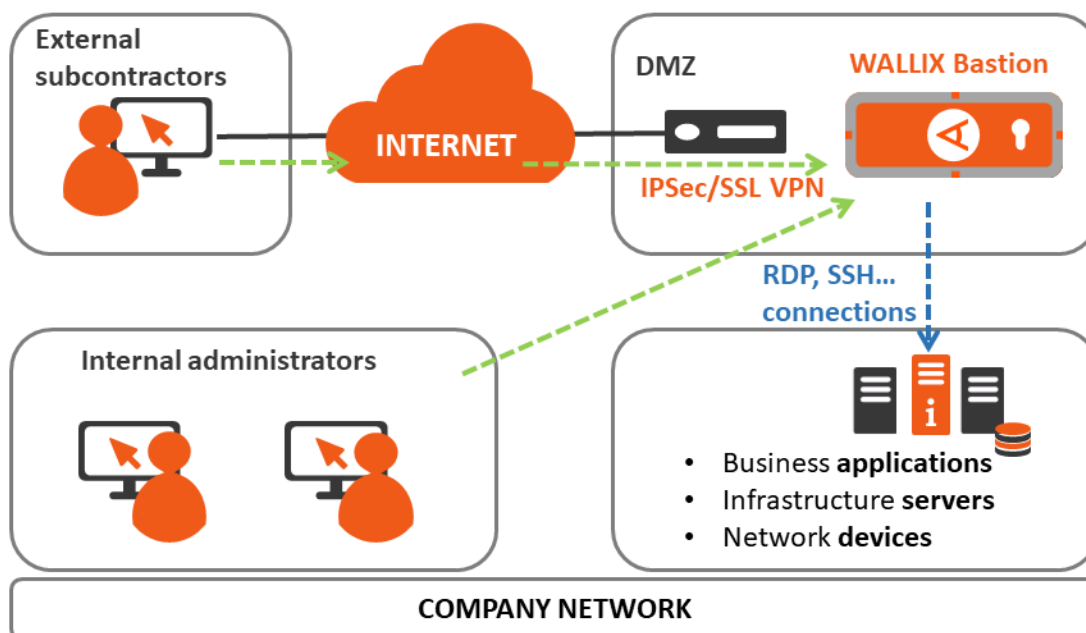
The high trust domain is represented by the set of devices isolated by WALLIX Bastion. These devices and their related accounts are called "target accounts" in the WALLIX Bastion terminology.

The low trust domain is represented by the population with direct access to WALLIX Bastion:

- the company's workforce
- the Internet zone

For users of the solution, access to the target accounts (in the high trust domain) is only possible through WALLIX Bastion.

WALLIX Bastion in the network infrastructure



5.3. WALLIX Bastion ACLs

WALLIX Bastion features an advanced rights management engine relying on Access Control Lists (ACLs) to determine who has access to what, when, and with which protocols.

These ACLs consist of the following objects:

- Users: that is physical users of WALLIX Bastion from internal or external user directory
- User groups: a set of users
- Devices: that is physical or virtual devices to which access is requested through WALLIX Bastion
- Target accounts: the accounts declared on a device or an application
- Target groups: a set of target accounts
- Applications: any type of application and services running on a device or a set of devices

In WALLIX Bastion, an authorization must be configured to grant a user the access to a target account. Authorizations are declared between a group of users and a group of target accounts. That means that each target account must belong to a target group, and that each user must belong to a user group.

The authorization allows users in group X to access target accounts in group Y, with protocols A, B, or C.

Other elements are added to these primary entities to allow you to define:

- connection time frames
- criticality of access to target resources
- whether the session is recorded or not
- the type of user authentication procedure

You can also define a number of various WALLIX Bastion administrator profiles, with a full access to the WALLIX Bastion features or limited rights to specific features. For example, you can define that



WALLIX Bastion auditors only access audit data, or allow WALLIX Bastion administrators to add/edit users, configure the system administration, manage authorizations, etc.

5.4. WALLIX Bastion user base roll-out

The following list shows the three steps to obtain a properly set up user base in WALLIX Bastion.

1. Manage access at scale.
 - a. Import or create profiles to restrict user access to features and actions.
 - b. Import or create user groups to simplify authorization management.
2. Build the user base.
 - a. If your user base is stored on a source outside WALLIX Bastion, configure a connection to the external source.
 - b. If you require local users, then import or create user accounts locally.
3. Customize communication with users.
 - a. Brand communication to personalize the experience.
 - b. Set notification triggers and create templates to keep users informed of any relevant event.



6. Rights and access control for user accounts

Control which features and actions are available to users by creating permission profiles and assigning group memberships.

6.1. Permission profiles

What are permission profiles?

A profile specifies the authorizations for the main features of the web interface accessible from the WALLIX Bastion menu. Profiles can be assigned to individual users or directly to user groups. They can also be assigned to API keys.

If a user has conflicting profiles, they always receive the highest level of authorization for each feature.

Example of conflicting profiles

John Doe has two profiles. Individually, John has **Profile A**, but John also belongs to a group with **Profile B**. Both profiles grant different right levels on different features. The following table presents what each profile grants as feature rights.

	Profile A	Profile B
Feature 1	View	Modify
Feature 2	View	None

Because the highest right always applies, the effective rights for John are:

- **Modify** right on feature 1 (thanks to **Profile B**)
- **View** right on feature 2 (thanks to **Profile A**).

Default and custom permission profiles

WALLIX Bastion includes a set of default profiles designed to maintain security by ensuring proper separation of authorizations. These profiles are preconfigured and cannot be modified or deleted, serving as a baseline to meet security standards. For more information, refer to [Default permission profiles \(on page 34\)](#).

To provide greater flexibility and address specific needs, WALLIX Bastion also provides the ability to create custom profiles. By creating custom profiles, you can tailor the delegation of rights to better align with your unique requirements. For more information on the granularity of profile parameters, refer to [Permission profile overview \(on page 23\)](#).

While default profiles ensure a standard level of security, custom profiles enable fine-tuning of access controls and permissions to meet specific operational needs.



Tip:

WALLIX advises against creating a single tailored profile for a user account with broad requirements. For example, WALLIX suggests creating two accounts with two different profiles for a user who has administrator permissions as well as target access. In other words, that user should have one account which grants typical user rights and a second account with an administrator profile.



API keys specification

When a user authenticates using an API key, the resulting profile is determined by combining the profile of the authenticated user and the profile of the API key. This means that the final profile is created as follows:

- The intersection of the user and API key profiles defines the feature rights and transferable rights. The resulting permission profile is the highest degree of right shared between both profiles. For example, for any feature, if the API key profile has the **None** right but the user has the **Modify** right, **None** applies because it is the highest shared right. Similarly, if the API key profile has the **Modify** right but the user profile has the **View** right, **View** applies because it is the highest shared right.
- Dashboards access, IP limitations, user group limitations, and target group limitations are inherited from the profile of the authenticated user.

6.1.1. Permission profile overview

Introduction

A permission profile is a set of several parameters, each addressing specific questions:

- Profile type: is the profile editable?
- Feature rights: what can a user with this profile view, use, and configure?
- Transferable rights: what can a user with this profile delegate to other users?
- Dashboard access: what data can a user with this profile view?
- Limitations and restrictions: are there specific conditions under which a user with this profile can exercise their permissions?



Important:

A profile which grants no features rights and no dashboard access in fact forbids authentication to the web interface.



Note:

It is not possible to view the profiles and users with a profile having at least one permission that the authenticated user does not have. However, it does not apply to the **Session audit** and the **Target account access** features.

6.1.1.1. Profile type

All profiles have a type declared at the moment of their creation. There are two available types:

Editable

Editable profiles can be modified multiple times after creation. They can also be deleted.

New custom profiles are set to **Editable** by default.

Read-only

Read-only profiles cannot be modified after creation, but they can be deleted.

All default profiles are read-only, but they cannot be deleted.



The read-only profile type is required for API keys.

6.1.1.2. Feature rights

Permission profiles define the rights for the main features of WALLIX Bastion. Each feature has different levels available.

Session audit

This feature manages access to the following pages in the web interface:

- **Audit > Current sessions**
- **Audit > Session history**
- **Audit > Account history**
- **Audit > Approval history**
- **Audit > Authentication history**
- **Audit > Connection statistics**

Right	Description
None	All related menu entries are hidden.
View	Users with this authorization can view the information inside the related pages and use the available options.

System audit

This feature manages access to the following pages in the web interface:

- **Configuration > Audit logs**
- **System > Status**
- **System > Syslog**
- **System > Boot messages**

Right	Description
None	All related menu entries are hidden.
View	Users with this authorization can view the information inside the related pages and download the available log files.

Users

This feature manages access to the following pages in the web interface:

- **Users > Accounts**
- **Import/Export > CSV**
- **Import/Export > Users from LDAP/AD**



Right	Description
None	All related menu entries are hidden.
View	From the Users > Accounts page, users with this authorization can: • view the complete list of users from available configured domains. • view the configuration information for any user. • download the CSV file. From the Import/Export > CSV page, users with this authorization can export files for the Users data type. The Users from LDAP/AD page is hidden and unavailable to this level of authorization.
Modify	This level of authorization grants the View rights and the following additional rights: From the Users > Accounts page, users with this authorization can • create local users. • modify user account configurations. • delete user accounts. • download and import the CSV files available. From the Import/Export > CSV page, users with this authorization can also import files for the Users data type. From the Users from LDAP/AD, users with this authorization can import users.

User groups

This feature manages access to the following pages in the web interface:

- **Users > Groups**
- **Import/Export > CSV**

Right	Description
None	All related menu entries are hidden.



Right	Description
View	From the Users > Groups page, users with this authorization can: • view the complete list of user groups. • view the configuration information for any user group. From the Import/Export > CSV page, users with this authorization can export files for the following data types: • Authentication domain mappings on user groups • User groups
Modify	This level of authorization grants the View rights and the following additional rights: From the Users > Groups page, users with this authorization can • create user groups. • edit user groups configuration. • delete user groups. From the Import/Export > CSV page, users with this authorization can also import files for the following data types: • Authentication domain mappings on user groups • User groups

**Note:**

You must at least grant the **View** right on **Target groups** and **User groups** features when setting rights to manage authorizations or approvals.

Targets & accounts

This feature manages access to the following pages in the web interface:

- **Targets > Devices**
- **Targets > Applications**
- **Targets > Domains**
- **Targets > Accounts > Global accounts**
- **Targets > Accounts > Device accounts**
- **Targets > Accounts > Application accounts**
- **Targets > Clusters**
- **Targets > Password vault plugins**
- **Targets > Checkout policies**
- **Targets > Discovery > Onboarding**
- **Import/Export > CSV**



Right	Description
None	All related menu entries are hidden.
View	From any listed page of the Targets menu, users with this authorization can consult information on all configured items. From the Import/Export > CSV page, users with this authorization can export files for the following data types : • Accounts • Applications • Clusters • Devices • Global domains • Local domains • Restrictions • User groups
Modify	This level of authorization grants the View rights and the following additional rights: From any listed page of the Targets menu, users with this authorization can also create, manage, delete items. From the Import/Export > CSV page, users with this authorization can also import files for the following data types : • Accounts • Applications • Clusters • Devices • Global domains • Local domains • Restrictions • User groups

**Note:**

You must at least grant the **View** right on **Target groups** and **User groups** features when setting rights to manage authorizations or approvals.

Target groups

This feature manages access to the following pages in the web interface:

- **Target > Groups**
- **Import/Export > CSV**.



Right	Description
None	All related menu entries are hidden.
View	From the Target > Groups page, users with this authorization can: • view the complete list of target groups. • view the configuration information for any target group. From the Import/Export > CSV page, users with this authorization can export files for the Target group data type.
Modify	This level of authorization grants the View rights and the following additional rights: From the Target > Groups page, users with this authorization can: • create target groups. • modify target groups configurations. • delete target groups. From the Import/Export > CSV page, users with this authorization can also import files for the Target group data type.

**Note:**

You must at least grant the **View** right on **Target groups** and **User groups** features when setting rights to manage authorizations or approvals.

Manage Authorizations

This feature manages access to the following pages in the web interface:

- **Authorizations > Manage authorizations**
- **Import/Export > CSV**

Right	Description
None	All related menu entries are hidden.



Right	Description
View	From the Authorizations > Manage authorizations page, users with this authorization can: • view the complete list of authorizations. • view the configuration information for any authorization. From the Import/Export > CSV page, users with this authorization can export files for the Authorizations data type.
Modify	To grant this level of right, User groups and Target groups must both be set to View or Modify. This level of authorization grants the View rights and the following additional rights: From the Authorizations > Manage authorizations page, users with this authorization can create, manage, delete authorizations. From the Import/Export > CSV page, users with this authorization can also import files for the Authorizations data type.

**Note:**

You must at least grant the **View** right on **Target groups** and **User groups** features when setting rights to manage authorizations or approvals.

Manage Approvals

This feature manages access to the following pages in the web interface:

- **Authorizations > My current approvals**
- **Authorizations > My approval history**

Right	Description
None	All related menu entries are hidden.
View	From the Authorizations > My current approvals page, users with this authorization can view the list of approvals and their status. From the Authorizations > My approval history page, users with this authorization can view the latest answered requests, their status, and who answered the requests.



Right	Description
Modify	To grant this level of right, Manage Authorizations must be set to View or Modify. This level of authorization grants the View rights and the following additional rights: From the Authorizations > My current approvals page, users with this authorization can approve or reject approval requests, and access more details. From the Authorizations > My approval history page, users with this authorization can also access more details for the answered request, comment, and cancel a request.

**Note:**

You must at least grant the **View** right on **Target groups** and **User groups** features when setting rights to manage authorizations or approvals.

User profiles

This feature manages access to the following pages in the web interface:

- **Users > Profiles**
- **Import/Export > CSV**

Right	Description
None	All related menu entries are hidden.
Modify	From the Users > Profiles page, users with this authorization can: • create new custom profiles. • view existing profiles, whether they are default or custom. However, only if these profiles have the same or less rights than the authenticated user. For example, a user without any right on the Session audit feature cannot see profiles with rights on that feature. • edit profile under the following conditions: the authenticated user can view the profile, the profile is custom and editable, and that profile does not apply to the authenticated user. • delete profiles under the following conditions: the authenticated user can view the profile, the profile is custom, and that profile does not apply to the authenticated user. From the Import/Export > CSV page, users with this authorization can import and export files for the Profiles data type.



Settings

This feature manages access to the following pages in the web interface:

- **Configuration > Configuration options**
- **Configuration > Time frames**
- **Configuration > External authentications**
- **Configuration > Authentication domains**
- **Configuration > Notifications**
- **Configuration > Local password policy**
- **Configuration > Connection messages**
- **Configuration > X509 configuration > Certificates**
- **Configuration > X509 configuration > CRL**
- **Configuration > X509 configuration > OCSP**
- **Configuration > Certificate Authorities**
- **Configuration > License**
- **Configuration > Encryption**
- **Import/Export > CSV**

Right	Description
None	All related menu entries are hidden.
View	From any listed page of the Configuration menu, users with this authorization can view information and configuration. From the Import/Export > CSV page, users with this authorization can export files for the Authentication domains data type.
Modify	This level of authorization grants the View rights and the following additional rights: From any listed page of the Configuration menu, users with this authorization can also modify information and configuration. From the Import/Export > CSV page, users with this authorization can also import files for the Authentication domains data type.

System settings

This feature manages access to the following pages in the web interface:

- **System > Network**
- **System > Time service**
- **System > Remote storage**
- **System > SIEM integration**
- **System > SNMP**
- **System > SMTP server**
- **System > Service control**



Right	Description
None	All related menu entries are hidden.
Modify	This level of authorization grants the View rights and the following additional rights: From the Import/Export > CSV page, users with this authorization can export and import files for the Authentication domains data type.

Backup/Restore

This feature manages access to the following pages in the web interface:

- **System > Backup/Restore**

Right	Description
None	All related menu entries are hidden.
Execute	Users with this authorization can create a backup file of WALLIX Bastion or restore WALLIX Bastion to a previous state using a backup file.

Credential recovery

This authorization does not manage access to a specific web page. However, it manages access to the Break Glass mechanism.

Right	Description
None	All related menu entries are hidden.
Execute	Users with this authorization can configure the GPG key in their preferences and receive a Break Glass e-mail if the feature is configured.

Target account access

This feature manages access to the following pages in the web interface:

- **My authorizations > Secrets**
- **My authorizations > Sessions**
- **My authorizations > Approval requests**



Right	Description
No	All related menu entries are hidden.
Yes	Users with this authorization can access to the pages and can use the available features such as checking out secrets or launching sessions.

6.1.1.3. Transferable rights

Transferable rights are permissions that profile members can grant to others. These permissions are derived from the rights assigned to the profile. Profile members cannot transfer rights that exceed their own permissions.



Important:

There are two exceptions: **Session audit** and **Target account access**. These can be transferred by profiles with no permission granted on the features.

The **Transferable rights** table appears when the **Modify** right is enabled for any of the following features from the **Rights** section:

- **Users**
- **User profiles**
- **Settings**

Example of transfer limitations

Profile A has the following rights:

- **Modify** on the **Users** feature.
- **View** on the **Settings** feature.
- **None** on the **Credential recovery** feature.

As a result, Profile A can transfer:

- **None**, **View**, or **Modify** right on the **Users** feature.
- **None** or **View** on the **Settings** feature.
- **None** on the **Credential recovery** feature.

Because it exceeds Profile A's own rights, it cannot transfer the **Modify** right on the **Settings** feature or the **Execute** right on the **Credential recovery** feature.

6.1.1.4. Dashboards access

You can select the dashboards which can be viewed by the users with this profile. The list of dashboards displayed on this area is inherited from the authorizations set for your own profile.

The available dashboards are:

Administration

For an overview of the activities on all of WALLIX Bastion.



Audit

For an overview of session activities.

6.1.1.5. Profile limitations

You can set additional limitations to the profile to further restrict access and privileges.

IP limitations

This option ensures that access and authentication to WALLIX Bastion is restricted to approved and trusted sources.

To set this limitation, provide the source IP for which the access is restricted for primary connection. This address can be a single IP address, sub-network mask, or hostname.

User group limitations

This option ensures that rights and privileges are only granted in relation to approved user groups.

To set this limitation, select all user groups on which you want to grant authorizations (view or modify).

Target group limitations

This option ensures that rights and privileges are only granted in relation to approved target groups.

To set this limitation, select all target groups on which you want to grant authorizations (view or modify). You must also define a default group from the list to ensure that profile members always have access to items they create.

Setting limitations on user groups and target groups implies that actions on users and target accounts are restricted to the selected groups.

Advanced configuration

User group and target group limitations can cause a misconfiguration or a misunderstanding of configuration. You must use the feature carefully.

For example, a profile with the **View** right on the **Session Audit** feature can only audit data if the authorization for the session matches the profile limitation. An authorization contains both a user group and a target group. That means, to audit a session, both the user group and the target group in the authorization must be in the lists of selected groups for the profile. If this is not the case, for example if the user group or target group is not included in the profile's list of limitations, then the profile's perimeter is not respected and the auditor is unable to audit the session.



Attention:

If **Target account access** is set to **Yes** for the profile, you must not define limitations for the profile. It can lead to functional inconsistencies.

6.1.2. Default permission profiles

WALLIX Bastion comes with predefined permission profiles to make it easier to delegate access and rights. To guarantee that all rights remain secure and that no configuration is compromised, default profiles are set to read-only, meaning they cannot be edited. They also cannot be deleted.



If default profiles ensure a level of standard security in the distribution of privileges, not all default profiles are mandatory to use on WALLIX Bastion. However, WALLIX recommends their use when applicable.

Presentation of default profiles

Each default profile serves a dedicated purpose and should be assigned to WALLIX Bastion users depending on their role inside WALLIX Bastion.

approver

The role of an approver is to accept or reject approval requests from users wanting to access targets.

Configuration

This profile has the **Modify** right for the **Manage Approvals** feature.

auditor

The role of an auditor is to view live sessions, but also to consult the session history in the WALLIX Bastion audit data. However, they cannot access the targets themselves.

Configuration

This profile has the **View** right for the **Session audit** feature.

This profile has access to the **Audit** dashboard.

operation_administrator

The role of an operation administrator is to manage users and targets. They also have access to some appliance-level configuration options, such as notifications, time frames, authentication methods, etc.

Configuration

This profile has the **Modify** right for the following feature rights:

- **Users**
- **User groups**
- **Target & accounts**
- **Target groups**
- **Manage Authorizations**
- **Manage Approvals**
- **User profiles**
- **Settings**

This profile has the **Execute** right for the **Credential recovery** feature.

This profile has access to the **Administration** dashboard.

product_administrator

A product administrator, also called super administrator, has the highest privileges on WALLIX Bastion. It has access to and can use any feature, it can also connect to target accounts. This profile is also the only profile allowed to create API keys and to assign the **product_administrator** or the **system_administrator** profile to other users.

You should restrict this profile to limited usage.

Configuration



This profile has the **View** right for the **Session audit** and **System audit** features.

This profile has the **Modify** right for the following features:

- **Users**
- **User groups**
- **Target & accounts**
- **Target groups**
- **Manage Authorizations**
- **Manage Approvals**
- **User profiles**
- **Settings**

This profile has the **Execute** right for the **Backup/Restore** and the **Credential recovery** features.

This profile has the **Yes** option for the **Target account access** feature.

This profile has access to both **Administration** and **Audit** dashboards.

system_administrator

The role of a system administrator is to manage the interaction between WALLIX Bastion and the infrastructure. It can change the appliance configuration, access the console to create and restore backups, and view all the system logs. However, this profile cannot access functional configuration or use target accounts.

Configuration

This profile has the **View** right for the **System audit**.

This profile has the **Modify** right for the **System settings** feature.

This profile has the **Execute** right for the **Backup/Restore** feature.

user

The role of users is to launch sessions or retrieve the secrets of a target account. This profile has no administration rights or features.

Configuration

This profile has the **Yes** option for the **Target account access** feature.

wallix_access_manager_audit

This profile is dedicated to API access to WALLIX Bastion from WALLIX Access Manager.

It provides the ability to leverage the WALLIX Bastion API endpoints related to viewing live sessions and reviewing the sessions history.

Configuration

This profile has the **View** right for the **System audit**.

wallix_access_manager_session

This profile is dedicated to API access to WALLIX Bastion from WALLIX Access Manager.



It provides the ability to leverage WALLIX Bastion API endpoints related to accepting and rejecting approval requests from users who want to access target accounts as well as accessing targets.

Configuration

This profile has the **Modify** right for the **Manage Approvals**.

This profile has the **Yes** option for the **Target account access** feature.

wallix_access_manager_session_audit

This profile is dedicated to API access to WALLIX Bastion from WALLIX Access Manager.

It provides ability to leverage WALLIX Bastion API endpoints related to viewing live sessions and reviewing the sessions history, and related to accepting and rejecting approval requests from users who want to access target accounts as well as accessing targets.

Configuration

This profile has the **View** right for the **System audit** feature.

This profile has the **Modify** right for the **Manage Approvals**.

This profile has the **Yes** option for the **Target account access** feature.



Important:

WALLIX Access Manager allows the use of only one API key. As default profiles, depending on the privileges you require, you can choose between:

- **wallix_access_manager_audit** (for only audit requirements)
- **wallix_access_manager_session** (for only session management requirements)
- **wallix_access_manager_session_audit** (for both audit and session management requirements)

6.1.3. Create a custom permission profile

About this task



Tip:

For more information on all parameters and options available for a profile, refer to [Permission profile overview \(on page 23\)](#).

Procedure

1. Go to the **Users > Profiles** page.
2. Click **Add a profile**.
3. Give this new custom permission profile a name.

Use a recognizable name as this name appears in WALLIX Bastion when selecting profiles.

4. Define the profile type.
 - **Editable**
 - **Read-only** (mandatory for API keys).



5. Decide which rights are authorized for this custom profile.
6. **Optional:** If you set either one of the **Users**, **User profiles**, **Settings** features to **Modify**, you can define transferable rights.
7. **Optional:** Authorize access to dashboards for this profile.
8. If necessary, apply limitations to the profile.
 - **IP limitations:** limit the connection to an IP address, a subnet, or a hostname.
 - **User group limitations:** limit rights to a specific list of user groups.
 - **Target group limitations:** limit rights to a specific list of target groups. If you add this limitation, you must also select a group from the **Default group for target accounts** drop-down to ensure that an authorized target group is always selected.



Important:

Do not set the limitation to **Yes** without selecting user or target groups otherwise this profile has rights but no visibility on any group.

9. Click **Apply**.

6.1.4. Export custom permission profiles

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** and the **List separator** from the drop-down lists.

The separator values must differ.

3. Select **Profiles** from the **Data** options.
4. Select the desired **Archive type**.

To import the file in WALLIX Bastion at a later time, the type must be csv.

5. Click **Export**.

6.1.5. Import custom permission profiles

About this task

You can import custom permission profiles directly using a .csv file. WALLIX Bastion performs the following operations depending on the situation:

1. If a custom profile listed in the .csv file does not already exist in WALLIX Bastion, that profile is created.
2. If a custom profile listed in the .csv file already exists in WALLIX Bastion, any conflicting configuration information is overwritten by the .csv file. The only exception is the value for the profile type, which cannot be modified if set to read-only.
3. If a custom profile exists in WALLIX Bastion but is not listed in the imported .csv file, no changes are made to that profile.



Tip:

For more information on all parameters and options available for a profile, refer to [Permission profile overview \(on page 23\)](#).



Before you begin

The CSV file must begin with a line containing the `#wab1040 profile` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each parameters requires the following configuration:

Field	Type	[R]equired [O]ptional	Description and expected values
Name	Text	R	This value configures the name of the custom permission profile. The expected values are: [aA-zZ], [0-9], '-', '_'
Description	Text	O	This value configures the description of the custom permission profile. The expected values are: Free text
Editable	Boolean	R	This defines the profile type of the custom permission profile. The expected values are: <code>True</code> (Editable) or <code>False</code> (Read only) Default value: <code>True</code> If the value is set to <code>False</code>, it cannot be changed to <code>True</code>.



Field	Type	[R]equired [O]ptional	Description and expected values
Rights	Text	R	This value defines the list of features right that you want to authorize for the profile members. The expected values are: ☐: none ☒: right to View ☒: right to Modify ☒: right to Execute These rights are to be defined in compliance with the order of the WALLIX Bastion web interface features list displayed for a given profile. The following list details the features in the appropriate order and their possible values: • Session audit ('-', 'r') • System audit ('-', 'r') • Users ('-', 'r', 'w') • User groups ('-', 'r', 'w') • Targets & accounts ('-', 'r', 'w') • Target groups ('-', 'r', 'w') • Manage Authorizations ('-', 'r', 'w') • Manage Approvals ('-', 'r', 'w') • User profiles ('-', 'w') • Settings ('-', 'r', 'w') • System settings ('-', 'w') • Backup/Restore ('-', 'x') • Credential recovery ('-', 'x')
Access to device	Boolean	R	This value defines if this profile gives access to target accounts. The expected values are: True or False Default value: False
IP limitations	IP/ subnet/hostname	O	The expected values are: [aA-zZ], [0-9], '-', '/', '.' For example, for a subnet, you can enter 1.1.1.0/24. There can be either no network address or a single address.
Limitations on user group	Boolean	R	The expected values are: True or False Default value: False



Field	Type	[R]equired [O]ptional	Description and expected values
User groups	Text	O	User groups defined There can be no user group, or one or several user groups defined.
Limitations on target group	Boolean	R	The expected values are: True or False Default value: False
Target groups	Text	O	Target groups defined There can be no target group, or one or several target groups defined.
Default target group	Text	O	Default target group defined
Transferable rights	Text	O	This value defines rights transferable by the profile members. The expected values are: ☐: none - r: right to View - w: right to Modify - x: right to Execute These rights are to be defined in compliance with the profile rights specified in the "Rights" column. List of the features in the appropriate order and possible rights for each: • Session audit ('-', 'r') • System audit ('-', 'r') • Users ('-', 'r', 'w') • Targets & accounts ('-', 'r', 'w') • Manage Authorizations ('-', 'r', 'w') • Manage Approvals ('-', 'r', 'w') • User profiles ('-', 'w') • Settings ('-', 'r', 'w') • System settings ('-', 'w') • Backup/Restore ('-', 'x') • Credential recovery ('-', 'x')



Field	Type	[R]equired [O]ptional	Description and expected values
Dashboards	Text	O	Selected dashboards for the profile. The expected values are: • opsadmin for the administration dashboard • audit for the sessions audit dashboard • both opsadmin & audit • none

Procedure

1. To make sure you have the right CSV syntax, export the current list of custom profiles.

For more information, refer to [Export custom permission profiles \(on page 38\)](#).

2. Edit the CSV file to add new custom profiles or modify the configuration of existing profiles and save.
3. Go to the **Import/Export > CSV** page.
4. Select your preferred **Field separator** and **List separator** from the drop-down lists.

The separator values must differ. If you exported the CSV file as recommended, use the same separator values.

5. Select **Profiles** from the **Data** options.
6. Retrieve the CSV file from your computer.
7. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of profiles created and updated, but also the rejected data.

If you are attempting to save modifications to a read-only profile, the profile causes an error explaining it has not been successfully saved.

In case of rejection, the corresponding error is detailed with the line number for the csv. For example, you can have missing values for a field or invalid feature rights for the profile X at line X. You can modify the csv file and re-import the modified file.

6.1.6. Edit a custom permission profile

About this task



Attention:

Read-only profiles cannot be edited.

Procedure

1. Go to the **Users > Profiles** page.
2. Click the name of the custom profile that you want to edit.
3. Edit the necessary information.



The name of a custom profile cannot be modified.

4. Click **Apply**.

6.1.7. Delete a permission profile

About this task



Attention:

Default profiles cannot be deleted.

You cannot delete a profile if at least one user, user group, or API key is linked to this profile.

Procedure

1. Go to the **Users > Profiles** page.
2. Select the profiles that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion of all the selected profiles.

6.2. User groups

The **Users > Groups** page allows you to:

- list declared user groups
- add/edit/delete a group
- view the number of local users in each user group
- view the profile of users in the user group



Note:

On this page, the administrator only sees the profiles defined for the group. The profile column corresponds to the profile attributed to mapped users and not to local users. For more information, refer to [Permission profiles \(on page 22\)](#).

6.2.1. Add a user group

Procedure

1. Go to the **Users > Groups** page.
2. Click **Add a group**.
3. Give the new group a name and optionally add a description.
4. Select one or more time frames that apply to this new group.

If several time frames are selected, the time frame applied is the combination of all the selected times frames. By default, the `allthetime` time frame is selected.

5. Compose the group of users in the **Local users** zone,
 - To add users: double-click the name of a user from the **Available** column to move it to the **Selected** column. You can also perform a multi-selection by clicking several users from the **Available** column and clicking **>** to move them to the selection.
 - To remove users: double-click the name of a user from the **Selected** column to put it back in the **Available** column. You can also perform a multi-selection by clicking several users from the **Selected** column and clicking **<** to remove them from the selection.



You can search for a user by name in the search field.

6. **Optional:** Select a language for the e-mail notifications sent to this group.

The language is English by default.

7. **Optional:** Specify a list of e-mail addresses or a mailing list of recipients who must receive approval notifications.

Entering a mailing list simplifies the configuration or the update of the list of the approval notification recipients

8. Click **Apply** to create the user group.

9. Switch to the **Mappings** tab.

10. Set the profile to apply to users in this group.

11. In case of LDAP, AD, Azure AD, or other IdP integration, the domain mapping allows to set the profile of the user group members.

12. **Optional:** Switch to the **Restrictions** tab to create one or more rules to specify one or more actions to apply when certain character sequences are detected in the upward flow from proxies.

Character sequence detection is only enabled for data sent by the client to the server and only for connections under specific protocols (available in the list from the **Subprotocol** field).

- Click **Add**.
- Choose the **Action** type.
- Set the **Rule**.
- Specify the **Subprotocol**.
- Click **Apply and close**.

6.2.2. Import user groups

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the #wab1040 usersgroup tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(equired) O(ptional)	Possible values
Name	Text	R	Group name. [aA-zZ], [0-9], '-', '_'
Description	Text	O	Group description. Free text.

Field	Type	R(equired) O(ptional)	Possible values
Profile	Text	O	Profile for users in this group. Profiles defined.
Timeframes	Text	R	Authorized timeframes for the group. Time frames defined. There can be several time frames for the same user group.
Users	Text	O	Users who are group members. Users defined. There can be no user or one or several users defined.
Language	Text	R	Language for approval notifications. For example, <code>en</code> , <code>fr</code> , <code>de</code> . By default, it is <code>en</code> .
Email list	Text	O	Email list for approval notification recipients, separated by a semicolon (;). For example, <code>leaddevs@acme.com;seniordevs@acme.com</code> .

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **User groups** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

6.2.3. Edit a user group configuration

About this task



Note:

The administrator cannot view the area **LDAP authentication mapping** when the profile mapped to the group has at least one permission that the administrator's profile cannot grant as a transferable right. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Users > Groups** page.
2. Click the name of the group that you want to edit.
3. Click **Edit this group**.
4. Modify the necessary information.
5. Click **Apply**.

6.2.4. Manage members of a user group

About this task



Note:

The administrator cannot view the area **LDAP authentication mapping** when the profile mapped to the group has at least one permission that the administrator's profile cannot grant as a transferable right. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Users > Groups** page.
2. Click the name of the group that you want to edit.
3. Click **Edit this group**.
4. Modify the list of members,
 - To add users: double-click the name of a user from the **Available users** column to move it to the **Selected users** column. You can also perform a multi-selection by clicking several users from the **Available users** column and clicking **>** to move them to the selection.
 - To remove users: double-click the name of a user from the **Selected users** column to put it back in the **Available users** column. You can also perform a multi-selection by clicking several users from the **Selected users** column and clicking **<** to remove them from the selection.

You can search for a user by name in the search field.



Tip:

You can select or remove all users for either column.

5. Click **Apply**.

6.2.5. Delete user groups

About this task



Attention:

It is not possible to delete a user group linked to active authorizations (refer to [Authorizations \(on page 189\)](#)).

Procedure

1. Go to the **Users > Groups** page.
2. Select one or more user groups.
3. Click **Delete selected groups**.
4. Confirm the permanent deletion all of the selected user groups.

6.3. Control Local and LDAP/AD users access

About this task

You can access a list of user accounts filtered either on the local domain or on any configured LDAP/AD domain. If you filter on an LDAP or Active Directory domain, WALLIX Bastion shows users from the directory mapped with a user group.

Procedure

1. Go to the **Users > Accounts** page.
2. Select the domain you are interested in from the **Display users on domain** drop-down list.



Tip:

You can increase the number of users displayed in the table, and for local users you can also sort user accounts by column values.

3. For all local user accounts, some information is directly displayed (not available for LDAP/AD users).
 - In the **Profile** column, the key icon () identifies users with a permission profile that grants them the **Credential recovery** right. For more information, refer to [Permission profiles \(on page 22\)](#).
 - In the **Status** column, the icon identifies the account current state.
 - The tick icon () identifies users with an active account.
 - The lock icon () identifies users with too many authentication failures. For more information, refer to [Unlock local user accounts \(on page 90\)](#).
 - The hourglass icon () identifies users with an expired account.
 - The warning icon () identifies users with a disabled account.
4. From the list of all user accounts, click the name of the account you interested in to access its summary. From the summary page, you can also expand several sections from to get more information about access and rights.
 - **Rights on GUI** lists the level of authorization for interface features, and indicates if this user has network limitations and target account access.
 - **Authorizations on devices** lists which devices are available to this user.
 - **Authorizations on applications** lists which applications are available to this user.
 - **Authorizations on accounts** lists which target accounts are available to this user.



Note:

For **Authorizations on devices** and **Authorizations on applications**, click the icon at the beginning of a line to download the configuration file to establish a connection.



7. User accounts management

7.1. General information

This section explains and details all available authentication and authorization protocols for WALLIX Bastion user accounts.

Introduction

In WALLIX Bastion, accounts do not always match a unique individual but rather match a set of permissions. That means one individual can have access to several accounts. For example, for an individual tasked to administrate WALLIX Bastion but also requires access to targets, WALLIX recommends creating two separate accounts. Another example is the use of a service account, if an administrator with all privileges exists in WALLIX Bastion, that account can be used by different individuals.

This is done because an account contains details like username, e-mail, but also a designated profile which provides permissions, possible group memberships, and possible restrictions. That way, one individual can have different accounts which manage different aspects of their tasks. However, it can happen that one individual has one account, if they have only one task to achieve.

Authentication and authorization

Each account has a source type and WALLIX Bastion supports importing users from various sources. For instance, accounts created directly in WALLIX Bastion are local users, while those imported from Active Directory are of the AD type.

As a reminder, authentication involves verifying a user's identity, typically through credentials such as passwords, to confirm they are who they claim to be. Authorization defines what actions an authenticated user can perform in WALLIX Bastion, such as accessing specific resources or executing certain tasks. In short, authentication confirms identity, while authorization grants permissions.

In WALLIX Bastion, the first authentication also assumes the authorization check. If there is a secondary authentication, no authorization check is performed.

7.1.1. Overview of authentication protocols

WALLIX Bastion supports several authentication protocols. However, with WALLIX Bastion, users have access to three different network protocols: HTTPS with the web interface, and SSH and RDP with dedicated clients.

Each network protocol has particularities in relation to the authentication protocols users have access to. The available authentication protocols for each network protocol are detailed in the following table.

Authentication protocols availability

The following matrix details which authentication protocols are available for each network protocol.



Authentication protocols		Network protocols		
		HTTPS	SSH	RDP
Login and password	Kerberos-Password	✓	✓	✓
	LDAP/AD bind password	✓	✓	✓
	Local password	✓	✓	✓
	RADIUS	✓	✓	✓
	TACACS+	✓	✓	✓
Kerberos Ticket (standard)		✓	✓	✗
OIDC		✓	! 1	! 1
PingID		✓	✓	✓
SAML		✓	! 1	! 1
SSH Key and SSH CA		✗	✓	✗
X.509 certificate		✓	! 2	! 2

¹ The authentication protocol is supported, but the workflow is not fully integrated. Users attempting to authenticate using this protocol are required to copy a provided link and paste it into a web browser to retrieve a token. Then, users must add the token to the client.

² The authentication protocol is supported, but the workflow is not fully integrated. Users must first authenticate using the HTTPS network protocol and while authenticated, users can open the client and confirm the request to authenticate on the client.

One-Time Password

WALLIX Bastion also offers a One-Time Password (OTP) authentication method. When users are authenticated to the web interface, no matter their authentication protocol, they can connect to their SSH or RDP client using a token. This token is only valid one time and allows WALLIX Bastion to recognize and identify the user.



The token is automatically added when users download a session file for a SSH session (🔑 One-Time password, limited in time), or an RDP session (💻 One-Time password, limited in time) from the **My authorizations > Sessions** page.

7.1.2. Overview of authorization protocols

Access to WALLIX Bastion is granted differently depending on where user identities exist.

- Locally: user identities exist directly inside WALLIX Bastion. As a consequence, user access is managed and verified internally.
- Externally: user identities exist outside of WALLIX Bastion. As a consequence, user access is managed outside of WALLIX Bastion and is verified against the outside source with one of the following authorization protocols:
 - LDAP/AD
 - OIDC
 - SAML

7.1.3. Overview of Multi-Factor Authentication

With WALLIX Bastion, you can setup a single-factor authentication (SFA) and a two-factor authentication (2FA). However, it is not possible to directly configure a multifactor authentication (MFA).

If you require more than a two-factor authentication, WALLIX recommends that you configure MFA directly inside your identity and access management solution. Users connecting to WALLIX Bastion must comply with the configured authentication procedure, meaning that if their IdP implements an MFA, that MFA is requested from users to access WALLIX Bastion. For example, RADIUS or Microsoft Entra can be used for MFA.

7.1.4. Setup recommendations

Authentication protocols	Description
Kerberos Password	Kerberos Password is an authentication protocol for LDAP/AD. To manage authorization, you must pair it with an LDAP/AD directory. If you implement this authentication method, you should configure it as a primary authentication for users.
Kerberos Ticket	Kerberos ticket is an authentication protocol for LDAP/AD. To manage authorization, you must pair it with an LDAP/AD directory. If you implement this authentication method, you should configure it as a primary authentication for users.
LDAP/AD bind password	Bind password is an authentication protocol for LDAP/AD. To manage authorization, you must pair it with an LDAP/AD directory. If you implement this authentication method, you should configure it as a primary authentication for users.



Authentication protocols	Description
Local password	Local password is an authentication protocol for local users. To manage authorization, it is by default paired with the WALLIX Bastion user database. If you implement this authentication method, you should configure it as a primary authentication for users.
OpenID Connect	OIDC is a self-contained authentication and authorization protocol. If you implement this method, you should configure all authentication and authorization requirements on the provider side.
PingID	PingID is an authentication protocol for either LDAP/AD or local users. To manage authorization, you must pair it with an LDAP/AD directory or rely on the WALLIX Bastion user database for local users. If you implement this method, you should either: • configure it as the only authentication method for local users • configure it as a secondary authentication method for LDAP/AD users
RADIUS	RADIUS is an authentication protocol for either LDAP/AD or local users. To manage authorization, you must pair it with an LDAP/AD directory or rely on the WALLIX Bastion user database for local users. If you implement this method, you should either: • configure it as the only authentication method for local users • configure it as a secondary authentication method for LDAP/AD users
SAML	SAML is a self-contained authentication and authorization protocol. If you implement this method, you should configure all authentication and authorization requirements on the provider side.
SSH Key and SSH CA	SSH Key is an authentication protocol for either LDAP/AD or local users. It is reserved to SSH connections. To manage authorization, you must pair it with an LDAP/AD directory or rely on the WALLIX Bastion user database for local users. If you implement this authentication method, you should configure it as a primary authentication for users. In case of LDAP/AD users, the SSH CA authentication protocol is also available.

Authentication protocols	Description
TACACS+	TACACS+ is an authentication protocol for either LDAP/AD or local users. To manage authorization, you must pair it with an LDAP/AD directory or rely on the WALLIX Bastion user database for local users. If you implement this method, you should either: • configure it as the only authentication method for local users • configure it as a secondary authentication method for LDAP/AD users
X.509 certificate	X.509 certificate is an authentication method for LDAP/AD or local users. To manage authorization, you must pair it with an LDAP/AD directory or rely on the WALLIX Bastion user database for local users.

7.2. Directory Services users

Introduction to Directory identities

Directory identities are users imported to WALLIX Bastion from a directory service. That means their identity type is LDAP or AD.

Conditions for Displaying Users

Local users are always displayed.

Through a directory service:

- LDAP, AD, and Azure AD users are only displayed in the WALLIX Bastion when a specific user query is made for a given domain.
- Other users are not displayed.



Important:

When you delete local, LDAP, AD, or Azure AD users, they no longer appear in the user list, and cannot access the system after logging out. If you modify these users, changes are valid from the user's next connection.



Note:

Only IAG service allows displaying the full list of users allowed to access the WALLIX Bastion.

About Directory user accounts

WALLIX Bastion provides four authentication methods for Directory Services identities:

- Login/password bind
- X.509 certificate
- Kerberos Ticket
- Kerberos Password
- RADIUS
- TACACS+

7.2.1. Connect to an Active Directory server



Note:

The minimum version for the Active Directory server is Windows Server 2008 R2.

Protected User Groups specifications

Protected Users are a security group for Active Directory which enhances protection measures against credential theft. This type of users can only authenticate to WALLIX Bastion using the Kerberos Ticket authentication.

To ensure that everything is correctly setup for this type of user, you must configure [Kerberos Ticket authentication \(LDAP/AD\) \(on page 63\)](#) as an authentication method and follow the [Connect to an Active Directory server \(on page 53\)](#) procedure.

7.2.1.1. Add an Active Directory external authentication

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **Active Directory**.
3. Give this Active Directory a recognizable name.
4. Specify the server address of the Active Directory. You can use an IP address or FQDN.
5. Specify the port number of the server. The default port is 389.
6. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 30 seconds.



CAUTION:

This timeout applies to any new LDAP external authentication. The LDAP external authentications inherited from an earlier version of WALLIX Bastion keep the former timeout value defined.

7. Set the appropriate encryption protocol. The connection port is then updated depending on the selection.
 - If **None**, skip to the next step.
 - If **StartTLS** or **SSL**, upload the **CA certificate**. The authenticity of the certificate is compared with the LDAP server certificate during the connection. The hostname



specified in the **Server** field must be identical to the one entered in the **CN** field of the certificate to be valid.



Tip:

Setting either **StartTLS** or **SSL** protocol is necessary to allow user to reset their password. For more information, refer to [Activate Password reset \(on page 57\)](#).

8. **Optional:** Provide a description of this Active Directory to simplify management.
9. Enable **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, user@domain) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

10. Click **Test network parameters** to test the configuration. You can cancel the test at any time.
11. In the **Authentication** section, you must configure the service account information depending on your preferred bind method.



Important:

The SASL bind method based on GSS-API must be selected when users are part of the Protected Users group.

- If you select **anonymous**, there is no element to provide. You can skip to the next step.
- If you select **simple (password)** or **GSS-API**, provide the user name and related password to use to search for the WALLIX Bastion user name in the directory.



Note:

The user must have read rights for the base DN used.

- If you select **simple (client certificate)** (available only if there is an encryption protocol set up), provide the client certificate and client key files (PKCS#12). After the files are uploaded, a passphrase can be provided for the certificate on the dedicated field. The authenticity of the certificate is compared with the CA certificate during the connection.
12. Click **Test authentication** to test the configuration. You can cancel the test at any time.
 13. In the **User attributes** section, you must configure how to read the Active Directory.
 - a. Enter the **Base DN** depending on the domain name. For example, for the domain mycorp.lan, the base DN is dc=mycorp,dc=lan..
 - b. Specify the **Login attribute** used for the connection.

By default, this connection attribute corresponds to sAMAccountName.

If the email domain and authentication domain configured on the authentication domain side are different, you can use the mail attribute instead. This allows users associated with this authentication to use their e-mail when logging into the web interface. The following login formats are supported:



- `jdoe@mycompany.com@domain`. The format is `login@domain` with the e-mail defined as `login` (for example, `jdoe@mycompany.com`)
- `domain\\jdoe@mycompany.com`. The format is `domain\\login` with the e-mail defined as `login` (for example, `jdoe@mycompany.com`)
- `jdoe@mycompany.com` with the domain defined as the default LDAP/AD domain

- c. Specify the **User name attribute**. It must be the name of the AD attribute where the WALLIX Bastion user name is stored. By default, it corresponds to `sAMAccountName`.



Important:

Due to an Active Directory limitation, the `sAMAccountName` attribute must be up to 20 characters long and cannot contain the following characters: `"/\[]:;|=, +*? <>.`

14. Click **Apply**.

7.2.1.2. Add an Active Directory authentication domain

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Click **Add** and click **Active Directory**.
3. Give this Active Directory a recognizable name.
4. In **Domain server name**, provide a name for the domain inside WALLIX Bastion.
5. In **Authentication domain name**, enter the Active Directory domain name.

If you want to implement the Kerberos Ticket authentication, this name must exactly match the Kerberos realm.

6. If you want to use this domain as the default one, activate **Default domain**.

It allows stripping the domain part (that is `@acme.com` from the previous example) from the login when users authenticate to WALLIX Bastion. That means users defined in WALLIX Access Manager can be mapped to users in the Bastion.

One default domain should be defined in WALLIX Bastion.

7. For **Directory**, select the external authentication previously configured. For more information, refer to [Add an Active Directory external authentication \(on page 53\)](#).

WALLIX does not recommend selecting multiple directories. Configuring one with the correct setup for the server is preferred as AD automatically looks for the directory that is both active and closest to the user's geographical location.

If you select several directories, their configuration must be exact replicates. Directories are used in the specified order, one after the other, until the server responds. This allows resilience in case of a directory server failure. You can use a maximum of 3 directories, as the maximum response time before a timeout corresponds to 3 directory failures.

8. **Optional:** If required, select other authentication methods as a secondary means of authentication.

If you select several authentication methods, they are used one after the other, according to the defined order.

9. **Optional:** Provide a description of this Active Directory to simplify management.
10. From the **User attributes** section, configure the mapping between your Active Directory attributes and WALLIX Bastion parameters.



- a. For **Group attribute**, enter the attribute that matches user group membership in your AD.

The default value is `memberOf` for an AD server. However, it is possible to manage recursive groups. To do so, replace the default value with the following query.

```
(&(ObjectClass=group)(member:1.2.840.113556.1.4.1941:=${distinguishedName}))
```

This query can be slower than the default configuration.

- b. For **Display name attribute**, enter the attribute that matches the names you want to display in WALLIX Bastion.
 - c. For **Email attribute**, enter the attribute that matches the user e-mails.
 - d. For **Default email domain**, enter the fallback domain component to use if the **Email attribute** is empty for the authenticating user. This e-mail address for these users is built by prefixing that default domain with their user name.
 - e. For **Language attribute**, enter the attribute that contains the user language.
 - f. For **Default language**, set the language for users whose language is not defined in the directory.
11. For authentication,
 - If you want to allow SSH Key authentication, refer to [SSH Key authentication \(LDAP/AD\) \(on page 67\)](#).
 - If you want to allow X.509 certificate authentication, refer to [X.509 certificate authentication \(LDAP/AD\) \(on page 69\)](#).
 - If you want to allow SSH Certificate, refer to [SSH Certificate authentication \(LDAP/AD\) \(on page 68\)](#).
 12. Click **Apply**.
 13. Go to **Configuration > Configuration options > Global**.
 14. Show **Advanced options**.
 15. For **Ldap attributes**, enter the **Group attribute** previously configured (`memberOf` by default).

You can also set the value to `*` to retrieve all the attributes, but the performance of WALLIX Bastion can be affected.

16. Click **Apply**.

7.2.1.3. Add Active Directory group mappings

About this task

A mapping links your Active Directory groups to WALLIX Bastion groups.

Administrators cannot view mappings whose profiles have at least one permission that the administrator's profile cannot grant as a transferable right. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Edit the Active Directory authentication domain of your choice.
3. Switch to the **Mappings** tab and click **Add**.
4. Select user group created on WALLIX Bastion from the **User group** drop-down list.
5. Select a profile created on WALLIX Bastion from the **User group profile** drop-down list.



6. **Optional:** If you want to set the selected WALLIX user group and profile as default for all AD users that do not match another group mapping, activate **Default group for users without group in this domain**.

Having a default group ensures that all users from your Active Directory can access WALLIX Bastion.

7. In **Group**, enter the Distinguished Name (DN) for the Active Directory group that you want to match.

The input is case insensitive.

For example, the following DN matches users that belong to both IT and London user groups inside the corp.acme.com domain.

```
OU=IT,OU=London,DC=corp,DC=acme,DC=com
```

8. Click **Add and continue** to save and add another group mapping or click **Add and close** if you are done.

What to do next

Configure the approver group by specifying the **Language** and **Email list** fields (refer to [User groups \(on page 43\)](#)) to allow the approver to be notified by e-mail of the approval requests.



Tip:

Group mappings can also be edited on the user group modification page (refer to [User groups \(on page 43\)](#)).

7.2.1.4. Activate Password reset

You can request users to reset their passwords when they log in to WALLIX Bastion or when they establish an RDP or SSH session.

Procedure

1. Go to the **Configuration > Configuration options > Global** page.
2. Under the **[main]** section, activate the **AD user password change** option.
3. Click **Apply**.
4. Go to the **Configuration > External authentications** page.
5. Click the desired Active Directory external authentication and ensure that the **Encryption** protocol is set to either **StartTLS** or **SSL**. If not, change the value to one of the two protocols and click **Apply**.

7.2.2. Connect to an LDAP server

Solutions which communicate with or host directory services with the LDAP protocol can be configured in WALLIX Bastion to retrieve users. For example, OpenLDAP, SaMBa-LDAP, 389 Directory Server, IBM Security Directory Server, Okta Cloud Identity, etc.



Note:

To use Okta Identity Cloud as an LDAP domain, make sure to set these three parameters, in **Configuration > Configuration options > Global** under the **main** section, as follows:

- the **Ldap attributes** parameter must correspond to **dn**
- the **Ldap partial search** parameter must be checked
- the **Ldap bind login** parameter must be unchecked

These parameters are displayed when the check box of the **Advanced options** field at the top right of the page is selected. These parameters must only be changed when instructed by the WALLIX support team.

7.2.2.1. Add an LDAP external authentication

About this task



Important:

If you require the GSS-API bind mechanism, you must instead configure an Active Directory external authentication. For more information refer to [Add an Active Directory external authentication \(on page 53\)](#).

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **LDAP**.
3. Give the LDAP authentication a name.
4. Specify the server address of the Directory. You can use an IP address or the FQDN.
5. Specify the port number of the server. The default port is 389.
6. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 30 seconds.



CAUTION:

This timeout applies to any new LDAP external authentication. The LDAP external authentications inherited from an earlier version of WALLIX Bastion keep the former timeout value defined.

7. Set the appropriate encryption protocol. The connection port is then updated depending on the selection.
 - If **None**, skip to the next step.
 - If **StartTLS** or **SSL**, upload the **CA certificate**. The authenticity of the certificate is compared with the LDAP server certificate during the connection. The hostname specified in the **Server** field must be identical to the one entered in the **CN** field of the certificate to be valid.
8. **Optional:** Provide a description of this Directory to simplify management.
9. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, user@domain) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

10. Click **Test network parameters** to test the configuration. You can cancel the test at any time.
11. In the **Authentication** section, you must configure the service account information depending on your preferred bind method.
 - If you select **anonymous**, there is no element to provide. You can skip to the next step.
 - If you select **simple (password)**, provide the user name and related password to use to search for the WALLIX Bastion user name in the directory.



Note:

The user must have read rights for the base DN used.

- If you select **simple (client certificate)** (available only if there is an encryption protocol set up), provide the client certificate and client key files (PKCS#12). After the files are uploaded, a passphrase can be provided for the certificate on the dedicated field. The authenticity of the certificate is compared with the CA certificate during the connection.
12. Click **Test authentication** to test the configuration. You can cancel the test at any time.
 13. In the **User attributes** section, you must configure how to read the Directory.

- a. Specify the organization unit Distinguished Name in **Base DN**.
- b. Specify the **Login attribute** used for the connection.

By default, this connection attribute corresponds to `uid`.

If the email domain and authentication domain configured on the authentication domain side are different, you can use the `mail` attribute instead. This allows users associated with this authentication to use their e-mail when logging into the web interface. The following login formats are supported:

- `jdoe@mycompany.com@domain`. The format is `login@domain` with the e-mail defined as login (for example, `jdoe@mycompany.com`)
- `domain\\jdoe@mycompany.com`. The format is `domain\\login` with the e-mail defined as login (for example, `jdoe@mycompany.com`)
- `jdoe@mycompany.com` with the domain defined as the default LDAP/AD domain

- c. Specify the **User name attribute**. It must be the name of the LDAP attribute where the WALLIX Bastion user name is stored. By default, it corresponds to `uid`.

14. Click **Apply**.

7.2.2.2. Add an LDAP authentication domain

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Click **Add** and click **LDAP**.
3. Give this LDAP a recognizable name.
4. In **Domain server name**, provide a name for the domain inside WALLIX Bastion.
5. In **Authentication domain name**, enter the LDAP domain name.

If you want to implement the Kerberos Ticket authentication, this name must exactly match the Kerberos realm.

6. If you want to use this domain as the default one, activate **Default domain**.

It allows stripping the domain part (that is `@acme.com` from the previous example) from the login when users authenticate to WALLIX Bastion. That means users defined in WALLIX Access Manager can be mapped to users in the Bastion.



One default domain should be defined in WALLIX Bastion.

7. For **Directory**, select the external authentication previously configured. For more information, refer to [Add an LDAP external authentication \(on page 58\)](#).

WALLIX does not recommend selecting multiple directories. Configuring one with the correct setup for the server is preferred as LDAP automatically looks for the directory that is both active and closest to the user's geographical location.

If you select several directories, their configuration must be exact replicates. Directories are used in the specified order, one after the other, until the server responds. This allows resilience in case of a directory server failure. You can use a maximum of 3 directories, as the maximum response time before a timeout corresponds to 3 directory failures.

8. **Optional:** If required, select other authentication methods as a secondary means of authentication.

If you select several authentication methods, they are used one after the other, according to the defined order.

9. **Optional:** Provide a description of this LDAP to simplify management.
10. From the **User attributes** section, configure the mapping between your LDAP attributes and WALLIX Bastion parameters.

- a. For **Group attribute**, enter the attribute that matches user group membership in your LDAP.

The default value for an LDAP server is (&(ObjectClass=posixGroup)(memberUid=\${uid})).

This is LDAP query finds groups containing the user defined by their uid. By default, some servers may not support for each account the list of groups to which it belongs. It is then necessary to specify an additional query.

The `${uid}` syntax is specific to the Bastion. The `uid` attribute can be replaced by any user attribute.

If the LDAP server supports the `memberOf` value, its use is then recommended. This is the case with OpenLDAP servers configured with the `memberOf` overlay.

- b. For **Display name attribute**, enter the attribute that matches the names you want to display in WALLIX Bastion.
- c. For **Email attribute**, enter the attribute that matches the user e-mails.
- d. For **Default email domain**, enter the fallback domain component to use if the **Email attribute** is empty for the authenticating user. This e-mail address for these users is built by prefixing that default domain with their user name.
- e. For **Language attribute**, enter the attribute that contains the user language.
- f. For **Default language**, set the language for users whose language is not defined in the directory.

11. For authentication,

- If you want to allow SSH Key authentication, refer to [SSH Key authentication \(LDAP/AD\) \(on page 67\)](#).
 - If you want to allow X.509 certificate authentication, refer to [X.509 certificate authentication \(LDAP/AD\) \(on page 69\)](#).
 - If you want to allow SSH Certificate, refer to [SSH Certificate authentication \(LDAP/AD\) \(on page 68\)](#).
12. Click **Apply**.
 13. Go to **Configuration > Configuration options > Global**.
 14. Show **Advanced options**.
 15. For **Ldap attributes**, enter the **Group attribute** previously configured (memberOf by default).

You can also set the value to * to retrieve all the attributes, but the performance of WALLIX Bastion can be affected.
 16. Click **Apply**.

7.2.2.3. Add LDAP group mappings

About this task

A mapping links your LDAP groups to WALLIX Bastion groups.

Administrators cannot view mappings whose profiles have at least one permission that the administrator's profile cannot grant as a transferable right. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Edit the LDAP authentication domain of your choice.
3. Switch to the **Mappings** tab and click **Add**.
4. Select user group created on WALLIX Bastion from the **User group** drop-down list.
5. Select a profile created on WALLIX Bastion from the **User group profile** drop-down list.
6. **Optional:** If you want to set the selected WALLIX user group and profile as default for all directory users that do not match another group mapping, activate **Default group for users without group in this domain**.

Having a default group ensures that all users from your directory can access WALLIX Bastion.

7. In **Group**, enter the Distinguished Name (DN) for the directory group that you want to match.

The input is case insensitive.

For example, the following DN matches users that belong to both IT and London user groups inside the corp.acme.com domain.

```
OU=IT, OU=London, DC=corp, DC=acme, DC=com
```

8. Click **Add and continue** to save and add another group mapping or click **Add and close** if you are done.

What to do next

Configure the approver group by specifying the **Language** and **Email list** fields (refer to [User groups \(on page 43\)](#)) to allow the approver to be notified by e-mail of the approval requests.



Tip:

Group mappings can also be edited on the user group modification page (refer to [User groups \(on page 43\)](#)).



7.2.3. Import users from an LDAP or AD server

This process involves a one-time import of users from a remote LDAP or AD directory.

About this task

If you only want to replicate a snapshot of your directory into the WALLIX Bastion database, you can import users from an LDAP or AD server using this procedure. However, to include users from a directory and keep them synchronized with any updates, you need to use the group mappings feature. For more information, refer to [Add Active Directory group mappings \(on page 56\)](#) or [Add LDAP group mappings \(on page 61\)](#).

Before you begin



Attention:

If the imported users must authenticate on the directory used for the import, you must first create the authentication method (refer to [Connect to an LDAP server \(on page 57\)](#) or [Connect to an Active Directory server \(on page 53\)](#)).

Procedure

1. Go to the **Import/Export > Users from LDAP/AD** page.
2. Enter the server address (IP or FQDN).
3. Specify the port number of the server. The default port is 389 for StartTLS and 636 for SSL.
4. IF the import is done from an Active Directory, then activate the **Active Directory** option. If the import is from any other LDAP directory, then keep the option deactivated.
5. Select the relevant encryption protocol.

The connection port can change depending on the selected protocol.

6. Enter the **Base DN** depending on the domain name. For example, for the domain mycorp.lan, the base DN is `dc=mycorp,dc=lan`.
7. In **User name attribute**, enter the attribute depending on your needs:
 - `domain_name\SAMAccountName` for an LDAP server
 - `domain_name\uid` for an Active Directory server



Restriction:

Due to an Active Directory limitation, the `sAMAccountName` attribute must be up to 20 characters long and cannot contain the following characters: `/\ [ ] : ; | = , + * ? < >`

8. In **User email attribute**, enter the attribute for the e-mail address of users.
9. In **Search filter**, provide the query allowing to retrieve all the users from the directory.

A query is specified by default. It can be modified to retrieve the appropriate users using AD syntax.

10. Select either the anonymous or the simple bind method.

If you select the **simple** method, you must also enter a user name and a password to use for searching the user name in the directory.

**Note:**

The user must have read rights for the base DN used.

11. Click **Import**.

Results

If the import is successful, a page listing the users extracted from the directory is displayed: choose the users you want to import in WALLIX Bastion by clicking the check box at the beginning of their line. Before final import, you must assign an authentication and a profile to the selected users. A user group and a domain name can also be assigned to the selection. Click **Import** to import data on the user database of WALLIX Bastion.

After the import operation is performed, a summary report is displayed. This report lists the number of users which were created or rejected in the WALLIX Bastion database. In case of rejection, the corresponding error is mentioned.

7.2.4. Authentication protocols for LDAP/AD users

7.2.4.1. Login/password with bind authentication (LDAP/AD)

How to enable Password bind authentication for LDAP/AD users?

All users from an LDAP/AD directory have a password bind authentication by default.

7.2.4.2. Kerberos Ticket authentication (LDAP/AD)

Limitations

WALLIX cannot require users to stop using LDAP bind passwords, meaning it cannot enforce the exclusive use of Kerberos tickets. If a Kerberos ticket is configured on the SSH client or web browser, the Bastion prioritizes it. However, if no Kerberos ticket is configured, the Bastion attempts to log in with the provided credentials. As a result, the Bastion uses this information.

For Protected Users (specific to Active Directory), this means the password is sent through the LDAP/AD channel, which is highly discouraged by Microsoft. Additionally, if LDAP/AD TLS is not used, the password is transmitted over the network unencrypted.

How to enable Kerberos Ticket authentication for LDAP/AD users?

To allow LDAP/AD users to authenticate using Kerberos Ticket, you must create the Kerberos Ticket authentication first and then link that authentication to the domain that contains the users.

Procedure

Create the Kerberos Ticket external authentication.

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **Kerberos**.
3. Give the new authentication method a name.
4. Specify the domain name (or realm).

This name must exactly match the **Authentication domain name** for your LDAP/AD server in WALLIX Bastion.



5. Specify the domain name or the IP address of the KDC server in **Key distribution center**.
6. Specify the port number of the KDC server. By default, the port is 88.
7. Upload to the keytab file used for the service authentication. By default, each uploaded keytab file is merged with the previously loaded files.

If an HTTP service is present in the keytab file, the Kerberos support is activated for authenticating on the interface. This requires adding the iwab suffix to the URL: `https://bastion_ip_address/iwab` OR `https://<bastion_name>/iwab`.

HOST services are used for Kerberos authentication to the SSH proxy. It is then possible to use a **forwardable** ticket to connect to a target in the same Kerberos domain using account mapping (refer to [Add a target account to a global domain \(on page 159\)](#), [Add a target account to a device \(on page 160\)](#) or [Add a target account to an application \(on page 160\)](#)).

8. **Optional:** Enable the **Overwrite the existing keytab** option to overwrite the previously loaded keytab files with the new keytab file.
9. **Optional:** Provide a description of this authentication method to simplify management.
10. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, `user@domain`) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

11. Click **Apply**.

Link the Kerberos Ticket authentication method to the domain.

12. Go to the **Configuration > Authentication domains** page.
13. Edit the LDAP or AD authentication domain or create a new one.
14. In **Secondary authentication**, select the Kerberos Ticket authentication method.
15. Click **Apply**.

7.2.4.3. Kerberos Password authentication (LDAP/AD)

About this task

This authentication is considered by users to be standard authentication (that means entering a login and a password). WALLIX Bastion then acts as a Kerberos client.

Before you begin

For Kerberos-Password authentications, ensure that the Kerberos infrastructure is properly configured to authenticate.

For a Kerberos-Password authenticated user to be acknowledged by WALLIX Bastion, at least one of the following two conditions is required:

- the user is defined locally on WALLIX Bastion, and a Kerberos-Password external authentication is configured for this user
- Kerberos-Password is used as a second factor after first authenticating through LDAP with or without using Active Directory

How to enable Kerberos Password authentication for LDAP/AD users?

To allow LDAP/AD users to authenticate using Kerberos Password, you must create the Kerberos Password authentication first and then link that authentication to the domain that contains the users.

Procedure

Create the Kerberos Password external authentication.



1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **Kerberos-Password**.
3. Give the new authentication method a name.
4. Specify the domain name (REALM).
5. Specify the domain name or the IP address of the KDC server in **Key distribution center**.
6. Specify the port number of the KDC server. By default, the port is 88.
7. Browse to the keytab files used for the service authentication. Each uploaded keytab file is merged with the previously loaded files.
8. Enable the **Overwrite the existing keytab** option to overwrite the previously loaded keytab files with the new keytab file.
9. **Optional:** Provide a description of this authentication method to simplify management.
10. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, user@domain) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

11. Click **Apply**.

Link the Kerberos Password authentication method to the domain.

12. Go to the **Configuration > Authentication domains** page.
13. Edit the LDAP or AD authentication domain or create a new one.
14. In **Secondary authentication**, select the Kerberos Password authentication method.
15. Click **Apply**.

7.2.4.4. RADIUS authentication (LDAP/AD)

About this task

For RADIUS authentications, WALLIX Bastion supports the challenge-response mechanism.

For a second factor authentication, if a user performs several connections and the client's IP address is the same as the one used for the previous authentication, then they are not prompted to authenticate again.

How to enable RADIUS authentication for LDAP/AD users?

To allow LDAP/AD users to authenticate using RADIUS, you must create the RADIUS authentication first and then link that authentication to the domain that contains the users.

Procedure

Create the RADIUS external authentication.

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **RADIUS**.
3. Give the RADIUS authentication a name.
4. Specify the server address (IP or FQDN) and the port number of that server (by default, the port is 1812).
5. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 5 seconds.

**CAUTION:**

This timeout applies to any new RADIUS external authentication. The RADIUS external authentications inherited from an earlier version of WALLIX Bastion keep the former timeout value defined.

6. For **New secret** and **Confirm secret**, enter the packet encryption key.
7. **Optional:** Provide a description of this authentication method to simplify management.
8. Enable the **Use mobile device for two-factor authentication (2FA)** option. This displays a message on the login page informing the user that they must authenticate through a push notification sent to their mobile device.

This option is only relevant when this authentication is used as a second factor after a first authenticating through bind password.

9. Enable the **Use primary domain name for two-factor authentication (2FA)** option. This forces the domain name to be mentioned in the login (for example, `user@domain`) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through bind password.

10. Click **Apply**.

Link the RADIUS authentication method to the domain.

11. Go to the **Configuration > Authentication domains** page.
12. Edit the LDAP or AD authentication domain or create a new one.
13. In **Secondary authentication**, select the RADIUS authentication method.
14. Click **Apply**.

7.2.4.5. TACACS+ authentication (LDAP/AD)

About this task

The TACACS+ external authentication is used to authenticate with a TACACS+ (Terminal Access Controller Access Control System Plus) authentication server.

How to enable TACACS+ authentication for LDAP/AD users?

To allow LDAP/AD users to authenticate using TACACS+, you must create the TACACS+ authentication first and then link that authentication to the domain that contains the users.

Procedure

Create the TACACS+ external authentication.

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **TACACS+**.
3. Give the new authentication method a name.
4. Enter the IP address or FQDN of the TACACS+ server.
5. Enter the port on which the TACACS+ server listens for authentication requests.

By default, the TACACS+ port is 49.

6. For secret, enter and confirm the secret used to access the TACACS+ server. This secret must correspond to the server key configured on the TACACS+ server.
7. **Optional:** Provide a description of this authentication method to simplify management.



8. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, `user@domain`) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

9. Click **Apply**.

Link the TACACS+ authentication method to the domain.

10. Go to the **Configuration > Authentication domains** page.
11. Edit the LDAP or AD authentication domain or create a new one.
12. In **Secondary authentication**, select the TACACS+ authentication method.
13. Click **Apply**.

7.2.4.6. SSH Key authentication (LDAP/AD)

How to enable SSH Key authentication for LDAP/AD users?

When configuring the LDAP or Active Directory authentication domain, you must fill out the **SSH public key attribute** from the **User attributes** section. It is the attribute that contains the SSH public keys from the LDAP or AD server for users, which allows them to authenticate. The `altSecurityIdentities` attribute is recommended for the AD server.

If the **SSH public key attribute** field is empty, users authenticate using only their LDAP or AD password.



Note:

LDAP/AD users with an SSH Key authentication do not have access to the **SSH Key** tab in their user preferences. Key management is done through the directory service directly.

SSH Key requirements

The values defined in the LDAP or AD server must be prefixed as `sshKey: <public key>`.

Multiple SSH keys can be defined for each user.

The SSH public keys must be in the OpenSSH format and encrypted with the following algorithms.

Key type	Size allowed
RSA	1024 bits 2048 bits 4096 bits 8192 bits
ECDSA	256 bits 384 bits 521 bits
ED25519	N/A

7.2.4.7. SSH Certificate authentication (LDAP/AD)



Important:

X.509 certificate authentication and SSH certificate authentication are not compatible.

A Certificate Authority (CA) is defined by an SSH key pair (a private key and a public one). The CA private key signs the public keys of the user accounts on the domain. These signed public keys are also called "certificates" and are used by the user to authenticate to WALLIX Bastion. The certificates are checked against the CA public key by WALLIX Bastion during connections.



Note:

WALLIX Bastion does not support Key Revocation Lists (KRL) for SSH certificates.

How to enable SSH CA authentication for LDAP/AD users?

Procedure

1. Add a Certificate Authority in WALLIX Bastion.
 - a. Go to the **Configuration > Certificate authorities** page.
 - b. Click **Add**.
 - c. Give the certificate a name (up to 255 characters) and an optional description (up to 1024 characters).
 - d. Upload the CA file.

The file size cannot exceed 16,384 octets and the following SSH algorithms are supported:

 - RSA
 - ED25519
 - ECDSA NIST p256
 - ECDSA NIST p384
 - ECDSA NIST p521
 - e. Click **Apply**.
2. Link the Certificate Authority to the authentication domain.
 - a. Go to the **Configuration > Authentication domains** page.
 - b. Edit the LDAP or AD authentication domain or create a new one.
 - c. Activate the **Enable SSH certificate authentication** option.
 - d. Select the certificate from the drop-down list.
 - e. Click **Apply**.

Results

When configured, users can authenticate to the LDAP or AD domain using SSH CA authentication method. During the user authentication, the certificate signature date is checked by WALLIX Bastion.



Attention:

It is not possible to delete a certificate linked to an authentication domain.



7.2.4.8. X.509 certificate authentication (LDAP/AD)



Important:

X.509 certificate authentication and SSH certificate authentication are not compatible.

How to enable X.509 Certificate authentication for LDAP/AD users?

When configuring the LDAP or Active Directory authentication domain, in the **X509 options** section, you must activate the **Enable X509 authentication** option.

When configured, users can only authenticate to the LDAP or AD server using X.509 certificate authentication method.

Matching condition

You must provide the condition to match an LDAP or AD domain to the X.509 certificate. If no condition is specified, the LDAP or AD domain can be used for X.509 authentication regardless of the certificate.

Requirements:

- The operator && (that is **AND**) has precedence over the operator || (that is **OR**).
- The values are case sensitive unlike variables.
- The condition is formatted according to the following variables retrieved from the certificate.

Variables of WALLIX Bastion	Description
<code>\${issuer}</code>	Issuer DN of client's certificate.
<code>\${issuer_c}</code>	Country name in Issuer DN.
<code>\${issuer_l}</code>	Locality name in Issuer DN.
<code>\${issuer_o}</code>	Organization name in Issuer DN.
<code>\${issuer_ou}</code>	Organization Unit name in Issuer DN.
<code>\${issuer_cn}</code>	Common name in Issuer DN.
<code>\${issuer_st}</code>	State or Province name in Issuer DN.
<code>\${issuer_email}</code>	E-mail Address in Issuer DN.
<code>\${subject}</code>	Subject DN in client's certificate.
<code>\${subject_c}</code>	Country name in Subject DN.



Variables of WALLIX Bastion	Description
<code>\${subject_l}</code>	Locality name in Subject DN.
<code>\${subject_o}</code>	Organization name in Subject DN.
<code>\${subject_ou}</code>	Organization Unit name in Subject DN.
<code>\${subject_cn}</code>	Common name in Subject DN.
<code>\${subject_st}</code>	State or Province name in Subject DN.
<code>\${subject_email}</code>	E-mail Address in Subject DN.
<code>\${subject_uid}</code>	UID in Subject DN.
<code>\${mail}</code>	Server certificate's <code>subjectAltName</code> extension entries of the <code>rfc822Name</code> type.
<code>\${msupn}</code>	Client certificate's <code>subjectAltName</code> extension entries of the <code>otherName</code> type, Microsoft User Principal Name form.
<code>\${dns}</code>	Server certificate's <code>subjectAltName</code> extension entries of type <code>dNSName</code> .
<code>\${username}</code>	Common name from Subject DN or local part of Subject DN if Subject DN is an e-mail (for example, <code>local-part@domain</code>).



Important:

The format corresponds to the syntax used in the advanced search filters of the REST API. For more information, refer to the related online help page at this address: https://bastion_IP_address/api/doc/Usage.html#search.

Example of a matching condition

```
${issuer_o}~Company Ltd. || ${issuer_cn}~Security Cert &&  
${subject_ou}=Finance&Accounting
```

This matching condition associates the domain with a certificate issued by an organization whose name (`issuer_o`) includes `Company Ltd.` OR a certificate whose common name (`issuer_cn`) includes `Security cert` and whose user's organization unit (`subject_ou`) corresponds to `Finance&Accounting`.

Search filter

The LDAP or AD search filter to retrieve users from the domain. This data is expressed using LDAP filter syntax, but any available variables as listed in the field **Matching condition** field can also be used.



Note:

All variables specified in the **Search filter** field must be present in the certificate to provide a valid LDAP or AD filter and retrieve users accordingly.

For example, the following filter syntax retrieves LDAP or AD users whose `cn` is the `subject_cn` of the certificate or whose `uid` is the `subject_uid` of the certificate and whose `preferredLanguage` attribute is `fr` :

```
(&(|(cn=${subject_cn})(uid=${subject_uid}))(preferredLanguage=fr))
```

For example, the following filter syntax retrieves AD users whose local part of the `userPrincipalName` is the `subject_cn` of the certificate and whose domain includes either `company.com` or `biz.company.com`:

```
(|  
(userPrincipalName=${subject_cn}@company.com)(userPrincipalName=${subject_cn}@biz.compa  
ny.com))
```

Domain name to match SAN Email

When using X.509 authentication with an Active Directory server, the mention of the domain name to match the SAN e-mail. The domain is used to check the e-mail field from the X.509 `Subject Alternative Name` (SAN) extension.

7.3. Federated Identity users

7.3.1. SAML 2.0

SAML as a Service Provider (SP) allows users to authenticate to WALLIX Bastion and retrieve authorizations based on their Identity Provider (IdP) profile and rights. To ensure that users authenticate with credentials provided by their IdP, WALLIX Bastion must be configured as an SP against the IdP.

The following SAML authentication flows are supported:

- **Identity Provider (IdP) Initiated:** the user can log on the IdP and is then forwarded to WALLIX Bastion.
- **Service Provider (IdP) Initiated:** the user tries to log on the WALLIX Bastion web interface or start an SSH or RDP session and is forwarded to their IdP to authenticate.



Important:

Only SAML Generic is compatible with WALLIX Access Manager.

The configuration of a SAML authentication with WALLIX Access Manager means that it is impossible to authenticate directly to WALLIX Bastion in SAML.



7.3.1.1. SAML Generic with any Identity Provider

You can configure SAML 2.0 authentication for any provider. For example, WALLIX IDaaS, Entra ID, Okta, PingOne, TrustBuilder, etc.

7.3.1.1.1. Add a SAML external authentication

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **SAML**.
3. Give the new authentication method a name.
4. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 900 seconds.

This time starts from the moment the user clicks on the IdP authentication button on the login page.

5. **Optional:** Provide a description of this authentication method to simplify management.
6. For **IdP metadata** under **IdP information**, click **Choose file** and upload the identity provider (IdP) metadata XML file.

In the **IdP claim customization** section, the file upload prefills the **Username**, **Display name**, and **Email** fields automatically.

7. For **IdP claim customization**, verify the information and if necessary, modify it.

- a. Provide the **Username**.

When authenticating with SAML to WALLIX Bastion through Access Manager, the username must be identical to the Login attribute in the Identity Provider configuration on WALLIX Access Manager (**SAML Identity Providers** menu).

- b. **Optional:** Provide the display name, e-mail, and language.

- c. Provide the group if you want to configure the group mapping after configuring the IdP authentication domain.

8. Click **Apply**.
9. Retrieve and copy the information required on the provider side to connect with WALLIX Bastion.
 - **SP metadata:** you can download the service provider metadata file.
 - **SP entity ID:** identifier to refer to WALLIX Bastion in interactions with the identity provider in the SAML communication. It corresponds to the `entityID` attribute of the **EntityDescriptor** element in the service provider metadata file.
 - **SP assertion consumer service:** this is the URL to which the identity provider redirects the user when the user authenticated. It corresponds to the `AssertionConsumerService` attribute of the **SPSSODescriptor** element in the service provider metadata file.
 - **IdP entity ID:** Identifier of the identity provider interacting with the service provider (SP), that is WALLIX Bastion, in the SAML communication process. It corresponds to the `entityID` attribute of the **EntityDescriptor** element in the identity provider metadata file.
 - **IdP SAML request URL:** URL to which WALLIX Bastion redirects the user for authentication. It corresponds to the `Location` attribute of the **SingleSignOnService** element in the identity provider metadata file.

Results

The Identity Provider metadata XML file can be downloaded by clicking **Download registered IdP metadata**.



The Service Provider metadata XML file can be downloaded by clicking **Download SP metadata**.



Note:

The Service Provider information is the same for all SAML external authentications.

7.3.1.1.2. Add a provider authentication domain

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Click **Add** and select **SAML > Other IdPs** from the drop-down list.
3. In **Domain server name**, give your provider a recognizable name.



Note:

When authenticating through SAML to WALLIX Bastion through Access Manager, the server domain name must be identical to the **Domain Name** field in the domain configuration on WALLIX Access Manager (**SAML Identity Providers** menu).

4. Add the IdP domain name in **Authentication domain name**.

During the IdP configuration, in the **Name ID format** field, select **email address**. The domain of the e-mail address must be the same as the authentication domain name.

5. Enable or disable **Default domain**.

Enabling this option strips the domain part (that is @domain) from the user login when authenticating to WALLIX Bastion. Thus, local users defined in WALLIX Access Manager can be mapped to users in the Bastion domain.

6. Select the previously configured SAML external authentication from the **Authentication protocol** from the drop-down list.

For more information, refer to [Add a SAML external authentication \(on page 72\)](#).

7. **Optional:** Provide a description to simplify management.
8. Enter the text you want to display on the login button in **Label for authentication button on the login page**. By default, it is SAML.
9. Set the **Default language** for domain member if their language cannot be found or is undefined in the identity provider.
10. Set the **Default email domain**.

It is the domain component used to build the user's e-mail address if it is not found from the claim customization (refer to the **IdP claim customization** fields in [Add a SAML external authentication \(on page 72\)](#)) or in the IdP. This address is built by prefixing the default e-mail domain with the user name. If this field is not specified, then the address is built by prefixing the authentication domain name with the user name.

11. Set the **IdP initiated URL**.

It is the URL to allow users to be redirected and logged in WALLIX Bastion from the IdP portal. After all the fields are specified and applied, the URL is displayed and can be copied from the **IdP initiated URL** field into the related field of the IdP Single Sign-On configuration. For more information, refer to [Add a SAML external authentication \(on page 72\)](#).

12. **Optional:** Activate **Force authentication**.



When this option is activated, users are required to re-authenticate to their identity provider to access WALLIX Bastion, even if they already have an active IdP session.

This feature natively supports SAML with Entra ID and Okta. However, other IdPs may require further configuration on their side.

13. Click **Apply**.

7.3.1.1.3. Add group mappings

About this task

A mapping links your groups to WALLIX Bastion groups.

Administrators cannot view mappings whose profiles have at least one permission that the administrator's profile cannot grant as a transferable right. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Edit the authentication domain of your choice.
3. Switch to the **Mappings** tab and click **Add**.
4. Select user group created on WALLIX Bastion from the **User group** drop-down list.
5. Select a profile created on WALLIX Bastion from the **User group profile** drop-down list.
6. **Optional:** If you want to set the selected WALLIX user group and profile as default for all directory users that do not match another group mapping, activate **Default group for users without group in this domain**.

Having a default group ensures that all users can access WALLIX Bastion.

7. For **Group**, enter the value of the group sent in the SAML response.

Input is case insensitive. You can only add one value. That value must be part of the group attribute defined in the **IdP claim customization** section of SAML external authentication. For more information, refer to [Add a SAML external authentication \(on page 72\)](#).

8. Click **Add and continue** to save and add another group mapping or click **Add and close** if you are done.

What to do next

Configure the approver group by specifying the **Language** and **Email list** fields (refer to [User groups \(on page 43\)](#)) to allow the approver to be notified by e-mail of the approval requests.



Tip:

Group mappings can also be edited on the user group modification page (refer to [User groups \(on page 43\)](#)).

7.3.1.2. SAML for Microsoft Entra ID (with Graph API)



Important:

This configuration is not compatible with WALLIX Access Manager. If you have an Access Manager, WALLIX recommends using [SAML Generic with any Identity Provider \(on page 72\)](#).



Instead of configuring an **Other IdPs** authentication domain, you can configure an **Entra ID** one. This configuration allows the Graph API to retrieve information for users in the Microsoft Application.

7.3.1.2.1. Add a SAML external authentication

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **SAML**.
3. Give the new authentication method a name.
4. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 900 seconds.

This time starts from the moment the user clicks on the IdP authentication button on the login page.

5. **Optional:** Provide a description of this authentication method to simplify management.
6. For **IdP metadata** under **IdP information**, click **Choose file** and upload the identity provider (IdP) metadata XML file.

In the **IdP claim customization** section, the file upload prefills the **Username**, **Display name**, and **Email** fields automatically.

7. For **IdP claim customization**, verify the information and if necessary, modify it.
 - a. Provide the **Username**.

When authenticating with SAML to WALLIX Bastion through Access Manager, the username must be identical to the Login attribute in the Identity Provider configuration on WALLIX Access Manager (**SAML Identity Providers** menu).
 - b. **Optional:** Provide the display name, e-mail, and language.
 - c. Provide the group if you want to configure the group mapping after configuring the IdP authentication domain.
8. Click **Apply**.
9. Retrieve and copy the information required on the provider side to connect with WALLIX Bastion.
 - **SP metadata:** you can download the service provider metadata file.
 - **SP entity ID:** identifier to refer to WALLIX Bastion in interactions with the identity provider in the SAML communication. It corresponds to the `entityID` attribute of the **EntityDescriptor** element in the service provider metadata file.
 - **SP assertion consumer service:** this is the URL to which the identity provider redirects the user when the user authenticated. It corresponds to the `AssertionConsumerService` attribute of the **SPSSODescriptor** element in the service provider metadata file.
 - **IdP entity ID:** Identifier of the identity provider interacting with the service provider (SP), that is WALLIX Bastion, in the SAML communication process. It corresponds to the `entityID` attribute of the **EntityDescriptor** element in the identity provider metadata file.
 - **IdP SAML request URL:** URL to which WALLIX Bastion redirects the user for authentication. It corresponds to the `Location` attribute of the **SingleSignOnService** element in the identity provider metadata file.

Results

The Identity Provider metadata XML file can be downloaded by clicking **Download registered IdP metadata**.

The Service Provider metadata XML file can be downloaded by clicking **Download SP metadata**.



Note:

The Service Provider information is the same for all SAML external authentications.

7.3.1.2.2. Add an Entra ID authentication domain

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Click **Add** and select **SAML > Entra ID** from the drop-down list.
3. Add the WALLIX Bastion domain name in **Domain server name**.
4. Add the Entra ID authentication domain name in **Authentication domain name**.
5. Enable or disable **Default domain**.

Enabling this option strips the domain part (that is @domain) from the user login when authenticating to WALLIX Bastion. Thus, local users defined in WALLIX Access Manager can be mapped to users in the Bastion domain.

6. Select the previously configured SAML external authentication from the **Authentication protocol** from the drop-down list.

For more information, refer to [Add a SAML external authentication \(on page 72\)](#).

7. **Optional:** Provide a description to simplify management.
8. Provide a **Label for authentication button on the login page** of WALLIX Bastion. By default, the field is already specified with **Entra ID**.
9. Add the Entra ID cloud tenant ID in **Tenant ID**. Retrieve the information from the **Directory (tenant) ID** field of the application page in Entra ID.
10. Add the Entra ID cloud client ID in **Application ID**. Retrieve the information from the **Application ID** field of the application page in Entra ID.
11. Provide the **Client secret**. This is the secret generated by Entra ID and shared between WALLIX Bastion and Entra ID. Retrieve the information from the application page in Entra ID.
12. Upload the **Server certificate**. This is the WALLIX Bastion certificate shared between WALLIX Bastion and Entra ID.
13. Upload the **Server private key**. This is the private key associated with the certificate shared between WALLIX Bastion and Entra ID.
14. Enter the **Server private key passphrase**. This is the passphrase of the private key associated with the certificate shared between WALLIX Bastion and Entra ID.
15. Set the **Default language** for domain member if their language cannot be found or is undefined in the identity provider.
16. Set a **Default email domain**.

This is the domain component used to build the user's e-mail address if not found in Entra ID. This address is built by prefixing the default e-mail domain with the user name. If this field is not specified, then the address is built by prefixing the authentication domain name with the user name.

17. Set the **IdP initiated URL**.

It is the URL to allow users to be redirected and logged in WALLIX Bastion from the Entra ID portal. After all the fields are specified and applied, the URL is displayed and can be copied from the **IdP initiated URL** field into the **Sign on URL (Optional)** field of the Enterprise Application of Entra ID during the Single Sign-On configuration. For more information, refer to [Add a SAML external authentication \(on page 72\)](#).

18. **Optional:** Activate **Force authentication**.



When this option is activated, users are required to re-authenticate to their identity provider to access WALLIX Bastion, even if they already have an active IdP session.

19. Click **Apply**.

7.3.1.2.3. Add Entra ID group mappings

About this task

A mapping links your Entra ID groups to WALLIX Bastion groups.

Administrators cannot view the mappings whose profiles have at least one permission that the administrator's profile cannot grant as a transferable right. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Edit the authentication domain of your choice.
3. Switch to the **Mappings** tab and click **Add**.
4. Select user group created on WALLIX Bastion from the **User group** drop-down list.
5. Select a profile created on WALLIX Bastion from the **User group profile** drop-down list.
6. **Optional:** If you want to set the selected WALLIX user group and profile as default for all Entra ID users that do not match another group mapping, activate **Default group for users without group in this domain**.

Having a default group ensures that all users can access WALLIX Bastion.

7. For **Group**, enter the value of the group sent in the SAML response.

Input is case insensitive. The value must match the group attribute defined in the **IdP claim customization** section of SAML external authentication. For more information, refer to [Add a SAML external authentication \(on page 75\)](#).

8. Click **Add and continue** to save and add another group mapping or click **Add and close** if you are done.

What to do next

Configure the approver group by specifying the **Language** and **Email list** fields (refer to [User groups \(on page 43\)](#)) to allow the approver to be notified by e-mail of the approval requests.



Tip:

Group mappings can also be edited on the user group modification page (refer to [User groups \(on page 43\)](#)).

7.3.2. Generic OpenID Connect (OIDC)

7.3.2.1. Add an OIDC external authentication

Before you begin

Before you can create an OpenID Connect authentication method in WALLIX Bastion, you must register an OIDC application on your identity provider (IdP). This process varies depending on your provider, you can refer to the official documentation of your IdP to complete this task.

**Important:**

WALLIX Bastion only supports the Authorization Code Flow.

**Tip:**

OpenID Connect providers can offer a discovery mechanism. This mechanism provides all configuration information in a dedicated document publicly accessible through a URL ending in `/.well-known/openid-configuration`. For example, `http://auth.example.com/.well-known/openid-configuration`.

WALLIX recommends using this discovery mechanism if available to configure your external authentication in the Bastion.

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **OIDC**.
3. Give the new authentication method a name.
4. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 900 seconds.

This time starts from the moment the user clicks on the IdP authentication button on the login page.

5. **Optional:** Provide a description of this authentication method to simplify management.
6. Enter the provider application information.
 - In **Client ID**, enter the unique identifier of the registered OIDC application on the IdP side.
 - In **Client Secret**, enter the client secret of the registered OIDC application on the IdP side.
7. Provide the discovery URL for the application and click **Match**. This prefills all the required information.

You may skip this step and manually provide the necessary information for each required field if you prefer. However, WALLIX recommends the URL discovery method.

8. Verify that all information returned with the discovery URL match is valid and complete.

**Important:**

Grant type and **Response type** cannot be modified.

9. Enter the corresponding mappings for claims.

Username and **Group** are mandatory to provide.

10. Click **Apply**.

7.3.2.2. Add a provider authentication domain

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Click **Add** and select **OIDC** from the drop-down list.
3. In **Domain server name**, give your provider a recognizable name.
4. Add the IdP domain name in **Authentication domain name**.



5. Enable or disable **Default domain**.

Enabling this option strips the domain part (that is @domain) from the user login when authenticating to WALLIX Bastion. Thus, local users defined in WALLIX Access Manager can be mapped to users in the Bastion domain.

6. Select the previously configured OIDC external authentication from the **Authentication protocol** from the drop-down list.

For more information, refer to [Add an OIDC external authentication \(on page 77\)](#).

7. **Optional:** Provide a description to simplify management.

8. Enter the text you want to display on the login button in **Label for authentication button on the login page**. By default, it is `OIDC`.

9. Set the **Default email domain**.

It is the domain component used to build the user's e-mail address if it is not found from the claim customization (refer to the **IdP claim customization** fields in [Add an OIDC external authentication \(on page 77\)](#)) or in the IdP. This address is built by prefixing the default e-mail domain with the user name. If this field is not specified, then the address is built by prefixing the authentication domain name with the user name.

10. Set the **Default language** for domain member if their language cannot be found or is undefined in the identity provider.

11. Click **Apply**.

7.3.2.3. Add group mappings

About this task

A mapping links your groups to WALLIX Bastion groups.

The list of profiles is filtered based on the transferable rights of the administrator creating the group mapping. Administrators cannot assign a profile to a group if any permission in a profile is not listed as part of their own transferable rights. However, administrators can view and edit existing group mappings with a profile that does not match their transferable right configuration. For more information, refer to [Permission profiles \(on page 22\)](#).

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Edit the authentication domain of your choice.
3. Switch to the **Mappings** tab and click **Add**.
4. Select user group created on WALLIX Bastion from the **User group** drop-down list.
5. Select a profile created on WALLIX Bastion from the **User group profile** drop-down list.
6. **Optional:** If you want to set the selected WALLIX user group and profile as default for all directory users that do not match another group mapping, activate **Default group for users without group in this domain**.

Having a default group ensures that all users can access WALLIX Bastion.

7. For **Group**, enter the value of the group sent in the OIDC response.

Input is case insensitive. You can only add one value. That value must be part of the group attribute defined in the **IdP claim customization** section of OIDC external authentication. For more information, refer to [Add an OIDC external authentication \(on page 77\)](#).

8. Click **Add and continue** to save and add another group mapping or click **Add and close** if you are done.



What to do next

Configure the approver group by specifying the **Language** and **Email list** fields (refer to [User groups \(on page 43\)](#)) to allow the approver to be notified by e-mail of the approval requests.



Tip:

Group mappings can also be edited on the user group modification page (refer to [User groups \(on page 43\)](#)).

7.4. Local users

Local identities only exist inside WALLIX Bastion.

Introduction to local identities

Local Bastion identities are users with accounts created on WALLIX Bastion. That means their identity type is WALLIX.

WALLIX recommends keeping local identities to a restricted usage. For example, as a temporary solution during a service breakdown of the outside identity management solution, or for specific cases such as high-level solution administrators.

The default **admin** account created for WALLIX is a local identity. However, WALLIX recommends deleting the default administrator account after the solution deployment. For high-level solution administrators, you should create a new local identity with a different name.

About local user accounts

There are three methods to create users with a local identity on WALLIX Bastion:

- Manual operations, one user account at a time.
- CSV import feature. For more information, refer to [Import local user accounts \(on page 82\)](#).
- WALLIX Bastion APIs

WALLIX Bastion provides five primary authentication methods for local identities:

- Login and password
- SSH key
- X.509 certificate
- RADIUS
- TACACS+
- PingID



Important:

If you are planning on using an external authentication method such as RADIUS, TACACS+, or PingID, you must configure the external authentication first. For more information, refer to [Authentication protocols for local users \(on page 85\)](#).

7.4.1. Create local user accounts

Procedure

1. Go to the **Users > Accounts** page.
2. Click **Add a user**.
3. Enter the user name used to authenticate to the web user interface and proxies.

User account names are not case sensitive but case is preserved as account is created.

4. Enter a display name to identify the person to whom the user name corresponds.
5. Enter an e-mail address. The user can modify their e-mail address later.
6. **Optional:** Upload a GPG public key. The user will receive the new password in an encrypted e-mail. The user can modify this key later.



Attention:

If the GPG key is not specified for the user with the **product_administrator** or **operation_administrator** profile, then a warning e-mail is sent daily to notify the user of the missing declaration of the GPG key.

The sending of this warning e-mail can be managed with the **Missing GPG key warning email** option in the menu **Configuration > Configuration options > Global**. By default, this option is enabled.

7. Set a preferred language for the user.

This is the language for the interface and messages sent to the user from the proxies. The user can modify their preferred language.

8. Assign a profile to the user to define their rights and limitations. For more information, refer to [Permission profiles \(on page 22\)](#).
9. **Optional:** If access is forbidden to the user currently, activate the **Disable** option. When disabled, users are not allowed to log on to the WALLIX Bastion web interface and proxies.



CAUTION:

If this option is deactivated but no rights are defined in the user profile, the user will not be allowed to log on to the WALLIX Bastion web interface, the REST API web service, and RDP/SSH sessions.

10. **Optional:** If the user access is temporary, you can set an account expiration date using the calendar and clicking **Done**.
11. If the user should be part of one or more groups, select the relevant groups from the **Available Groups** column and add them to the **Selected Groups** column.
12. Select all of the authentication methods that you want to make available to that user.
 - If you want to allow local password authentication, refer to [Password authentication \(local\) \(on page 85\)](#).
 - If you want to allow X.509 certificate authentication, refer to [X.509 certificate authentication \(local\) \(on page 87\)](#).
 - If you want to allow SSH Key authentication, refer to [SSH Key authentication \(local\) \(on page 87\)](#).
 - If you want to allow RADIUS authentication, refer to [RADIUS authentication \(local\) \(on page 88\)](#).



- If you want to allow TACACS+ authentication, refer to [TACACS+ authentication \(local\) \(on page 89\)](#).
 - If you want to allow PingID authentication, refer to [PingID authentication \(local\) \(on page 90\)](#).
13. **Optional:** If required, you can restrict the access to proxies and the web interface to an IP/Subnets/Domain address or an IP range of addresses.
14. Click **Apply**.

7.4.2. Import local user accounts

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

Data related to user password, SSH key, or X.509 DN is not provided in the .csv file when exporting users. It must then be specified in the .csv file before importing.

The CSV file must begin with a line containing the `#wab1040 user` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	[R]equired [O]ptional	Description and expected values
Username	Text	R	[aA-zZ], [0-9], '-', '_'
Groups	Text	O	[aA-zZ], [0-9], '-', '_' There can be several groups for the same user. If the user group does not exist, it is created with the default time frame set as "allthetime".
Full name	Text	O	Free text
Source IPs	IP/FQDN	O	[aA-zZ], [0-9], '-', '_' Can be either an IP address or a domain or an IP range (for example, "10.10.10.11-10.10.10.42").
Profile	Text	R	Profiles defined
Account expiration date	Date and time	O	YYYY-MM-DD and HH:MM Date and time at which the account will expire



Field	Type	[R]equired [O]ptional	Description and expected values
User authentications	Text	R	Authentications defined There can be several authentications for the same user.
Public key	Text	Required for "local_sshkey"	[aA-zZ], [0-9], '-', '_' The corresponding data is not provided in the .csv file when exporting users. It must then be specified in the .csv file before import.
Password	Text	Required for "local_password"	Free text The corresponding data is not provided in the .csv file when exporting users. It must then be specified in the .csv file before import. Must be compliant with the current password policy (number of special characters, etc.).
Email	Text	R	E-mail address
Force change password	Boolean	R	True or False Default value: False
Lock counter	Integer number	O	Authentication failure counter Positive integer number, will lock out the user if greater than or equal to the value of the maximum number of allowed authentication failures per user specified in the password policy. Default value: 0
Last connection	Text	O	This field is ignored.



Field	Type	[R]equired [O]ptional	Description and expected values
Preferred language	Text	O	"de" for German "en" for English "es" for Spanish "fr" for French "ru" for Russian Default value: en
Certificate DN	Text	Required for "local_x509"	A certificate DN. The corresponding data is not provided in the .csv file when exporting users. It must then be specified in the .csv file before import.
Disabled	Boolean	O	Option used to define if the user account is disabled or not. True or False Default value: False

Example of import syntax:

```
#wab1040 user
martin;linuxadmins;Pierre Martin;;user;;local;;jMpdu9/x2z;martin@wallix.com;False;0;;fr
;/C=FR/O=Wallix/CN=PKI_USER;False
```

Procedure

1. To make sure you have the right CSV syntax, export the current list of user accounts.

For more information, refer to [Export local user accounts \(on page 91\)](#).

2. Edit the CSV file to add new user accounts or modify the configuration of existing user accounts and save.
3. Go to the **Import/Export > CSV** page.
4. Select your preferred **Field separator** and **List separator** from the dropdown lists.

The separator values must differ. If you exported the CSV file as recommended, use the same separator values.

5. Select **Users** from the **Data** options.
6. Retrieve the CSV file from your computer.
7. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

7.4.3. Authentication protocols for local users

There are three local authentication methods, and three external authentication methods available for local users.

7.4.3.1. Password authentication (local)

How to enable password authentication for local users?

User accounts can have the local password authentication through the following methods:

- With manual operations, from **Users > Accounts** page when creating or editing a user, select the **local_password** authentication method and entering the password. You can also force password reset by selecting **Yes** for the **Force password change** option.
- With CSV import, include the **Password** value in the CSV file. You can also force password reset by setting **True** for the **Force password change** option.
- With Bastion APIs,



Note:

The password must be robust, for example, avoid common words, logical or repeated patterns (such as Password123!, abcabcABCABC, etc.). You can specify further requirements regarding the password acceptance, but you cannot remove this limitation on weak passwords. For more information, refer to [Local password policy \(on page 85\)](#).

Force password change

Decide if you force password change for the user. The user will receive a notification message indicating that their account is created and that the password must be changed at first login.

If the administrator forces password change, users have to change the password next time they authenticate either to the web interface, or to a RDP or SSH session. No access will be granted as long as the password is not changed.

This option is about forcing a reset, however, users can always decide to change their password.

7.4.3.1.1. Local password policy

What is a Local password policy?

The password policy establishes a set of rules for storing local passwords. These rules define the level of complexity for the password that a local identity user can define.

Configuration

From the **Local Password Policy** page on the **Configuration** menu, you can define the password policy and configure the password expiration time. This page consists of the following fields:

Password expiration

The password validity period expressed in number of days. After this period, the user is asked to update their password on the login screen of WALLIX Bastion or when connecting to the RDP or SSH session.

If a modification to this value impacts users, a **Changes for password expiration** dialog appears to warn the administrator. This dialog lists all users whose password is



due to expire the next time they log in if this modification is confirmed. The administrator can choose to apply or cancel the change from this dialog.

Recommendation: setting for a period of less than one year.

Password expiration warning

The period in number of days before the display of the first password expiration warning.

Recommendation: setting this period to a value of at least 20 days.

Allowed authentication failures per user

The maximum number of authentication failures allowed per user.

Recommendation: setting this number to a value of at most 5 authentication attempts.

Previous passwords to reject

The number of previous passwords which cannot be reused.

Recommendation: rejecting at least the last 4 passwords.

Minimum password length

The minimum number of characters required in the password. This value must be greater than the sum of the other length constraints.

Recommendation: setting this length to a value of at least 12 characters.

Minimum number of special characters

The minimum number of special characters required in the password.

Recommendation: setting this number to a value of at least 1 character.

Minimum number of uppercase letters

The minimum number of uppercase letters required in the password.

Recommendation: setting this number to a value of at least 1 character.

Minimum number of lowercase letters

The minimum number of lowercase letters required in the password.

Recommendation: setting this number to a value of at least 1 character.

Minimum number of digits

The minimum number of digits required in the password.

Recommendation: setting this number to a value of at least 1 character.

Allowed SSH public key algorithms

The algorithms allowed for the SSH public key. The administrator can select one or several algorithms. If no algorithm is selected, users cannot define a SSH public key in their preferences. The SSH public key also cannot be set for the local user on the **Accounts** page from the **Users** menu.

Minimum RSA key length

If the **RSA** algorithm is selected, a minimum key length must be defined. This value must not be lower than 1024 bits.



User name and password can be similar

The option to allow or prevent passwords to be similar to the user name.

Recommendation: do not allow similarity.

Banned password list

Add the list of banned passwords through a file. The file containing the list of banned passwords must be in a UTF-8 format.

Download the existing file containing the list of banned passwords.

7.4.3.2. SSH Key authentication (local)

How to enable SSH Key authentication for local users?

User accounts can obtain SSH Key authentication through the following methods:

- With manual operations, from **Users > Accounts** page when creating or editing a user, select the **local_sshkey** authentication method and uploading or entering the public key.
- With CSV import, include the **Public key** value in the CSV file.
- With Bastion APIs,



Tip:

This authentication method is not available on the web interface, as such, WALLIX recommends using it with another authentication method.

SSH public key requirements

The SSH public key must use the RSA, ED25519, or ECDSA algorithm. This key can be modified later on by the user.

It is not possible to set a key if no algorithm is allowed for the SSH public key on the **Configuration > Local Password Policy** page. For more information, refer to [Local password policy \(on page 85\)](#).

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

If you use PuTTYgen to generate the key, you must save in a text file the public key displayed in the OpenSSH format during the generation. As an example, this key is labeled as follows.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA0yR9lBQov6[ . . . . . ]c3xu9p/xNjw== rsa-key-20151204
```

You can upload this key on the dedicated area.

If a key already exists, you can load a private key using PuTTYgen to generate the corresponding public key in the appropriate format.

7.4.3.3. X.509 certificate authentication (local)

How to enable X.509 certificate authentication for local users?

User accounts can obtain X.509 certificate authentication through the following methods:



- With manual operations, from **Users > Accounts** page when creating or editing a user, select the **local_X509** authentication method and enter a value in the **Certificate DN** field.
- With CSV import, include the **Certificate DN** value in the CSV file.
- With Bastion APIs,

Certificate DN requirements

For X.509 certificate authentication to be valid, each user must have a Certificate DN (Distinguished Name). The DN must be comply with the following standard.

```
CN=Lucas Martin,O=MyCorp,L=PARIS,ST=IDF,C=FR
```



CAUTION:

Some certificates include the attribute "emailAddress" mentioned as "E =..." in the certificate DN. This attribute must be replaced by "emailAddress =..." in the field provided.

When the certificate is used, the associated user is authenticated on WALLIX Bastion.

There are several limitations:

- The certificates must be signed by the same Certificate Authority as the web server certificate.
- The maximum supported length of a DN is 1,024 bytes. The exact number of characters can be less depending on the length of the UTF-8 encoding.
- The Unicode character set is supported in the DN if the certificate is UTF-8-encoded according to RFC2253, if not, only standard ASCII code is supported.

7.4.3.4. RADIUS authentication (local)

About this task

For RADIUS authentications, WALLIX Bastion supports the challenge-response mechanism.

For a second factor authentication, if a user performs several connections and the client's IP address is the same as the one used for the previous authentication, then they are not prompted to authenticate again.

How to enable RADIUS authentication for Local users?

To allow local users to authenticate using RADIUS, you must create the RADIUS authentication first and then add that authentication method to the user accounts.

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **RADIUS**.
3. Give the RADIUS authentication a name.
4. Specify the server address (IP or FQDN).
5. Specify the port number of the server. By default, the port is 1812.
6. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 5 seconds.

**CAUTION:**

This timeout applies to any new RADIUS external authentication. The RADIUS external authentications inherited from an earlier version of WALLIX Bastion keep the former timeout value defined.

7. For **New secret** and **Confirm secret**, enter the packet encryption key.
8. **Optional:** Provide a description of this authentication method to simplify management.
9. Enable the **Use mobile device for two-factor authentication (2FA)** option to display a message on the login page informing the user that they must authenticate through a push notification sent to their mobile device.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

10. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, user@domain) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

11. Click **Apply**.

7.4.3.5. TACACS+ authentication (local)

About this task

The TACACS+ external authentication is used to authenticate with a TACACS+ (Terminal Access Controller Access Control System Plus) authentication server.

How to enable TACACS+ authentication for local users?

To allow local users to authenticate using TACACS+, you must create the TACACS+ authentication first and then add that authentication method to the user accounts.

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **TACACS+**.
3. Give the new authentication method a name.
4. Enter the IP address or FQDN of the TACACS+ server.
5. Enter the port on which the TACACS+ server listens for authentication requests.

By default, the TACACS+ port is 49.

6. For secret, enter and confirm the secret used to access the TACACS+ server. This secret must correspond to the server key configured on the TACACS+ server.
7. **Optional:** Provide a description of this authentication method to simplify management.
8. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, user@domain) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

9. Click **Apply**.

7.4.3.6. PingID authentication (local)

About this task



Note:

The WALLIX Bastion administrator must remind users to specify only the login field to access the web interface when authenticating with PingID.

How to enable PingID authentication for local users?

To allow local users to authenticate using PingID, you must create the PingID authentication first and then add that authentication method to the user accounts.

Procedure

1. Go to the **Configuration > External authentication** page.
2. Click **Add** and click **PingID**.
3. Give the new authentication method a name.
4. For **Timeout**, specify the maximum waiting time (expressed in seconds) for a connection attempt to the server. By default, the timeout is 30 seconds.
5. Upload the PingID properties file (named `pingid.properties`) containing several account-specific settings.

This file can be downloaded from the PingID administrator interface.

6. **Optional:** Provide a description of this authentication method to simplify management.
7. Enable the **Force OTP** option to force the one-time password (OTP) authentication only. In this case, no other authentication method is proposed.
8. Enable the **Use primary domain name for two-factor authentication (2FA)** option to force the domain name to be mentioned in the login (for example, `user@domain`) during the second authentication.

This option is only relevant when this authentication is used as a second factor after a first authenticating through LDAP.

9. Click **Apply**.

7.4.4. Unlock local user accounts

About this task

Users lock their account if they reach the maximum number of allowed authentication failures defined in the local password policy. For more information, refer to [Local password policy \(on page 85\)](#).

Procedure

1. Go to **Users > Accounts**.
2. Ensure that the **Display users on domain** drop-down list points to **Local**.
3. Look for users with a lock icon (🔒) in the **Status** column.
4. Click the icon to unlock the account.
5. Confirm that you want to unlock the account.

7.4.5. Edit local user accounts

Procedure

1. Go to the **Users > Accounts** page.
2. Ensure that the **Display users on domain** drop-down list points to **Local**.



3. Click the name of the user account that you want to edit.
4. Click **Edit this user** and modify the necessary information.

If the "password" field is not changed, the user password is not modified.

5. Click **Apply**.

7.4.6. Export local user accounts

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** and the **List separator** from the dropdown lists.

The separator values must differ.

3. Select **Users** from the **Data** options.
4. Select the desired **Archive type**.

To import the file in WALLIX Bastion at a later time, the type must be csv.

5. Click **Export**.

7.4.7. Delete local user accounts

Procedure

1. Go to the **Users > Accounts** page.
2. Ensure that the **Display users on domain** drop-down list points to **Local**.
3. Select the user accounts that you want to delete.
4. Click **Delete**.
5. Confirm the permanent deletion of all the selected user accounts.

7.5. External sources management

Introduction

To prevent local user creation in WALLIX Bastion, users can be imported directly from LDAP, Active Directory (AD), Entra ID (ex Azure AD), AD, or any other IdP directory.

To integrate an LDAP, AD, Entra ID, or other IdP domains into WALLIX Bastion, you must configure both the external authentication and the external authentication domain. They are used to allow the connection to the directories

External authentication

External authentication methods are used to authenticate users. These methods are linked to user accounts during their creation, importation, or modification. WALLIX Bastion supports the following external authentication methods:

- Active Directory
- Kerberos Ticket
- Kerberos-Password
- LDAP
- PingID
- RADIUS
- SAML
- TACACS+

**Note:**

The default authentication configured on WALLIX Bastion is **local**. This authentication method allows users to log in using the product's internal data engine.

External authentication domains

An authentication domain lists the attributes of the directory schema to be used to find the attributes needed for a Bastion account. These attributes are listed in the various areas of the **Authentication domains** page.

WALLIX Bastion user account management can be used with one or more LDAP or Active Directory (AD) directories. When this is the case, user accounts are not stored locally in WALLIX Bastion. Instead, account information is retrieved from the directory whenever a user connects to a WALLIX Bastion service.

**Note:**

Configure TLS options to request a CA certificate for LDAP server authentication by editing the `/etc/ldap/ldap.conf` file. For more information on this file, refer to <http://www.openldap.org/software/man.cgi?query=ldap.conf>.

7.5.1. Import authentication domains

About this task

**Important:**

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the `#wab1040 domain` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	[R]equired [O]ptional	Description and expected values
Name	Text	R	[aA-zZ], [0-9], '-', '_', '' Name for the WALLIX Bastion domain
Label	Text	R if "Type" = AzureAD	[aA-zZ], [0-9], '-', '_', '' Label for Entra ID authentication button on WALLIX Bastion login page



Field	Type	[R]equired [O]ptional	Description and expected values
Type	Text	R	Type of the authentication domain "AzureAD" "LDAP" "AD"
Description	Text	O	Free text
Is default domain	Boolean	R	True or False Default value: False
Authentication domain	Text	R	[aA-zZ], [0-9], '-', '_', '' Name for the defined authentication domain
X509 authentication	Boolean	R if "Type" = LDAP or AD	True or False Default value: False
SAN email DN	Text	O	[aA-zZ], [0-9], '-', '_' LDAP/AD domain name for the defined SAN e-mail Empty if "Check X509 SAN email" = False
User authentications	Text	R	[aA-zZ], [0-9], '-', '_' External authentications defined At least one external authentication must be defined
User secondary authentications	Text	O	[aA-zZ], [0-9], '-', '_' External secondary authentications defined for the LDAP/AD domain



Field	Type	[R]equired [O]ptional	Description and expected values
Group attribute	Text	O	[aA-zZ], [0-9], '-', '_' Group attribute defined for the LDAP/AD domain Default value: <code>memberOf (AD) or (&(ObjectClass=posixGroup)(memberUid=\${uid})) (LDAP)</code>
Full name attribute	Text	O	[aA-zZ], [0-9], '-', '_' Full name attribute defined for the LDAP/AD domain Default value: <code>displayName (AD) or cn (LDAP)</code>
Public key attribute	Text	O	[aA-zZ], [0-9], '-', '_' Public key attribute defined for the LDAP/AD domain
Email attribute	Text	O	[aA-zZ], [0-9], '-', '_' E-mail attribute defined for the LDAP/AD domain Default value: <code>mail</code>
Language attribute	Text	O	[aA-zZ], [0-9], '-', '_' Language attribute defined for the LDAP/AD domain Default value: <code>preferredLanguage</code>
Default language	Text	R	Default language of the domain's members if the language is not defined in the directory. <code>de</code> (German), <code>en</code> (English), <code>es</code> (Spanish), <code>fr</code> (French), <code>ru</code> (Russian).
Default email domain	Text	R if "Type" = LDAP or AD	Default domain for the defined e-mail. Spaces and special characters are not allowed. Default value: <code>wallix.com</code>



Field	Type	[R]equired [O]ptional	Description and expected values
X509 condition	Text	O	Condition to match an LDAP/AD domain with the X.509 certificate. This condition is formatted according to the variables retrieved from the certificate.
X509 search filter	Text	O	LDAP/AD search filter to retrieve users in the domain. Expressed using LDAP filter syntax but any available variables as listed for field "X509 condition" can also be used.
Tenant ID	Text	R if "Type" = AzureAD	[aA-zZ], [0-9], '-', '_' Identifier of the Entra ID cloud tenant
Client ID	Text	R if "Type" = AzureAD	[aA-zZ], [0-9], '-', '_' Identifier of the Entra ID cloud client
Client Secret	Text	O	Secret shared between WALLIX Bastion and Entra ID Either the client secret or the association client certificate/client private key/passphrase must be defined
Client Certificate	Text	O	Certificate in PEM format shared between WALLIX Bastion and Entra ID Either the client secret or the association client certificate/client private key/passphrase must be defined
Client Private Key	Text	O	Private key in PEM format in relation with the certificate shared between WALLIX Bastion and Entra ID Either the client secret or the association client certificate/client private key/passphrase must be defined



Field	Type	[R]equired [O]ptional	Description and expected values
Passphrase	Text	O	Passphrase of the private key in relation with the certificate shared between WALLIX Bastion and Entra ID Either the client secret or the association client certificate/client private key/passphrase must be defined
Enable CA	Boolean	O	True or False Default value: False
Certificate Authority	Text	R if "Enable CA" = True	[aA-zZ], [0-9], '-', '_' Name of the CA in WALLIX Bastion

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select your preferred **Field separator** and **List separator** from the dropdown lists.

The separator values must differ. If you exported the CSV file, use the same separator values.

3. Select **Authentication domains** from the **Data** options.
4. Retrieve the CSV file from your computer.
5. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

7.5.2. Import user group mappings

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the `#wab1040 usersgroupmappings` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:



Field	Type	[R]equired [O]ptional	Description and expected values
Name	Text	R	[aA-zZ], [0-9], '-', '_' Canonical name for the WALLIX Bastion user group concerned by the mapping This user group must exist with a defined profile.
Domain Name	Text	O	[aA-zZ], [0-9], '-', '_' Canonical name for the authentication domain concerned by the mapping This domain must exist. If no domain name and no external group is specified, then all the existing mappings for the group are deleted during import.
External Groups	Text	O	In the context of an Entra ID domain, name of the external user groups. For example: ext_group1 ext_group2 "ext group3" IMPORTANT: If several groups are entered, then they must be separated by spaces. Additionally, if the name of the group includes one or more spaces, then it must be enclosed in double quotes (as shown in the previous example). In the context of an LDAP domain, rule allowing to define the users in the authentication domain mapped to the WALLIX Bastion user group. This rule indicates the value to map for the defined group attribute (that is, its full DN for "memberOf"). For example: <pre>'CN=Account Mapping users,CN=Users,DC=2008,DC=system,DC=enterprise'</pre> IMPORTANT: If this string includes spaces or commas, then it must be enclosed in simple quotes (as shown in the previous example). If no external group is specified, then all the existing mappings for the group/domain pair are deleted during import. If an external group is specified without an authentication domain, then the import fails.



Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Authentication domain mappings on user groups** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

7.5.3. Edit an external authentication

Procedure

1. Go to the **Configuration > External authentications** page.
2. Click the name of the external authentication that you want to edit.
3. Edit the necessary information.
4. Click **Apply**.

7.5.4. Edit an authentication domain

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Click the name of the authentication domain that you want to edit.
3. Edit the necessary information.
4. Click **Apply**.

7.5.5. Disable and unset X.509 certificate authentication

About this task



Attention:

When disabling X.509 certificate authentication, the web interface is restarted. That means, no user connections must be active.

Procedure

1. Go to the **Configuration > X509 configuration > Certificates** page.
2. Unselect **Enable X509 authentication** and click **Apply**.
3. Click **Unset X509 configuration**.

Results

Users can no longer log on using their certificates.

The default configuration is restored. The certificates are deleted and new auto-signed certificates are generated.

7.5.6. Delete an external authentication

About this task



Attention:

You cannot delete an external authentication if at least one user account is assigned to this authentication.

Procedure

1. Go to the **Configuration > External authentications** page.
2. Select the external authentications that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion of all selected external authentications.

7.5.7. Delete an authentication domain

About this task



Attention:

You cannot delete an authentication domain if at least one user group is mapped to this domain.

Procedure

1. Go to the **Configuration > Authentication domains** page.
2. Select the authentication domains that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion of all the selected authentication domains.



8. User communication

8.1. System notifications

8.1.1. Add connection messages for users

About this task

View and edit the messages displayed to users on primary and secondary connections according to their preferred language. These messages are displayed on:

- the web interface login screen
- the RDP proxy login screen
- the SSH terminal during authentication



Note:

These messages are not displayed to users for the following sessions: SFTP, SCP, or remote command (SSH_REMOTE_COMMAND) with an SSH key for primary authentication or a Kerberos ticket.

Procedure

1. Go to **Configuration > Connection messages** and click the language in which you want to write the messages.
2. Edit the message for **Primary connection**.
3. Edit the message for **Secondary connection**.
4. Click **Apply**.

8.1.2. Add a banner message

About this task

You can configure some alert, information, or warning messages to appear on the header of the web administration and user interfaces, and on the RDP and SSH selectors.

Procedure

1. Go to the **Configuration > Configuration options** page.
2. Click the **Global** option.
3. Under the **[banner]** section,
 - a. Add the text that you want to display to users in **Message**.
 - b. Choose the banner type that corresponds to the level of importance of your message.

Each type has a defined color-scheme and font weight which cannot be modified.
 - c. Click **Enable** to display the banner.



Tip:

To remove the banner, clear this option.

4. Click **Apply**.



8.2. E-mail notifications

WALLIX Bastion comes with default notifications in the form of e-mail templates. Each template is triggered by a different event and targeted to a different audience. Some notifications can be managed such as modifying the trigger conditions, deactivating the trigger altogether, or defining a list of recipients. Other notifications are non-manageable and cannot be deactivated. For more information, refer to [List of default e-mail notifications \(on page 101\)](#)

WALLIX Bastion also provides the option to create new templates, either for new events or for translation or branding purposes. For more information, refer to [Custom notification templates \(on page 105\)](#).

8.2.1. List of default e-mail notifications

To display the list of all notification templates, you can run the following command as root:

```
ls /usr/lib/python3/dist-packages/wallixgenericnotifier/templates/mail/
```

Notifications automatically sent to all users

This type of notification is automatically sent and cannot be deactivated. Notifications are sent to the e-mail address defined in the user preferences.

New account

An e-mail is sent to local users whose account was created.

Default template: `account_created.txt`

Locked account

An e-mail is sent to local users whose account is locked (for example, because of too many failed authentication attempts).

Default template: `locked_account.txt`

Expired account

An e-mail is sent to local users whose account expired because it reached the value set for **Account expiration date**.

Default template: `expired_account.txt`

Password expiration

An e-mail is sent to local users whose password is about to expire or is already expired because of the local password policy.

If the local password policy defines a password expiration warning, local users whose password expire within the specified number of days receive the e-mail. If there is no password expiration warning defined, only a password expiration, users receive an e-mail only when their password is expired.

Default template: `password_expiration_info.txt`

GPG key

Users with a profile that grants the **Execute** right on the **Credential recovery** feature must have a GPG key. When users with this executive right do not have a GPG key defined, a daily warning e-mail is sent to them.



The sending of this e-mail notification can be deactivated. For more information, refer to [Disable missing GPG key e-mail notification \(on page 109\)](#).

Default template: `gpg_request.txt`

Notifications with manual activation for specific recipients

This type of notification is not automatically sent. To send a notification, you need to configure and activate a notification in WALLIX Bastion for the type of event you want to send. Notification e-mails are then sent to the e-mail addresses defined in the **Recipient emails** field for the desired event. For more information on how to set up notifications, refer to [Configure e-mail sending for event notifications \(on page 108\)](#).

Reporting

An e-mail is sent daily with a metrics report.

Default template: `daily_reporting.txt`

Primary connections

Password has expired

An e-mail is sent with the list of all local users with expired passwords.

Default template: `password_expired.txt`

Authentication failure

An e-mail is sent with information concerning all failed user attempts to log in to WALLIX Bastion.

Default template: `primary_cx_failed.txt`

Secondary connections

Target connection failure

An e-mail is sent with information concerning all failed attempts to log in to a target.

Default template: `secondary_cx_failed.txt`

Session or password checkout on critical target

For authorizations that have the **Critical targets** option activated, enabling this event type generates a notification when any critical target is accessed by users.

Default template: `cx_equipment.txt`

New SSH key fingerprint saved

An e-mail is sent each time a new SSH key fingerprint is added.

Default template: `new_fingerprint.txt`

Wrong SSH key fingerprint detected

An e-mail is sent each time there is a failed SSH key fingerprint detected.

Default template: `wrong_fingerprint.txt`

Pattern(s) detected in the SSH flow



An e-mail is sent each time a flagged pattern is detected during an SSH session.

Default template: `pattern_found.txt`

Pattern(s) detected in the RDP flow

An e-mail is sent each time a flagged pattern is detected during a RDP session.

Default template: `rdp_pattern_found.txt`

Process detected in the RDP session

An e-mail is sent each time a flagged process is detected during a RDP session.

Default template: `rdp_process_found.txt`

Outbound connection detected in the RDP session

An e-mail is sent each time an outbound connection is detected during a RDP session.

Default template: `rdp_outcxn_found.txt`

Session files

Integrity error

An e-mail is sent with a summary for all corrupted or missing trace logs for a RDP or SSH session. The summary contains all errors for the number of days defined in **Session log policy**.

Default template: `integrity_error.txt`

Session purge

An e-mail is sent with a summary for archived and removed sessions.

Default template: `sessionlog_purge.txt`

System information

RAID error

For physical appliances.

Default template: `raid_error.txt`

No available space on external storage

An e-mail is sent when space is limited on the remote storage.

Default template: `external_storage_full.txt`

Not enough space on filesystem (90% full)

An e-mail is sent as a disk space alert.

Default template: `filesystem_full.txt`

Disk space is full (< 100MiB), emergency shutdown of all proxy servers

An e-mail is sent to warn of the shutdown of all proxy servers due to critical disk space consumption.



Default template: `disk_space_critical.txt`

Watchdog notifications

An e-mail is sent when the embedded controller notices a change of state for WALLIX Bastion.

Default templates:

- `watchdog_back_to_normal.txt`
- `watchdog_service_restarted.txt`
- `watchdog_wab_out_of_order.txt`

License warning

Several e-mails are sent whenever a license metrics is reached.

Default templates:

- `licence_expired.txt`
- `licence_invalid.txt`
- `licence_primary_cx_error.txt`
- `licence_quota_exceeded.txt`
- `licence_quota_warning.txt`
- `licence_secondary_cx_error.txt`
- `licence_waapm_cx_error.txt`
- `licence_will_expire.txt`
- `license_percentage_warning.txt`

Additional feature notifications

This type of notification is linked to specific features. They are managed independently. For more information on each notification, refer to the dedicated feature documentation.

Notification tests

A test notification which can be sent through the **SMTP server** page.

Default template: `notification_test.txt`

Local password policy

If the **Days before expiration** value is modified to a lesser value, an e-mail is sent out to all users whose password becomes expired at their next login.

Default template: `password_expiration_policy.txt`

Approval workflow

The approval workflow feature provides some notifications for different events.

Default templates:

- `approval_accepted_approver.txt`
- `approval_accepted_user.txt`
- `approval_auto_approver.txt`
- `approval_cancelled_approver.txt`
- `approval_cancelled_user.txt`
- `approval_closed_approver.txt`
- `approval_closed_user.txt`



- `approval_pending_approver.txt`
- `approval_pending_user.txt`
- `approval_rejected_approver.txt`
- `approval_rejected_user.txt`

Secret rotation

The secret rotation feature provides notifications for some events.

Default templates:

- `credential_change_failure.txt`
- `credential_change_success.txt`
- `credential_change_summary.txt`

HA Database Replication

The HA Database Replication feature provides notifications for some events. The list of recipients is configured with the related script.

Default templates:

- `ha_master_fault.txt`
- `ha_master_up.txt`
- `ha_slave_missing.txt`

Discovery

The assets discovery module provides some notifications. The list of recipients is configured when creating a scan configuration.

Default templates:

- `discovery_ad_for_accounts_error.txt`
- `discovery_ad_for_accounts_success.txt`
- `discovery_ad_for_devices_error.txt`
- `discovery_ad_for_devices_success.txt`
- `discovery_devices_for_accounts_error.txt`
- `discovery_devices_for_accounts_success.txt`
- `discovery_networks_for_devices_error.txt`
- `discovery_networks_for_devices_success.txt`
- `discovery_notification_ad_error.txt`
- `discovery_notification_network_error.txt`

8.2.2. Custom notification templates

What is a custom notification template?

You can create custom notification templates from the command line to modify the subject and body of the notifications to meet your requirements or to send notifications in HTML format.

After a custom notification template is created, the notification is sent based on the following order:



1. The custom notification in the user's language as set in WALLIX Bastion if a corresponding template exists. For example: `approval_pending_user_fr.txt`
2. The custom notification in English if a corresponding template exists. For example: `approval_pending_user_en.txt`
3. The default notification of WALLIX Bastion in the user's language. For example: `approval_pending_user.txt`

Template body rules

A custom template must abide by a set of rules:

- The first line corresponds to the subject of the notification. It must fit on a single line.
- The second line must contain two consecutive hyphens that indicate the separation between the subject and the body of the notification. They will not be displayed in the mail received by the user.
- The other lines correspond to the body of the notification.

You can use the same variables in your custom notifications as in the default notifications. Their format must be as follows: `{{name}}`. The following tables list these variables.

Table 1. Additional variables available for any custom notification

WALLIX Bastion's variables	Description
<code>{{ product_name }}</code>	Product name (WALLIX Bastion by default)
<code>{{ product_name_short }}</code>	Short version of the product name (Bastion by default)
<code>{{ product_support_name }}</code>	Name of the Support Team (WALLIX by default)
<code>{{ notifier.ip }}</code>	WALLIX Bastion user interface's IP address
<code>{{ notifier.hostname }}</code>	WALLIX Bastion's hostname
<code>{{ notifier.fqdn }}</code>	WALLIX Bastion's FQDN (if the FQDN is not set, the hostname is used by default)

Table 2. Variables for users requesting approval (`approval_*_user.txt` templates)

WALLIX Bastion's variables	Description
<code>{{ answer_user }}</code>	Name of the approver (for a notification sent after an answer)
<code>{{ approvers }}</code>	Comma-separated list of approver names who accepted the approval request
<code>{{ begin }}</code>	Start time (format: YYYY-MM-DD hh:mm)
<code>{{ duration }}</code>	Duration, in time units (h for hours, m for minutes)
<code>{{ end }}</code>	End time (format: YYYY-MM-DD hh:mm)
<code>{{ name }}</code>	Name of the user asking for approval
<code>{{ reason }}</code>	Reason given by the approver (for a notification sent after an answer)
<code>{{ target }}</code>	Target name

Table 3. Variables for approvers (`approval_*_approver.txt` templates)

WALLIX Bastion's variables	Description
<code>{{ approval_uid }}</code>	UID of the approval request

Table 3. Variables for approvers (approval_*_approver.txt templates) (continued)

WALLIX Bastion's variables	Description
{{ approvers }}	Comma-separated list of approver names who accepted the approval request
{{ begin }}	Start time (format: YYYY-MM-DD hh:mm)
{{ duration }}	Duration, in time units (h for hours, m for minutes)
{{ end }}	End time (format: YYYY-MM-DD hh:mm)
{{ reason }}	Approval comment (- if not set)
{{ target }}	Target name
{{ ticket }}	Approval ticket (- if not set)
{{ user }}	Name of the user asking for approval



Note:

If the list of approvers is not found, WALLIX Bastion uses the list of emails set by the administrator in the **Email list** field, available in the **Groups** page.



Tip:

If necessary, add the <html> element in the template to send a custom notification in the HTML format.

Example of a valid custom notification template

```
Your access request on {{ target }}
--
Target: {{ target }}

between {{ begin }} and {{ end }} ({{ duration }})

Your access request has been sent.

You will be promptly notified after your request is reviewed.
--
Your {{ product_name_short }} administrator.
```

Example of a valid custom notification template on HTML format

```
Your access request on {{ target }}
--
<html>
Target: {{ target }}
<br>
between {{ begin }} and {{ end }} ({{ duration }})
<br><br>
Your access request has been sent.
<br>
You will be promptly notified after your request is reviewed.
<br><br>
--
<br>
Your {{ product_name_short }} administrator.
</html>
```



8.2.2.1. Create custom notification templates

Procedure

1. Connect in SSH to the 2242 port as root.

```
wabadmin$ super
[sudo] password for wabsuper:
wabsuper$ sudo -i
[sudo] password for wabsuper:
```

2. Create a notification template in .txt format in the directory /var/wab/etc/notifier/.



CAUTION:

The name of the custom notification templates must be the same as the name of the default notification templates, followed by the language suffix. For example: approval_pending_user_en.txt.

The ownership of the custom notification templates must be set to root:wabuser . Every file in /var/wab/etc/notifier/ must be owned by root:wabuser using chown command.

3. Customize the notification template according to your needs.

To know the rules to follow, refer to [Template body rules \(on page 106\)](#).

8.2.3. Change sender for e-mail notifications

About this task



Note:

You cannot have different senders for different e-mail notifications.

Procedure

1. Go to the **System > SMTP server** page.
2. Modify the value for **Sender name** or **Sender email** depending on which you want to modify.
3. Click **Apply**.

8.2.4. Configure e-mail sending for event notifications

Procedure

1. Go to the **Configuration > Notifications** page.
2. Click **Add**.
3. Give the new notification a name and provide an optional description.
4. Choose to enable or disable the sending of e-mails for this notification.

By default, the **Enable notification** option is selected. If you do not want to send e-mail notifications yet, disable this option.

5. Add the e-mail addresses of the expected recipients. There is no limit to the number of recipients.

You can add new e-mail addresses by clicking **Add**. Any e-mail can be removed from the list by clicking the - icon next to the e-mail address.



6. Define the language in which the notification is sent to the recipients.
7. Select the event types which trigger this new notification.
8. Click **Apply**.

8.2.5. Edit e-mail sending for event notifications

Procedure

1. Go to the **Configuration > Notifications** page.
2. Click the name of the notification that you want to edit.
3. Edit the necessary information.

You can disable the sending of a notification, manage the list of recipients, modify the language for the notification, or manage the type of events selected for this notification. However, the name of a notification cannot be modified.

4. Click **Apply**.

8.2.6. Disable missing GPG key e-mail notification

About this task

By default, users who must provide a GPG key receive a daily warning e-mail if they do not have one configured on their preferences. You can deactivate the daily sending of that warning e-mail.

Procedure

1. Go to the **Configuration > Configuration options > Global** page.
2. Inside the **[main]** section, deactivate the **Missing GPG key warning email** option.
3. Click **Apply**.

8.2.7. Delete an e-mail notification trigger

Before you begin



Important:

Only notification with a manual activation can be deleted. For more information, refer to [List of default e-mail notifications \(on page 101\)](#).

Procedure

1. Go to the **Configuration > Notifications** page.
2. Select the notifications that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion of all selected notifications.



9. Devices

What are Devices?

A device is characterized by a physical or virtual equipment for which WALLIX Bastion manages the access to sessions or passwords.

9.1. Create a new device

Procedure

1. Go to the **Targets > Devices** page.
2. Click **Add** to display the device creation page.
3. Give the device a name.

This is the name users use to access the device. It can be unrelated to the machine's DNS name. An existing name cannot be assigned to another device.

4. **Optional:** Provide an alias to the device name.

The device name has priority over the alias. An existing alias cannot be assigned to another device.

5. Enter the device IP address, FQDN, or subnet (it corresponds to a network address).

You can also define a set of targets belonging to a subnet. It is achieved by entering a subnet instead of the IP address during the creation of device by using a CIDR notation (<network address>/<number of mask bits>). For example, 192.168.0.15/24.

6. **Optional:** Give the device a description to simplify management.
7. Click **Apply**.

Results

You have a new device registered on the Bastion. You can further configure the device with the following procedures.

Related information

[Manage services for a device \(on page 110\)](#)

[Manage local domains associated with a device \(on page 111\)](#)

[Manage local accounts on the device \(on page 111\)](#)

[Manage the target groups associated with the device \(on page 113\)](#)

9.2. Manage services for a device

About this task

The **Services** tab allows you to list, add, edit, and delete services which can be accessed on this device.

Procedure

1. Go to the **Targets > Devices** page.
2. Click the name of the device that you want to edit.
3. Switch to the **Services** tab.
4. Click  **Add** and select the desired protocol from the list.
5. Provide the service name.

This is the name users use to access the service. The name can be unrelated to the protocol name and the port number.



6. Set the default port.
7. Select a connection policy defining the authentication mechanism for the service on this device.
For more information, refer to [Connection policies \(on page 134\)](#).
8. **Optional:** To create targets for applications and clusters, select a global domain.
9. **Optional:** For RDP and SSH connections, choose proxy options.

For more information, refer to [SSH options \(on page 254\)](#) and [RDP options \(on page 252\)](#).

10. Click **Apply and close**.



Tip:

If you want to add more than one specific service, you can repeat this process as many times as necessary.

What to do next

After you added a service, you have the possibility to add it to a group to configure a target group for session management through account mapping or interactive login.

To add a service to a group, select the concerned service and click **Add to group**. A window opens and allows you to enter and select the following fields:

- the group name: you can select an existing group or create a new one
- a description
- the target type: either account mapping or interactive login
- the services

After clicking **Add and continue**, the data is saved and you have the possibility to associate the service with another group and/or target type. Otherwise, click **Add and close** to save the data and close the window.



Tip:

The resource associations can also be managed from the **Groups** page (for more information, refer to [Create a target group \(on page 167\)](#)).

9.3. Manage local domains associated with a device

The **Local domains** tab allows you to list and delete local domains associated with the device.

These local domains are associated with the device from:

- the **Local accounts** tab on the **Devices** page or
- the device account creation page of the **Accounts** page which can be accessed from the **Targets** menu (for more information, refer to [Add a target account to a device \(on page 160\)](#))

9.4. Manage local accounts on the device

About this task

The **Local accounts** tab allows you to list, add, edit and delete local accounts on the device.



Procedure

1. Go to the **Targets > Devices** page.
2. Click the name of the device that you want to edit.
3. Switch to the **Local accounts** tab.
4. Click **+ Add**.
5. Configure the general information of the local account .
 - a. Select an existing local domain or create a new one to associate with the device.
 - b. Set the account name. This is the name users use to access the local account.
 - c. Set the account login.
 - d. **Optional:** Provide a description of the local account.
 - e. Select the relevant checkout policy.
 - f. Choose to activate or deactivate the **Automatic password change** and the **Automatic SSH key change** options.
 - g. Click **Apply**.
6. Switch to the **Password** tab.
 - a. Enter a password and its confirmation.
 - b. Enable or disable the manual change of the password and its propagation on the target
 - c. Click **Apply and continue**.
7. Switch to the **SSH private key** tab and choose between generation and uploading.
 - For private key generation, select the relevant signature system of the private key. Click **Apply and continue** and download the corresponding SSH public key in the OpenSSH or ssh.com format.
 - For private key uploading, upload the SSH private key in the OpenSSH or PuTTY format and provide the corresponding passphrase (if any was defined). You can also enable or disable the manual change of the SSH private key and its propagation on the target. Click **Apply and continue** and download the corresponding SSH public key in the OpenSSH or ssh.com format.
8. Click **Close**.

What to do next

When you added a local account on the device, you have the possibility to add it to a group to configure:

- a target group for session management from an account (for more information, refer to [Configure a target group for session management from an account in the vault \(on page 168\)](#))
- a target group for session management for a scenario account (for more information, refer to [Configure a target group for a scenario account during SSH session \(on page 168\)](#))
- a target group for password management from an account (for more information, refer to [Configure a target group for password management from an account in the vault \(on page 170\)](#))

To add a local account to a group, select the concerned local account, then click **Add to group**. A window opens and allows you to enter and select the following fields:

- the group name: you can select an existing group or create a new one
- a description
- the target type: either account for session management or scenario account for session management or account for password management
- the service (if it is required for the selected target type)
- the local accounts

After clicking **Add and continue**, the data is saved and you have the possibility to associate the local account with another group and/or target type and/or service. Otherwise, click **Add and close** to save the data and close the window.

**Tip:**

The resource associations can also be managed from the **Groups** page (for more information, refer to [Target groups \(on page 167\)](#)).

9.5. Manage the target groups associated with the device

The **Groups** tab allows you to list, edit and delete resource associations which already exist with the device.

**Note:**

Target accounts and services must exist for the device to manage associations.

By clicking a group name, you are redirected to the data modification page of this group. You can then configure, edit, or delete the data related to this group. For more information, refer to [Target groups \(on page 167\)](#).

9.6. Import devices

About this task

**Important:**

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the #wab1040 resource tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(quired) O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_'
Alias	Text	O	Free text
Description	Text	O	Free text
Host	IP/ FQDN/Subnet	R	[aA-zZ], [0-9], '-', '/', ':' For example, for subnet: 1.1.1.0/24



Field	Type	R(equired) O(ptional)	Possible values
Local domains	Text	O	Local domains created using the association with a device or a target account There can be 0 local domain, one or several local domains (created on this device).
Services	Text	O	To specify a global domain for a subprotocol, respect the following pattern: <pre>name/PROTOCOL/port/connection_policy/ my_global_domain/subprotocol1 subpro- tol2</pre> If there is no global domain, respect the following syntax: <pre>name/PROTOCOL/port/connection_policy/ subprotocol1 subprotocol2</pre> name Free text PROTOCOL Protocol name⁽¹⁾ port Port number (optional) connection_policy Connection policy name subprotocol Subprotocol name⁽²⁾ (optional)



Field	Type	R(equired) O(ptional)	Possible values
Multi-tunneling infos	Text	O	Information about Multi-tunneling defined for the device. Each information is separated by a space. <pre>service_name/multi-tunneling/seamless_connection/interfaces</pre> service_name Name of the service RAW TCP/IP multi-tunneling True or False seamless_connection True or False interfaces list of additional interfaces with the syntax ip:port separated by a pipe character (). For example, RAWTCPIP/True/True/10.10.10.2:2000 10.10.10.2:40 10.10.20.10:50

(1) Protocol

One of the following values: SSH, TELNET, RLOGIN, RDP, VNC, RAWTCPIP.

(2) Subprotocol for SSH

One of the following values: SSH_SHELL_SESSION, SSH_REMOTE_COMMAND, SSH_SCP_UP, SSH_SCP_DOWN, SSH_X11, SFTP_SESSION, SSH_DIRECT_TCPIP, SSH_REVERSE_TCPIP, SSH_AUTH_AGENT, SSH_DIRECT_UNIXSOCK, SSH_REVERSE_UNIXSOCK.

For more information, refer to [SSH options \(on page 254\)](#).

(2) Subprotocol for RDP

One of the following values: RDP_CLIPBOARD_UP, RDP_CLIPBOARD_DOWN, RDP_CLIPBOARD_FILE, RDP_PRINTER, RDP_COM_PORT, RDP_DRIVE, RDP_SMARTCARD, RDP_AUDIO_OUTPUT, RDP_AUDIO_INPUT.

For more information, refer to [RDP options \(on page 252\)](#).

If a subprotocol is not specified, all the subprotocols are added. The value for the other protocols is exactly the same as PROTOCOL and can be omitted. To specify several subprotocols in the same protocol, separate subprotocols using a pipe character (|) such as

```
rdp/RDP/3389/RDP//RDP_CLIPBOARD_UP|RDP_CLIPBOARD_DOWN|RDP_PRINTER|RDP_SMARTCARD
```

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.



3. Select the **List separator** from the dropdown list.
4. Select **Devices** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

9.7. Edit a device

Procedure

1. Go to the **Targets > Devices** page.
2. Click the name of the device that you want to edit.
3. Switch to the relevant tab and edit the necessary information.

9.8. Use tags to organize devices

What are Tags?

Tags are used to organize the devices listed in this table to allow you to quickly identify the devices on which actions must be performed. Each device can have a maximum of 64 tags.

A tag is composed of a key (limited to 512 characters) and a value (limited to 256 characters). Keys and values are case sensitive and accept UTF-8 characters. Spaces are forbidden at the beginning and end of a key or value.



Important:

A tag cannot be edited. To change a key or a value, you must delete the tag and create a new one.

Using tags

From the **Devices** page on the **Targets** menu, you can view all the tags associated to your devices, and add and remove tags. You can also filter devices using tags from the **Tags** column.

Click the  icon in the header of the **Tags** column to display the search field. By clicking in this field, you access a list of all the tag keys and tag values existing in WALLIX Bastion. Enter then select the key or the value of the desired tag and click **Search**. The devices corresponding to the filter are listed in the table. An active filter is symbolized by the orange icon .

To delete a filter, click the  icon at the top right of the table or click the  icon then click the **Restore** button.



Attention:

If you delete a device, the associated tags are also deleted.



9.8.1. Manage the tags for a device

Procedure

1. Go to the **Targets > Devices** page.
2. Click the name of the device for which you want to manage tags.
3. Open the **Tags** tab.
4. To add a tag to the device,
 - a. Click **Add tags**.
 - b. From the **Add tags to devices** dialog, enter a new **Key** or select an existing key.

If you create a new key, click **Add item {key_name}** to select it.
 - c. Enter a value or select an existing value if the key already exist.

If you create a new value, click **Add item {key_name}** to select it.
 - d. Click **Add and close** to apply tags and close the window, or click **Add and continue** to apply and add another tag to the selected devices.
5. To remove tags from the device,
 - a. Select one or more tags.
 - b. Click **Delete**.
 - c. Confirm the removal from the selected devices.

9.8.2. Add tags to multiple devices

About this task



Attention:

It is not possible to add tags with identical keys on the same device.

Procedure

1. Go to the **Targets > Devices** page.
2. Select the devices to which you want to apply a tag.
3. Click **Add tags**.
4. From the **Add tags to devices** dialog, create a new or choose an existing **Key**.

To create a new key, enter the name and click **Add item {key_name}**.
5. Create a value or select an existing value for the selected key.

To create a new value, enter the name click **Add item {key_name}** to select it.
6. Click **Add and close** to apply tags and close the window, or click **Add and continue** to apply and add another tag to the selected devices.

9.8.3. Remove tags from multiple devices

Procedure

1. Go to the **Targets > Devices** page.
2. Select several devices from which you want to remove one or more tags.
3. Click **Remove tags**.
4. From the **Remove tags to devices** dialog, select one or more keys or values that you want to remove.



Removing a key or a value removes it from all the selected devices.

Selecting a key removes all the values for that key.

5. Click **Remove and close** to remove the keys and values from the selected devices and close the window.

9.9. View and delete certificates or keys on the device

From the **Devices** page, click a device name to display the device data and click the **Certificates** tab to view the list of certificates or keys on this device. A user is allowed to display the certificates on the device if the **View** right for the **Targets & accounts** feature is set in their profile.

To delete a certificate or a key, select the certificate or the key you want to delete, then click **Delete**. A user is allowed to delete the certificates on the device if the **Modify** right for the **Targets & accounts** feature is set in their profile.

For more information on user rights, refer to [Permission profiles \(on page 22\)](#).

9.10. Change target servers identification

When you connect to a target server through a secure protocol (such as RDP or SSH), WALLIX Bastion checks that the certificate or key presented to the proxy by the server corresponds to the one known for this server. If this certificate or key is different, the WALLIX Bastion proxy closes the connection as it can be considered an attack. As a result, it is necessary to inform WALLIX Bastion when this certificate or key is changed.

To do so, you can delete the declared certificate or key on the device and the new one is automatically saved at the next access to the device through the RDP or SSH proxy. For more information, refer to [View and delete certificates or keys on the device \(on page 118\)](#).

9.11. Delete a device

About this task



Attention:

You cannot delete a device on which target accounts are declared.

Procedure

1. Go to the **Targets > Devices** page.
2. Select the devices that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected devices.

10. Applications

What are Applications?

WALLIX Bastion enables you to manage application sessions through a standard jump server (based on Windows), on which applications are installed.

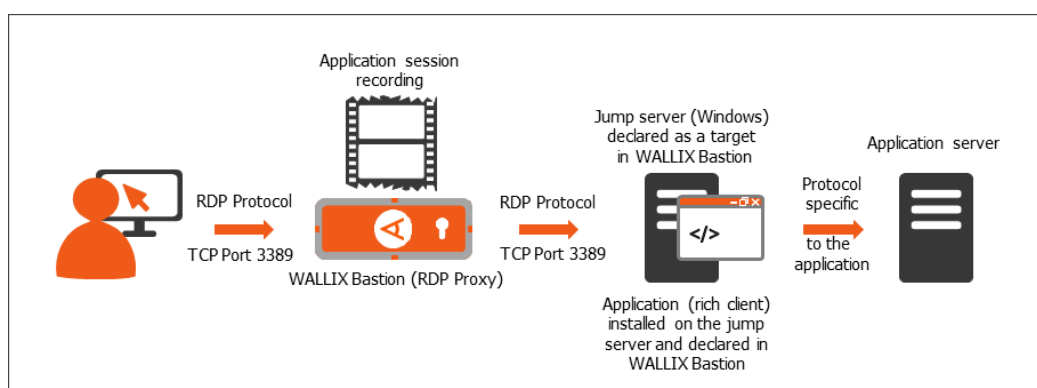
The user connects to WALLIX Bastion and chooses a standard application from the selector. WALLIX Bastion then initiates an RDP session and automatically launches the application. The application session is then recorded as an RDP session.



Important:

It is not possible to run a standard application associated with a target running on a Windows 10 operating system as the remote desktop service does not support the **alternate shell** function.

Application session flow



10.1. Add a standard application

Procedure

1. Go to the **Targets > Applications** page.
2. Click **Add**.
3. Give the application a name and an optional description.
4. Provide the parameters for the application.

Parameters are the command line arguments which are concatenated to the standard application path. To insert the user name, password and standard application ID, the variables `${USER}`, `${PASSWORD}`, and `${APPID}` are used for the corresponding value. WALLIX Bastion automatically replaces them with the appropriate information related to the account selected by the user and the application ID.

5. Select the relevant connection policy.
6. Select the relevant target or cluster.
7. Select one or more relevant global domains
8. Add one or more local domains.
9. Enter the the path of the application executable and the directory in which the standard application runs.

For a cluster, these values must be provided for each device. For more information, refer to [Clusters \(on page 268\)](#).

10. Click **Apply**.

Results

The following screenshot shows the configuration of an Hypervisor application.

What to do next

To enable users to connect to the standard application, accounts must be associated with it, as described in [Target accounts \(on page 158\)](#). User access rights are managed using authorizations. As a result, the RDP protocol must be used.

10.2. Add an account to a standard application

Procedure

1. Go to the **Targets > Applications** page.
2. Select the standard applications that you want to edit.
3. Expand the **Application accounts** area to display the list of the accounts associated with the standard application.
4. Click **Add an account**.

For more information on how to configure the account, refer to [Add a target account to an application \(on page 160\)](#).

5. Click **Apply** to save the configuration.

10.3. Manage the resource associations with a standard application

Procedure

1. Go to the **Targets > Applications** page.
2. Select the standard applications that you want to edit.
3. Expand the **Associated accounts** area to display the list of the accounts associated with the standard application.
4. Click **Manage association**.
5. Move desired resources from the **Available accounts** frame to the **Selected accounts** frame to perform the association. You can also remove a resource from the **Selected accounts** frame by doing the opposite.
6. Click **Apply** to save the configuration.



10.4. Import applications

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the `#wab1040 application` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(equired) O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_'
Description	Text	O	Free text
Local domains	Text	O	There can be no local domain, one or several local domains created on this application
Global domains	Text	O	There can be no global domain, one or several existing global domains
Target/Cluster	Text	R	Format for an application on a device: <code>account@domain@my_ device:rdp</code> , rdp being the name of the protocol defined on the device Format for an application on a cluster: name of the cluster
Parameters	Text	O	Command line arguments. The variables <code>\${USER}</code> , <code>\${PASSWORD}</code> and <code>\${APPID}</code> can be used to insert the user name, password and application ID.
Paths	Text	R	For an application on a device: path of the application For an application on a cluster: target1='path1' target2='path2' , for each target of the cluster, with target1 in format account@domain@my_ device:rdp
Startup directories	Text	O	For an application on a cluster: target1='wdir1' target2='wdir2'



Field	Type	R(equired) O(ptional)	Possible values
Connection policy	Text	O	Name of the connection policy on the RDP protocol Default value: RDP

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Applications** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

10.5. Edit a standard application

Procedure

1. Go to the **Targets > Applications** page.
2. Select the standard applications that you want to edit.
3. Click **Edit this application** and edit the necessary information.
4. Click **Apply**.

10.6. Delete a standard application

About this task



Attention:

You cannot delete a standard application on which target accounts are declared.

Procedure

1. Go to the **Targets > Applications** page.
2. Select the standard applications that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected standard applications.

10.7. Configure the jump server

Servers from Windows Server 2003 are supported as jump servers. From Windows Server 2008, the "Terminal Services" or "Remote Desktop" role must be installed.



Attention:

After the 120-day grace period, Client Access Licenses (CAL) must be installed to continue using these services.

You must provide the user with the right to launch the application. This can be done by providing access to unlisted programs or by adding the application to the authorized programs.

When using the session probe mode, it is necessary to publish the command prompt (cmd.exe) as the RemoteApp program. For more information regarding this mode and its configuration, we strongly recommend that you refer to [Session probe mode \(on page 138\)](#).

Providing access to unlisted programs

1. Click the **Start** menu.
2. Select **All Programs > Administrative Tools > Remote Desktop Services** and then click **RemoteApp Manager**.
3. In the **Overview** frame, click **Change Terminal Server Settings**.
4. On the **Terminal Server** tab, in the **Access to unlisted programs** frame, select **Allow users to start both listed and unlisted programs on initial connection**.

Adding the application to listed programs

1. Click the **Start** menu.
2. Select **All Programs > Administrative Tools > Remote Desktop Services** and then click **RemoteApp Manager**.
3. In the **Actions** frame, click **Add RemoteApp Programs**.
4. Choose the application from the list by checking the corresponding box and edit the application properties to allow the use of all command line arguments.

Further configuration

It is recommended to set the smallest possible value as the maximum period during which a disconnected user session is kept active on the server running Terminal Server. To do this, you can proceed as follows:

1. Click the **Start** menu.
2. Select **All Programs > Administrative Tools > Remote Desktop Services** and then click **Remote Desktop Session Host Configuration** to set the timeout to 1 minute. To do this:
 - in the **Connections** frame, select the **RDP-Tcp** connection
 - on the **Sessions** tab, select **Override user settings** and set the value in the **End a disconnected session** field to 1 minute.

You can also use group policies to manage this setting.

You can allow several connections with the same target account on a jump server. Under Windows Server 2008 or later:

1. Click the **Start** menu.
2. Select **All Programs > Administrative Tools > Remote Desktop Services** and then click **Remote Desktop Session Host Configuration**.
3. In the **Edit settings** frame, under **General**, double-click **Restrict each user to a single session** and deselect the check box.



Alternatively, you can use the corresponding setting with an account policy. Under Windows Server 2012 or later, you must set an additional setting to allow access to a client that does not use network-level authentication. To do this:

1. Open the **Server Manager** application and select **Remote Desktop Services**.
2. Select the needed collection in **Collections**. **Quick Session Collection** corresponds to the default collection.
3. In the **Properties** frame, select **Edit Properties**.
4. In the **Security** section, deselect the **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)** check box.

10.8. Configure the application launch using RemoteApp mode

The RemoteApp mode makes standard applications that are accessed remotely through RDP appear as if they are running on the user's local computer. That means this mode allows to start a remote desktop session that appears as a single application window. Instead of being presented to the user in the desktop of the RDP client, the RemoteApp application is integrated with the client's desktop. The RemoteApp application runs in its own resizable window, can be dragged between multiple monitors, and has its own entry in the taskbar.

The RemoteApp mode is enabled by default when accessing standard applications. This parameter can be managed through **Configuration > Configuration Options > GUI (Legacy)**, then select/deselect the option "**Rdp remote app mode**".

The window resizing is enabled by default for the RemoteApp application. This parameter can be managed through **Configuration > Configuration Options > RDP proxy**, then select/deselect the option **Allow resize hosted desktop** under the **remote program** section. When this functionality is enabled, a pin icon is displayed on the right upper part of the RemoteApp window hosting the classic RDP session. The window can be resized when the pin points to the left.

The RemoteApp session closes 20 seconds after the last window or taskbar icon is closed. This period can be shortened by defining a time period before the display of a disconnect message to close the session. This period can be set on the field **Remote programs disconnect message display** on the configuration page related to the connection policy for the RDP protocol. This page can be accessed from .

On the other hand, it can be necessary to convert RemoteApp session to Alternate Shell session to access a published RemoteApp application via a jump server for a session initiated by Access Manager. This can be done by selecting the option **Wabam uses translated remotapp**, under the section **rdp**, on the configuration page related to the connection policy for the RDP protocol. This page can be accessed from **Session Management > Connection Policies**.



Attention:

This field is displayed when the check box of the **Advanced options** field at the top right of the page is selected. It must only be changed when instructed by the WALLIX support team.

 Important:

The RemoteApp sessions of a user connected simultaneously on one or several standard applications are split by default when displayed from the "Current Sessions" and "Session History" pages under the "Audit" menu). If the option "**Rdp enable sessions split**" (accessible from **Configuration > Configuration Options > GUI (Legacy)** under the **main** section) is deselected, it can be possible to get an overlay view of these sessions.

The client Remote Desktop Connection (MSTSC) connected to Windows Server 2008 or 2012 does not allow several RemoteApp programs to share the same RDP session. There is as many RDP sessions created as the number of RemoteApp programs launched.

Display issues related to the Microsoft client were reported when using RemoteApp mode and multiple monitors. Dysfunctions occur when the primary monitor is not located in the upper left part of the virtual screen. The recommended workaround is to locate the primary monitor in the upper left part of the virtual screen. For more information on virtual screens, refer to the [official Microsoft documentation](#).

The session probe mode can be used to run the standard applications defined in the Bastion. This operating mode provides the benefit of blocking the launch of child processes. This is not the case when using the RemoteApp native mode. However, the restrictions defined during the creation of the RemoteApp program in Windows (which may concern user groups, command-line arguments allowed, etc.) will not apply. This mode can be managed using **Session Management > Connection Policies > RDP**, then selecting/clearing the **Use session probe to launch remote program** option under the **rdp** section. For more information regarding the session probe mode, refer to [Session probe mode \(on page 138\)](#).

10.9. Automate connections to an application using Autolt scripts

About this task

Business applications usually implement an authentication screen to allow a user to only access the needed data. The authentication step verifies the login and the password manually entered by this user. That means the user has knowledge of this sensitive information.

To restrict the disclosing of such information, we recommend using Autolt scripts. These scripts are supported by WALLIX Bastion and can be used, in particular, to fill in credential forms automatically. With this process, the credential information of the application is retrieved through the RDP virtual channel. In such a case, the user does not have access to this information.

When the technical constraint is strong and the safety risk is low, the credential information can also be passed to the application as command line arguments. However, we do not recommend using such approach as the user of the application can access the information.

 Note:

The WALLIX support team can provide you with a generic Autolt connection script. You can also contact the support team for any other question.

Procedure

1. Allow Autolt scripts to retrieve credential information through the RDP virtual channel.
 - a. Enable the option from **Configuration > Configuration Options > RDP proxy**.
 - b. Enter the name of this virtual channel in **Auth channel** in the **[mod_rdp]** section.



- The wildcard symbol (*) tells WALLIX Bastion to use the default name being **wablnch**. It is important that both WALLIX Bastion and the Autolt script use the same virtual channel name to operate properly.
- When the virtual channel option is enabled, the Autolt script must be deployed on the server running Terminal Server then added to the listed RemoteApp programs:
 - Click the **Start** menu.
 - Select **All Programs > Administrative Tools > Remote Desktop Services** and then click **RemoteApp Manager**.
 - In the **"Actions"** frame, click **"Add RemoteApp Programs"**.
 - Choose the path of the Autolt executable script in the list displayed by selecting the related check box.
 - When configuring the standard application from the **Applications** page on WALLIX Bastion:
 - Enter the connection URL in **Parameters**.
 - Enter the path of the Autolt executable script in **Application path**.

In the previous example, the script WABIELogon_VC_64.exe launches Internet Explorer, retrieves the credential information from the virtual channel and establishes a connection to the application.

- When the standard application is configured, it can be linked to a target group from **Targets > Groups**.

10.10. Automate connections to a web app using WALLIX Application Driver

WALLIX Application Driver is a tool used for accessing web applications by automatically injecting credentials (username and password) into authentication forms.



Note:

To automate connections to non web-based applications, refer to [Automate connections to an application using Autolt scripts \(on page 125\)](#).

Application Driver retrieves the authentication information from the application through an RDP virtual channel and automatically authenticates the user. That means the authentication forms are filled out without user intervention and sensitive data is not disclosed during the authentication phase.

Application Driver can be used without any specific deployment (refer to [Using WALLIX Application Driver without specific deployment \(on page 130\)](#)) or by manual deployment (refer to [Using WALLIX Application Driver through a manual deployment \(on page 132\)](#)).

**Note:**

WALLIX Bastion and Application Driver must use the same virtual channel name to operate properly.

To configure the virtual channel, it is necessary to enter the name of the RDP virtual channel in the **Auth channel** field located in **Configuration > Configuration options > RDP proxy** under the **[mod_rdp]** section.

By default, the asterisk symbol * is already specified and tells WALLIX Bastion to use the default virtual channel name: **wablnch**.

10.10.1. WALLIX Application Driver parameters for web app launch

Mandatory parameters

Parameter	Description
/lua_file:<Lua script file name>	Applies only when using WALLIX Application Driver with a manual deployment. Sets the Lua script's path used to open the web session.
/e:URL=<URL>	Defines the Website URL.

**Important:**

To access the command line help and the version number of the Lua script used by Application Driver, it is necessary to specify the `/e:ShowUsage=Yes` parameter in the **Parameters** field, such as:

```
/lua_file:<Lua script file name> /e:ShowUsage=Yes
```

Optional parameters for Internet Explorer

Parameter	Description
/e:EnterInPasswordField=Yes	Validates the form by pressing the return key in the password-input field. Is ignored when a two-page login is used. Is not compatible with the option <code>/e:EnterInsteadClicking=Yes</code> .
/e:EnterInsteadClicking=Yes	Validates the form by pressing the return key in the text-input fields instead of clicking the validation button.
/e:FirstPageReadyElementId=<Element ID>	Defines a HTML element id determining that the first web page is fully loaded and ready in the case of a two-page login.



Parameter	Description
/e:PasswordFieldId=<password field ID>	Defines the password field id on the login web page. Is ignored when a two-page login is used.
/e:PreSignInLinkClassName=<link class name>	Defines a HTML anchor link class name determining that the page is fully loaded and ready.
/e:SecondPageReadyElementId=<Element ID>	Defines a HTML element id determining that the second web page is fully loaded and ready in the case of a two-page login.
/e:SendInputInsteadSetValue=Yes	Simulates keystrokes instead of entering a value in the text-input field.
/e:SubmitButtonId=<Button Id>	Defines the validation button id on the login web page. Is ignored when a two-page login is used.
/e:TwoPageSignIn=Yes	Enables a two-page login.
/e:UsernameFieldId=<username field ID>	Defines user name field id on the login web page. Is ignored when a two-page login is used.

Optional parameters for Google Chrome and Microsoft Edge based on Chromium with UI Automation script

Parameter	Description
/e:DisableKioskMode=Yes	Prevents the launch of Google Chrome or Microsoft Edge based on Chromium in Kiosk mode.
/e:DisablePopupBlocking=Yes	Disables the blocking of pop-up windows.
/e:DontUseGuestMode=Yes	Disables the Guest mode.
/e:ExtraDelayBeforeFormSubmission=<milliseconds>	Adds an additional delay (in milliseconds) to the base delay of 1000 ms before form validation.
/e:ExtraDropdown=<option>	Fills out an extra drop-down list in the login web page.
/e:ExtraTextFieldAutomationIdAndValue= <AutomationId>;<value>	Fills out an extra input field in the login web page.



Parameter	Description
/e:HTTPAuthentication=Yes	Enables the connection through the HTTP authentication pop-up.
/e:IgnoreCertificateErrors=Yes	Requests Google Chrome or Microsoft Edge based on Chromium to ignore certificate check errors.
/e:RemoveDomainFromUsername=Yes	Removes @<domain> from the login.
/e:TwoPageSignIn=Yes	Enables two-page login.
/e:UseEdgeChromium=Yes	Applies only when using WALLIX Application Driver with a manual deployment. Uses Microsoft Edge based on Chromium instead of Google Chrome.
/e:UseDefaultUserDataDir=Yes	Lets the website browser use the existing profile of the Windows account.
/e:PreSignInElement2=<PropertyN>;<ValueN>	Lets the UI Automation specify pseudo-conditions for finding the element to be activated in a second pre-sign-in page of website.

Optional parameters for Google Chrome and Microsoft Edge based on Chromium with the DevTools script

Parameter	Description
/e:DisableKioskMode=Yes	Prevents the launch of Google Chrome or Microsoft Edge based on Chromium in Kiosk mode.
/e:DisablePopupBlocking=Yes	Disables the blocking of pop-up windows.
/e:DontUseGuestMode=Yes	Disables the Guest mode.
/e:ExtraFieldSelectorAndValue=<selector>;<value>	Fills out an extra input field in the login web page.
/e:IgnoreCertificateErrors=Yes	Requests Google Chrome or Microsoft Edge based on Chromium to ignore certificate check errors.



Parameter	Description
/e:PasswordFieldSelector=<selector>	Finds the password input field according to the CSS selector specified. Must be used with the UsernameFieldSelector parameter.
/e:PreSignInElementSelector=<selector>	Finds the element to enable in the pre sign-in page of the website according to the CSS selector specified.
/e:RemoveDomainFromUsername=Yes	Removes @<domain> from the login.
/e:SubmitButtonSelector=<selector>	Finds the validation button according to the CSS selector specified. Is not compatible with a two-page login. Must be used with the UsernameFieldSelector and PasswordFieldSelector parameters.
/e:TwoPageSignIn=Yes	Enables two-page login.
/e:UseEdgeChromium=Yes	Applies only when using WALLIX Application Driver with a manual deployment. Uses Microsoft Edge based on Chromium instead of Google Chrome.
/e:UsernameFieldSelector=<selector>	Finds the username input field according to the CSS selector specified. Must be used with the PasswordFieldSelector parameter.
/e:UseDefaultUserDataDir=Yes	Lets the website browser use the existing profile of the Windows account.
/e:PreSignInElement2Selector=<selector>	Lets CSS selectors be specified to find the element to enable in a second pre sign-in page of website.

10.10.2. Using WALLIX Application Driver without specific deployment

Before you begin

The session probe mode must be enabled to use Application Driver without specific deployment.

The prerequisites for the automatic deployment of Application Driver are the same as the prerequisites for running Session Probe. For more information, refer to [Session probe mode \(on page 138\)](#).



Note:

`__APP_DRIVER_IE__` is no longer maintained. We recommend using the markers for Google Chrome or Microsoft Edge based on Chromium.

The UI Automation script cannot be ran on Windows Server 2022 when the RemoteApp mode is enabled. We recommend:

- using the DevTools script or
- unchecking the **Rdp remote app mode** option in **Configuration optionsGUI (Legacy)** under the **main** section

Procedure

1. Go to the **Targets > Applications** page.
2. Create a new application.
3. In **Application path**, enter one of the following values:
 - `__APP_DRIVER_IE__` to select the launch of the web application in Internet Explorer
 - `__APP_DRIVER_CHROME_UIA__` to select the launch of the web application in Google Chrome with the UI Automation script
 - `__APP_DRIVER_EDGE_CHROMIUM_UIA__` to select the launch of the web application in Microsoft Edge based on Chromium with the UI Automation script
 - `__APP_DRIVER_CHROME_DT__` to select the launch of the web application in Google Chrome with the DevTools script
 - `__APP_DRIVER_EDGE_CHROMIUM_DT__` to select the launch of the web application in Microsoft Edge based on Chromium with the DevTools script
4. In the **Parameters** field, specify the necessary parameters to launch the web application according to the selected browser and script.

For more information, refer to [WALLIX Application Driver parameters for web app launch \(on page 127\)](#).

5. Click **Apply**.

Results

Example for the launch of the web application using Internet Explorer:



10.10.3. Using WALLIX Application Driver through a manual deployment

About this task

Application Driver can be deployed manually through an executable file as well as configuration scripts provided to the administrators of the jump servers upon request to the Support Team. Contact the Team for more information.

However, we recommend using WALLIX Application Driver in connection with the session probe mode. For more information, refer to [Using WALLIX Application Driver without specific deployment \(on page 130\)](#). You can, however, deploy Application Driver manually.

Procedure

1. Download the AppDriver .exe file and the scripts WABChromeLogonUIA .lua and WABIELogon .lua provided by the Support Team to the target server used to execute web applications.



Note:

The script WABChromeLogonUIA .lua will be used to select the launch of the web application using Google Chrome and the script WABIELogon .lua will be used to select the launch of the web application using Internet Explorer.

2. Copy the AppDriver .exe file to a dedicated folder. For example: C:\AppDriver\AppDriver.exe.
3. Copy both scripts to this same folder.

What to do next

To launch the web app, the setup must be performed from the **TargetsApplications** page.

1. In the **Parameters** field, specify either the path to the script WABChromeLogonUIA .lua or the path to the script WABIELogon .lua according to the selected browser for the launch of the web application as well as the necessary parameters. For more information, refer to [WALLIX Application Driver parameters for web app launch \(on page 127\)](#).
2. In the **Application path**, enter the path to the AppDriver .exe file.



Important:

AppDriver.exe /? must be entered in the **Application path** field to access the command line help and version number of Application Driver.

10.10.3.1. Block user input during Application Driver execution

About this task

To enhance the security of an application session after a manual deployment, you can prevent user input until Application Driver has completed executing the configuration scripts. During this period, no user input will be processed in the session.



Restriction: This option does not apply to desktop sessions.



Attention: Do not enable this option for application sessions that do not use Application Driver, or the user will not be able to interact with the session.



Procedure

1. In WALLIX Bastion, select **Session Management > Connection policies**.
2. Modify an existing policy or create a new one.
3. Go to the **[rdp]** section.
4. Enable the **Block user input until Application Driver completes** option.
5. Click **Apply**.

Results

Future application sessions using this connection policy will block user input until Application Driver has finished executing the scripts.

10.10.4. Using the browser extension with WALLIX Application Drive

By default, *WALLIX Application Driver* launches the web browser with a blank user profile. As a result, browser extensions installed in Windows are not loaded. This can be an issue for some applications. However, it is possible to authorize the use of Google Chrome extensions by using the following parameters simultaneously:

- `/e:UseDefaultUserDataDir=Yes`: with this parameter, **Application Driver** no longer creates a unique profile for the web browser, but uses a copy of the existing Windows account profile. That means all installed extensions are available. Copying the profile can take some time as it depends on the amount of data contained in the profile. The WALLIX Bastion administrator must ensure that this profile is as small as possible.
- `/e:DontUseGuestMode=Yes`: allows extensions to be loaded when the web browser is launched.



Important:

A user can install software components (plugins/extensions) in the user profile of the web browser. If this existing profile is used as a template when copying, these software components are loaded into the browser of the application session. The browser behavior can be affected by security vulnerabilities introduced by this method. The WALLIX Bastion administrator must be aware of these risks.

It is recommended not to give access to the associated Windows account other than through the website application. It is also recommended to use a password change policy for the associated Windows account.

11. Connection policies

What is a Connection policy?

Connection policies are defined as the authentication mechanisms available in WALLIX Bastion. The mechanisms available for RDP, VNC, SSH, TELNET, RLOGIN, and RAW TCP/IP protocols are predefined in WALLIX Bastion and cannot be deleted or edited.

A connection policy can be selected during the creation or modification of a device and is associated with a specific service on the device. For more information, refer to [Devices \(on page 110\)](#).



Attention:

The **Advanced options** must only be changed when instructed by the WALLIX support team. An icon representing an exclamation mark on an orange background is displayed near the concerned fields.



Note:

The `SSH_SHELL_SESSION`, `SSH_REMOTE_COMMAND`, `SSH_SCP_UP`, `SSH_SCP_DOWN`, and `SFTP_SESSION` options allow the opening of session channels. By default, only one session channel can be open during an SSH connection (or session). To allow the opening of several session channels, the option **Allow multi channels** must be selected at the level of the SSH connection policy (which can be accessed from **Session Management > Connection Policies**).

11.1. Add a connection policy

Procedure

1. Go to the **Session management > Connection policies** page.
2. Click **Add a connection policy**.



Tip:

You can also duplicate an existing policy to use its parameters. In this case, only the "**Policy name**" and "**Description**" are not inherited from the chosen policy and are empty.

3. Give the policy a name and an optional description.
4. Select the relevant protocol from the dropdown list.
5. Select the relevant policy type from the dropdown list.
6. Activate the relevant authentication methods.
7. If you the connection policy type is **TELNET** or **RLOGIN**, a sequence of commands to define an authentication is required in **Scenario**.

A default connection scenario is provided however it can be modified. For more information, refer to [TELNET/RLOGIN connection scenario on a target device \(on page 137\)](#).

8. **Optional:** You can add transformation rules.

- ■ Fill out **Transformation rule** to get a login for secondary connection. For more information, refer to [Get a login for secondary connection \(on page 135\)](#).
 - Fill out **Vault transformation rule** to get the credentials of an account in the vault. For more information, refer to [Retrieve account credentials in WALLIX Bastion vault \(on page 136\)](#).
9. **Optional:** If you the connection policy type is **SSH**, **TELNET**, or **RLOGIN**, you can add a startup scenario to perform specific actions at the beginning of the session.

For more information, refer to [Startup scenario on a target device \(on page 149\)](#).

10. **Optional:** If you the connection policy type is **RDP**, you can activate the session probe feature.

For more information, refer to [Session probe mode \(on page 138\)](#).

11. **Optional:** If you the connection policy type is **VNC**, you can create a SSH tunnel to secure connections to VNC session.

For more information, refer to [Connect to a VNC session over an SSH tunnel \(on page 151\)](#).

11.2. Edit a connection policy

About this task



Attention:

If the target account access is not allowed for a profile, then the profile members cannot delete or edit a connection policy.

The protocol cannot be edited.

Procedure

1. Go to the **Session management > Connection policies** page.
2. Select the connection policy that you want to edit.
3. Click **Edit this connection policy** and edit the necessary information.
4. Click **Apply**.

11.3. Transformation rules

11.3.1. Get a login for secondary connection

A transformation rule based on a character string can be defined to get a login for connection on a target account through a mapping from:

- a user account login if the target account is included in a group configured for account mapping (for more information, refer to [Configure a target group for session management through account mapping \(on page 169\)](#))
- a login of an account in the vault of WALLIX Bastion if the target account is included in a group configured for session management from accounts in the vault (for more information, refer to [Configure a target group for session management from an account in the vault \(on page 168\)](#)).

This rule is set in the **Transformation rule** field on the configuration page for the related connection policy, accessible from **Session Management > Connection Policies**.

The character string includes the required field `${LOGIN}` and possibly the optional field `${DOMAIN}` in an LDAP mapping context.

The transformation rule returns the string and replaces the fields `${LOGIN}` and `${DOMAIN}` with the appropriate values (that is the login and domain).

The result corresponds to the login for connection on the target.



Note:

The transformation rule defined is ignored if the target account is included in a group configured for interactive login (for more information, refer to [Configure a target group for session management through interactive login \(on page 170\)](#)).

Examples

'`${DOMAIN}WIN2K3\${LOGIN}`': addition of a suffix in the domain

'`${LOGIN}`': login forcing without any domain

'`${LOGIN}@DOMAIN1`': use of a different domain

11.3.2. Retrieve account credentials in WALLIX Bastion vault

A character string-based transformation rule can be defined to retrieve the credentials of an existing account in the vault of WALLIX Bastion for a target account configured for account mapping. This transformation rule is used to map a user account to an account located in the vault.

This transformation rule applies only when:

- the target account is in a group configured for account mapping (for more information, refer to [Configure a target group for session management through account mapping \(on page 169\)](#))
- the `PUBKEY_VAULT` and/or `PASSWORD_VAULT` authentication method must be selected in the connection policy associated with the target

This rule is set in the **Vault transformation rule** field on the configuration page of the connection policy, accessible from **Session Management > Connection Policies**.

The character string can include the following fields:

- `${USER}`: this field is substituted by the user login
- `${DOMAIN}`: this field is substituted by the user domain in the context of LDAP mapping
- `${USER_DOMAIN}`: this field is substituted by the user login + @ + user domain. If there is no user domain, then `${USER_DOMAIN}` is only substituted by the user login .
- `${GROUP}`: this field is substituted by the user group concerned by the authorization
- `${DEVICE}`: this field is substituted by the device name

A regular expression (or `regex`) can be specified for the transformation using this syntax: `${USER:/regex/substitution}`. For example, all user logins starting with A are substituted by B if the `${USER}` variable is specified as follows `${USER:/^A/B}`.

The transformation rule returns the string and substitutes the fields with the appropriate values.

The result corresponds to the account in the vault for which the credentials are to be retrieved. This result can be viewed on the **Syslog** page in the **System** menu.



There are two types of accounts in the vault: local domain account and global domain account. Their syntax is defined as follows:

- Local domain account: `<Account_Name>@<Domain_Name>@<Device_Name>`
 - `<Account_Name>`: name of the account in the vault
 - `<Domain_Name>`: name of the local domain in which the vault account is configured
 - `<Device_Name>`: name of the device linked to the vault account
- Global domain account: `<Account_Name>@<Domain_Name>`
 - `<Account_Name>`: name of the account in the vault
 - `<Domain_Name>`: name of the global domain in which the vault account is configured

Example of transformation rules for local domain account

```
${USER:/^bastion_/}_adm@local@${DEVICE}
```

The syntax is a regular expression which can be read as follows:

- `${USER}`: the transformation process applies to the user login
- `/^bastion_`: the check is performed on the login starting with `bastion_`
- `/}`: if the previous condition is fulfilled, then the field concerning the login is removed
- `@local@`: this field indicates the domain type
- `${DEVICE}`: this field is substituted by the device name

If the login of the user is `bastion_user1` and the device of the target in account mapping is `winprod`, the result of the transformation is the vault account: `user1@local@winprod`.

Example of transformation rules for global domain account

```
${USER:/^adm_/adm_domain1_}@domain1
```

The syntax is a regular expression which can be read as follows:

- `${USER}`: the transformation process applies to the user login
- `/^adm_`: the check is performed on the login starting with `adm_`
- `/adm_domain1_`: if the previous condition is fulfilled, then the field concerning the login is substituted by this value
- `@domain1`: this suffix is added after the substituted variable

If the login of the user starts with `adm_` then `adm_` becomes `adm_domain1_` and `@domain1` is added to the end of the login. As a consequence, if a user login is `adm_jdoe`, the result of the transformation is the global domain account `adm_domain1_jdoe@domain1` in the vault.

11.4. TELNET/RLOGIN connection scenario on a target device

An authentication sequence can be declared by specifying the **Scenario** field on the configuration page related to the connection policy for the TELNET or RLOGIN protocol. This page can be accessed from **Session Management > Connection Policies**. For more information, refer to [Connection policies \(on page 134\)](#).

This sequence can be used to interpret commands sent by an interactive shell and to automate logon. This pseudo language includes the following syntax:

- **SEND**: sends a character string
- **EXPECT**: expects to receive a character string in the next 10 seconds. This value must be labelled in the server's language.



- (?i): ignores the case
- \$login: sends a user name
- \$password: sends a password

The following is a sequence (supported on a 3Com Superstack switch accessible via TELNET) explained step-by-step:

Message	Interpreted as
SEND:\r\n	sends a carriage return
EXPECT:(?i)login:	expects to receive the "login" string (ignoring the case)
SEND:\$login\r\n	sends the user name followed by a carriage return
EXPECT:(?i)Password:	expects to receive the "password" string (ignoring the case)
SEND:\$password\r\n	sends the password followed by a carriage return

This sequence also works for TELNET servers running under Windows.

For TELNET servers running under Unix or Linux, use the following sequence:

```
EXPECT:(?i)login:
SEND:$login\n
EXPECT:(?i)Password:
SEND:$password\n
```

For RLOGIN devices, only the password is expected. As an example, the following authentication sequence was tested for a RLOGIN connection to a Debian 5.0 lenny system:

```
EXPECT:(?i)Password:
SEND:$password\n
```



Note:

As a rule of thumb, login is already provided for SSH connections (in keyboard interactive mode) and RLOGIN connections. It is necessary to provide it in the sequence only for TELNET connections.

11.5. Session probe mode

What is the Session probe mode?

The session probe allows the collection of a rich set of session metadata related to the activity of users. This information can be sent to a SIEM software to identify significant events.

The session probe requires no specific deployment. It runs in the user's RDP session according to their privileges. Consequently, it does not increase the attack surface of the information system.



Configuration

This mode can be enabled by selecting the option **Enable session probe** on the configuration page related to the connection policy for the RDP protocol. This page can be accessed from **Session Management > Connection Policies**.

Metadata collected by the session probe refers to the following events:

- change of active window
- operation on a button in a window
- selection of a radio button or a check box in a window
- change of content in a text field on a window
- change of the layout of the keyboard keys
- starting and ending of a process
- exchange of files using the clipboard
- exchange of files using redirected local drives

The session probe can also block the TCP jump connections. A jump connection passes through a WALLIX Bastion target to access another machine on the internal network. The session probe can then detect and stop this type of connection.

The session probe provides protection of the passwords entered in the session by detecting the input cursor into password input fields or a User Account Control (UAC) window. When such an event occurs in the session, the session probe informs WALLIX Bastion so that the latter can pause the collection of keyboard input data.

Default operating mode

The session probe is enabled by default on the configuration page related to the connection policy for the RDP protocol, which can be accessed from **Session Management > Connection Policies**. If startup fails, WALLIX Bastion can be configured to try a new connection without using session probe. This catch-up mechanism ensures the access to a usable RDP session but lengthens the time required to set up the connection. The default operation mode is designed for the parameter setting phase and must not be used for production purpose.

If the session probe stops for any reason, WALLIX Bastion stops the current session.

For a classic RDP session, if the user disconnects without closing a session using the session probe, the session continues to operate through the remote desktop service (for a predetermined period). During this time interval, the user can return to the session exactly where they left it. To ensure security, the session probe implements a mechanism which prevents the user from recovering an incompatible session instead of the current one.

The discrepancies which can prevent a session to be recovered by another one are as follows:

- a difference in primary account
- a difference in the target type ("device" or "application")
- a difference in the target application

If WALLIX Bastion detects that it is not possible to recover the RDP session, the current connection is closed and a new one will take over in a transparent way for the user.

Choice of the launcher

The smart launcher is used by default for a normal RDP session. However, the standard launcher can be used by editing the connection policy, which can be accessed from **Session Management > Connection Policies**.



There is an exception: when the RDP client has specified a program to run at connection startup, then the standard launcher is used for the session probe.

The connection to an application (as defined in **Targets > Applications**) can only be made through the standard launcher. This selection is automatically performed by the RDP proxy.

Prerequisites

The session probe operates under a Windows operating system with the Remote Desktop services supporting the "alternate shell" function.

Environments under Windows XP and servers from Windows Server 2003 support the smart launcher.

When the smart launcher is used:

- the redirection of clipboard must be allowed by Remote Desktop Services (or Terminal Services) on the target. This is the default setting.
- the keyboard shortcut **Windows+R** must be enabled at the level of the group policies for the target (this is the default setting). Keyboard shortcuts can be disabled via **Local Group Policy Editor > User Configuration > Administrative Templates > Windows Components > Windows Explorer or File Explorer > Turn off Windows+X hotkeys or Turn off Windows Key hotkeys**.

The standard launcher only operates on targets under Windows Server and Windows XP environments. It does not support targets under Windows 7, 8.x and 10.

From Windows Server 2008 and only when the standard launcher is used, it is necessary to publish the "Command Prompt" (cmd.exe) as the RemoteApp program. Moreover, all command line parameters must be allowed for this program by selecting the radio button "Allow any command-line parameters" in the "Remote Desktop Connection Program properties" dialog box.

The redirection of local disks must be allowed by Remote Desktop Services (or Terminal Services) on the target. This is the default setting.

The temporary folder of the secondary account (Windows account) must allow at least 5MB free disk space.

The Windows user account must be able to launch batch script and executables from their own temporary directory (this is the default setting). It is possible to set a software restriction via **Local Group Policy Editor > Computer configuration > Windows Settings > Security Settings > Software Restriction Policies** by adding a new rule in **Additional Rules**.

When opening a new RDP session, applications that launch automatically at startup and require a user account control (UAC) confirmation request may block the session probe. We recommend not configuring the automatic launch of applications requiring a UAC confirmation request.

Configuration options

The configuration of the session probe is set on the configuration page related to the connection policy for the RDP protocol, which can be accessed from **Session Management > Connection Policies**. The **session probe** section lists the following parameters:

Enable session probe

Select/deselect the check box to enable/disable the session probe.

Use smart launcher

Select/deselect the check box to enable/disable the use of the Smart Launcher when launching the session probe.

**Attention:**

The smart launcher is only available for standard RDP sessions.

When connecting to an application, only the standard launcher is used. The RDP proxy automatically chooses to launch the standard launcher.

Unlike the standard launcher, the smart launcher does not require the command prompt (cmd.exe) to be published as a RemoteApp program.

The redirection of clipboard must be enabled by Terminal Services to use the smart launcher (this is enabled by default).

Enable launch mask

The session probe is loaded by a batch script. Without WALLIX Bastion, this script will cause the display of a non-user friendly black console window in the RDP session. Moreover, the user may interact with it and disrupt the loading process. Enabling the launch mask can block the display as well as mouse and keyboard inputs during the loading of the session probe loading phase. As a consequence, the console window becomes invisible.

Data displayed in the console window is useful to diagnose any loading problem concerning the session probe. This is the reason why the user has the possibility to disable the launch mask.

**Attention:**

This field is displayed when the check box of the "Advanced options" field at the top right of the page is selected. It must only be changed when instructed by the WALLIX support team.

On launch failure

Select the desired behavior in the event of a failed launch of the session probe.

The option "0: ignore failure and continue" may not operate properly under some versions of Windows.

Launch timeout

This field is used when the behavior selected in the "On launch failure" field corresponds to "1: disconnect user". It allows to specify the waiting time (expressed in milliseconds) before WALLIX Bastion considers the failure of the session probe launch.

**Attention:**

This field is displayed when the check box of the "Advanced options" field at the top right of the page is selected. It must only be changed when instructed by the WALLIX support team.

Launch fallback timeout

This field is used when the behavior selected in the "On launch failure" field corresponds to "0: ignore failure and continue" or "2: reconnect without Session Probe". It allows to specify the waiting time (expressed in milliseconds) before WALLIX Bastion considers the failure of the session probe launch.

**Attention:**

This field is displayed when the check box of the "Advanced options" field at the top right of the page is selected. It must only be changed when instructed by the WALLIX support team.

Start launch timeout timer only after logon

Select the check box to optimize the launching of the session probe.

Only servers from Windows Server 2008 and later are supported.

Keepalive timeout

This field allows to specify the maximum waiting time (expressed in milliseconds) between the issue from WALLIX Bastion of a request from KeepAlive to the session probe and the receipt of the corresponding response.

WALLIX Bastion sends KeepAlive messages to the session probe on a regular basis. Without a response from the session probe and at the expiration of the defined period, WALLIX Bastion considers that the session probe is no longer active and stops the connection.

WALLIX Bastion can also stop the connection when the behavior selected in the "On keepalive timeout" field corresponds to "1: disconnect user".

**Attention:**

This field is displayed when the check box of the "Advanced options" field at the top right of the page is selected. It must only be changed when instructed by the WALLIX support team.

On keepalive timeout

Select the desired behavior when a loss of response to the KeepAlive message is detected.

The option "2: freeze session and wait for next keepalive response" freezes the current session and displays an error message. The session are reactivated upon receipt of the response to the KeepAlive message.

End disconnected session

If this check box is selected then disconnected sessions are automatically closed by the session probe.

**Attention:**

A network failure can cause the disconnection of the current RDP sessions. If this option is enabled, any unsaved data will be lost.

Enable log

If this check box is selected then the log files for the Windows session are stored on the user's temporary directory.

We recommend not keeping this log active for a long period as it can be rather verbose and cause hard disk saturation.

**Attention:**

This field is displayed when the check box of the "Advanced options" field at the top right of the page is selected. It must only be changed when instructed by the WALLIX support team.

Enable bestsafe interaction

Select/deselect the check box to enable/disable the interaction of the session probe with the WALLIX BestSafe agent. For more information, refer to [Session probe mode with the WALLIX BestSafe agent \(on page 266\)](#).

Public session

If this check box is selected then a disconnected session (that is, which was not signed off by the user) can be recovered by another user.

Outbound connection monitoring rules

This field allows to specify the rules for blocking TCP jump connections. These rules are generally formed as follows: `<$prefix:><connection address:port>`. The rules are separated by a comma (",").

The following formats are allowed for the destination port:

- a specific port, for example, "3389"
- any port. In this case: "0" or "*"
- an inclusive port range, for example, "1024-65535". One of the two range values can be omitted. In this case, "1" is the default value for the range beginning and "65535" is the default one for the range end.

An authorization rule is formed with the `$allow` prefix. It allows the connection to remote hosts.

A notification rule is formed with the `$notify` prefix. It allows the connection to remote hosts and the generation of a notification.

A prohibition rule is formed with the `$deny` prefix. It prohibits the connection. The `$deny` prefix can be omitted. A rule formed with the `$deny` prefix has precedence over a rule formed with the `$notification` prefix for the same connection address. For example, both of the following rules prohibit all RDP jump connections: `"$deny:0.0.0.0/0:3389"` and `"0.0.0.0/0:3389"`.

For more information about outbound connection detection, read [About outbound connection monitoring rules \(on page 145\)](#)

Process monitoring rule

This field allows to specify the monitoring rules when processes are launched. These rules are generally formed as follows: `<$prefix:><search pattern>`. The rules are separated by a comma (",").

A notification rule is formed with the `$notify` prefix. It allows to generate a notification. For example, `$notify:notepad.exe`: the opening of the application `notepad.exe` is notified but not forbidden.

A prohibition rule is formed with the `$deny` prefix. In addition to notifications, it allows to stop the process. The `$deny` prefix can be omitted. A rule formed with the `$deny` prefix has precedence over a rule formed with the `$notification` prefix.



For example, with `$deny:notepad.exe`, the opening of the application `notepad.exe` is forbidden and notified. With `notepad.exe,cmd.exe` the opening of the applications `notepad.exe` and `cmd.exe` is forbidden and notified. With `$notify:notepad.exe`, `$deny:notepad.exe`, it is the same result as for `$deny:notepad.exe`

The rules formed with `<$prefix:><@>` apply to all the child processes of the application (as defined in **Targets > Applications**). If this rule is:

- `$deny:@`, then the opening of any child process (whatever the name) is forbidden and notified
- `$notify:@`, then the opening of any child process (whatever the name) is notified but not forbidden

Extra system processes

This field allows to specify the processes which must be ignored at end of application detection. The processes are separated by a comma (",").

Childless window as unidentified input field

If this check box is selected then the data entered (such as passwords) in top-level windows of applications are masked when no graphic component is detected.

These windows are then considered as unidentified input fields.



Attention:

This parameter only works if the value **2: passwords and unidentified texts are masked** was selected in **Keyboard input masking level** below section **session log**, for information display in the session metadata.

Windows of these applications as unidentified input field

If application executable files (for example, "chrome.exe") are specified in this field, the data entered in the windows generated by these applications are masked. These windows are then considered as unidentified input fields. The executable files are separated by a comma (",").



Attention:

This parameter only works if the value **2: passwords and unidentified texts are masked** was selected in **Keyboard input masking level** below section **session log**, for information display in the session metadata.

Disabled feature

This field allows you to enter values to disable certain technologies used by the session probe mode, such as **MS Active Accessibility** and **MS UI Automation**. Disabling these technologies helps to overcome compatibility issues and limit the CPU load generated by the session probe mode.

When these technologies are disabled, passwords entered in the dedicated application fields can be visible in the session logs.

These technologies can only be safely disabled together in an application session running a Java application.



11.5.1. Launch the session probe from a specific directory

About this task

By default, the session probe is automatically executed from the temporary directory of the Windows user account when connecting to the target to perform an RDP session. However, hardware restrictions can sometimes prevent this execution. In this situation, it is possible to define another directory from which the session probe is launched.

Procedure

1. Create a new directory on the target to use as the startup directory by the session probe.

All Windows users must have write permission.
2. Configure an environment variable for all Windows users on the target pointing to this new directory.
The maximum length of the environment variable name is 3 characters.
3. Go to the **Session Management > Connection Policies** page on the web interface.
4. Specify the name of this environment variable in **Alternate directory environment variable** (displayed as an advanced option) under section **session probe** on the configuration page related to the connection policy for the RDP protocol.

Results



Attention:

The session probe executable file remains in the directory. This file is overwritten on the next connection.

11.5.2. About outbound connection monitoring rules

This page gives you some tips when using outbound connection monitoring rules and details the limitations of this feature.

Using domain names instead of IP addresses in rules

When you use a domain name in a rule, the Session probe component resolves it on the target device (using DNS) before adding it to its internal rule list.

If you use a round-robin DNS, only one of the host addresses is monitored.

Avoiding overly generic rules

Using a generic rule such as: `$deny:0.0.0.0/0:*` can:

- block legitimate connections established by certain system components operating in the user space.
- make diagnosing potential issues more difficult.

Outbound connection monitoring rules limitations

Outbound connection monitoring rules have the following limitations:



- The Session probe component monitors TCP connections only.

The Session probe component does not have the privileges to intercept connections when they are created. To work around this limitation, Session probe uses a "polling" detection mechanism. This can result in having short-lived connections escaping monitoring.

This is a minor limitation for Jump connections as they are inherently interactive. But it can lead to a serious security risk if the Outbound connection monitoring feature is used as a firewall. This feature cannot replace a kernel-mode firewall.

The polling interval is set to 500 ms by default. All TCP connections lasting longer than the polling interval can be detected.

- Only connections initiated by user application instances within the current session can be monitored.

On Windows, a network drive mount is often performed by the SYSTEM process, even if the mount request originates from the user session. These connections are excluded from monitoring.

Connections created by elevated processes such as **Administrator** account for example, also escape monitoring.

11.6. Authentication mechanisms for RDP target connections

Authentication mechanisms

WALLIX Bastion offers the possibility to configure the authentication methods for RDP targets. There are two options available:

- **Enable NLA** (enabled by default)
- **Enable Kerberos** (disabled by default until Bastion 12.0.0 and enabled by default starting Bastion 12.0.1)

When restoring the back up of a Bastion anterior to 12.0.1, the configuration of authentication mechanisms is not modified. That means that values set for NLA and Kerberos are restored as defined in that backup file. For example, if **Enable Kerberos** option was disabled, this option remains disabled after the restoration, even if the option is enabled by default starting Bastion 12.0.1.

Table 4. Summary of authentication methods applied depending on the options configuration

Enable Kerberos	Enable NLA	Authentication methods
Enabled	Enabled	NLA Kerberos
Disabled	Enabled	NLA NTLM
Enabled	Disabled	TLS only is attempted as an authentication method.
Disabled	Disabled	TLS only is attempted as an authentication method.



Fallback mechanisms

To ensure that the target cannot negotiate an authentication protocol lower than that specified by the connection policy, fallback mechanisms are disabled by default. However, for greater granularity, you can modify fallback mechanisms for connections to RDP targets.

When configuring a connection policy for the RDP protocol, several options are available:

- **Allow NLA NTLM fallback**
- **Allow TLS only fallback**
- **Allow RDP legacy fallback** (available under advanced options)



Tip:

We strongly encourage you to review your connection policies and make any necessary updates to the fallback mechanism to better suit your needs.

Recommendation for fallback mechanisms

WALLIX follows the Microsoft recommendation to use the domain account for RDP sessions. As a result, WALLIX recommends to use NLA Kerberos authentication when using target account in Active Directory.

When using a local account on a target, Microsoft and WALLIX recommend:

- to use NLA NTLM if NTLM support is enabled and NLA enabled.
- to use TLS only if NTLM support is disabled and NLA disabled.

For earlier targets (windows 2003 and older), the RDP legacy fallback is required.

Table 5. Summary of the recommendations for fallback

Situation	Prerequisites	Authentication mechanisms		Fallback mechanisms		
		Enable NLA	Enable Kerberos	Allow NLA NTLM fallback	Allow TLS only fallback	Allow RDP legacy fallback
NLA Kerberos	Domain account (AD based)	Enabled	Enabled	Disabled	Disabled	Disabled
Recommended by Microsoft & WALLIX	NLA active on the target					
NLA NTLM	NLA active on target Local account on target	Enabled	Disabled (recommendation)	Enabled	Disabled	Disabled
TLS only (No NLA)	NLA disabled on target Local account on target	Disabled (recommendation)	Disabled (recommendation)	Disabled	Enabled	Disabled



Table 5. Summary of the recommendations for fallback (continued)

Situation	Prerequisites	Authentication mechanisms		Fallback mechanisms		
		Enable NLA	Enable Kerberos	Allow NLA NTLM fallback	Allow TLS only fallback	Allow RDP legacy fallback
Old or incompatible targets (<= Windows 2003)	None	Disabled	Disabled	Disabled	Disabled	Enabled

11.7. Force screen resolution on RDP targets

About this task

Bastion administrators can force the screen resolution of RDP targets. This is useful for targets that have display constraints, usually found in Operational Technology (OT) environments. On these targets, unstable resolutions can make a session hard to navigate or even crash.

Forcing a screen resolution ensure stability on these sessions.



Note:

If you activate the **Rdp remote app mode** option in **Configuration > Configuration Options > GUI (Legacy)[main]** section, the **Force screen resolution** option is not applicable.

Procedure

1. Go to **Session management > Connection policies**.
2. Edit an existing policy or create one.
3. Go to the **[rdp]** section.
4. In the **Force screen resolution** field, enter the resolution you want to force on the target in widthxHeight format.
Enter 800x600.
No resolution is forced on the target if you set values to 0x0 or if you leave the field blank.
5. Click **Apply**.

Results

The resolution will be applied the next time the user connects to the target.

What to do next

Make sure the connection policy is associated with the target. For more information, refer to [Manage services for a device \(on page 110\)](#).



Note: For application targets in **Targets > Applications**, it is the connection policy of the target selected in the **Target/Cluster Name** field that applies.



11.8. Startup scenario on a target device

About this task

A startup scenario can be declared in a connection policy for SSH, TELNET, and RLOGIN protocols. For example, the scenario can be used at the beginning of the SSH Shell session to assign the user the root privileges using su and sudo commands without having knowledge of the password.

Procedure

1. Go to **Session Management > Connection Policies**.
2. Click the relevant connection policy to edit the configuration.
3. Find the **startup_scenario** section.
4. Add the **Scenario**.

For more information on how to build the scenario, refer to [Startup scenario options \(on page 149\)](#).

5. Click **Enable** to activate the startup scenario.
6. **Optional:** If you activate **Advanced options** on the connection policy, there are other configuration options available.
 - **Show output:** display or hide inputs/outputs on the Shell during the scenario execution. By default, this option is enabled.
 - **Timeout:** define the time period (expressed in seconds) before the failure of an EXPECT command.
 - **Ask startup:** enable or disable a prompt to ask users if they want to run the scenario. By default, the scenario is necessarily executed.
7. Click **Apply** to save the connection policy modifications.

11.8.1. Startup scenario options

Commands

A scenario is a sequence of commands separated by a carriage return, meaning a line of the scenario corresponds to a command. A command is defined by a type and value pair, separated by a colon ':', such as TYPE:VALUE.

A command starting with a hash-tag (#) is ignored.

This startup scenario consists of a sequence of commands based on response request and data sending. These commands are executed at the beginning of a Shell session related to an SSH target. The syntax includes the following commands:

Commands	Description
SEND	This command sends the value associated with the server and goes ahead with the scenario. The associated value can include a token (refer to Token (on page 150)). The following example sends the interactive sudo command. <pre>SEND:exec sudo -i</pre>



Commands	Description
EXPECT	this command waits for a response from the server in relation to the associated value before continuing the execution of the scenario. The associated value is a regular expression. It can include a token (refer to Token (on page 150)) which is interpreted before the regular expression. This value must be labeled in the server's language. The following example waits for a command prompt. <pre>EXPECT: .*@.*:~\$</pre> If after a given period of time, no response from the server corresponds to the associated value, the scenario fails. A scenario failure ends the session.

During the scenario execution, no action from the user is permitted except the use of **CTRL+C** or **CTRL+D** to stop the process. This causes the scenario failure and ends the session.

The user takes over the terminal when the scenario successfully completed.



Attention:

If no **EXPECT** command is used, the scenario executes the **SEND** command when the connection is established and does not wait for a data output.

If sensitive data is used, it is strongly recommended to use **EXPECT** commands.

Even if the **Show output** box is unchecked, it is necessary to use the **EXPECT** command to avoid displaying data output in the terminal.

Token

The value of a command can include a token. A token is a part of the value which is replaced by an attribute provided by the SSH proxy or WALLIX Bastion.

A token is represented by the following syntax: `${type}` or `${type:param}` and is defined by a type and an optional parameter.

The following token types can be used: `login`, `password`, and `user`.

- `${login}`: login of the current target account
- `${password}`: password of the current target account
- `${user}`: login of the primary account, that is the login of the WALLIX Bastion user

There is no parameter to provide for the `user` token type.

If no parameter is provided for the token types `login` and `password`, then the attribute is the one of the target account in the current session.

If a parameter is provided, it specifies the account in WALLIX Bastion for which the parameters ("login" and "password") are to be retrieved.

- `${login:account@domain}`: login of a global domain account
- `${password:account@domain}`: password of a global domain account



- `${login:account@domain@}`: login of an account on the current local domain for a device
- `${password:account@domain@}`: password of an account on the current local domain for a device

It is also possible to use placeholder attributes in the token parameter to specify a given scenario account. The following placeholder attributes can be used:

- `<user>`: user name
- `<user_group>`: user group name of the current authorization
- `<target_group>`: target group name of the current authorization
- `<authorization>`: name of the current authorization
- `<account>`: account name of the current target
- `<account_domain>`: account's domain name of the current target
- `<device>`: device name of the current target
- `<service>`: device's service name of the current target

As an example, the token `${password:<user>_root@domain}` for the user **wabuser** will be superseded by `${password:wabuser_root@domain}` and then replaced by the password of the scenario account `wabuser_root@domain` (global account).

As an example, the token `${login:<account>_<device>@sqldomain}` for a user connected to the target `admin@local@sqldevice:SSH:adminauth` will be superseded by `${login:admin_sqldevice@sqldomain}` and then replaced by the login of the scenario account `admin_sqldevice@sqldomain` (global account).

The scenario fails if no attribute is retrieved for the token.

The following example shows a script for privilege elevation using the `sudo` command:

```
SEND:exec sudo -i
EXPECT:password.*:
SEND:${password}
```

The following example shows a script for switching user on a "root" account on the same device using the `su` command:

```
SEND:exec su - root
EXPECT:Password:
SEND:${password:root@local@}
```

The following example shows an interactive access to a MySQL database on a global domain in WALLIX Bastion:

```
SEND:exec mysql -u ${login:<account>_<device>@sqldomain} -p mybdd
EXPECT:password:
SEND:${password:login:<account>_<device>@sqldomain}
```

11.9. Connect to a VNC session over an SSH tunnel

About this task

An unencrypted connection to a VNC server can be secured by tunneling the VNC connection over an SSH tunnel. For this to work, it is required to use an SSH server on which a TCP forwarding tunnel is enabled (for example, the **AllowTcpForwarding** option for OpenSSH). It is also recommended that the VNC server is only available in local.

Procedure

1. Go to **Session Management > Connection Policies**.
2. Click the relevant VNC connection policy to edit the configuration.



3. Find the **[vnc_over_ssh]** section.
4. Click **Enable** to activate the VNC connection over an SSH tunnel.
5. In **Ssh port**, set the SSH port number to establish the connection. By default, the port is 22.
6. For **Tunneling credential source**, choose the source of the credentials to establish the SSH tunnel.
 - **static_login**: credentials of the connection policy.
 - **scenario_account**: credentials of the scenario account.
7. Depending on the selected source, provide the corresponding credential information.
 - If you set the source to **static_login**, provide the credentials of the SSH server in **Ssh login** and **Ssh password**.
 - If you set the source to **scenario_account**, provide the name of the scenario account. The recommended syntax is:
 - `account@global_domain` for a scenario account on a global domain
 - `account@local_domain@` for a scenario account on a local domain



Important:

It is recommended to associate the global domain (when not associated with an external vault) or the local domain (domain type **Local for a device**) with an SSH Certificate Authority to use the certificate-based authentication. If the association is not made, the key-based authentication is used. For more information, refer to [Add a global domain with a local vault \(on page 173\)](#)

8. Click **Apply** to save the connection policy modifications.

11.10. Log all keyboard input

About this task

By default, only keyboard input displayed on the terminal is logged. However, the log of all keyboard input, whether displayed or not on the terminal, can be configured for all the connection policies based on RLOGIN, SSH, and TELNET protocols.



Attention:

When the full log option is enabled, the passwords entered during session are logged and then displayed as plain text.

Procedure

1. Go to **Session Management > Connection Policies**.
2. Click the relevant connection policy to edit the configuration.
3. Find the **[trace]** section.
4. Activate the **Log all kbd** option.
5. Click **Apply** to save the connection policy modifications.

Results

The full log can be viewed from the **Audit > Session History** page, in the "Session metadata" area.



11.11. Dynamic virtual channels for RDP protocol

About this task



Attention:

The **Advanced options** must only be changed when instructed by the WALLIX support team. An icon representing an exclamation mark on an orange background is displayed near the concerned fields.



Attention:

Rejecting dynamic virtual channels can disturb RDP connections.

Dynamic virtual channels can be open during connection to the RDP session to transfer any type of data. By default, all dynamic virtual channels are allowed. However, it is possible to configure the dynamic virtual channels which can be allowed or rejected during the RDP session.

Procedure

1. Go to **Session Management > Connection Policies**.
2. Click the relevant RDP connection policy to edit the configuration.
3. Click **Advanced options**.
4. Find the **rdp** section.
5. Provide the list of **Allowed dynamic channels** and **Denied dynamic channels**.



Important:

The configuration in the field **Denied dynamic channels** has precedence over the one set in the field **Allowed dynamic channels**

6. Click **Apply** to save the connection policy modifications.

Results

When attempting to open a dynamic virtual channel, the information related to its authorization or rejection is logged:

- in the session metadata displayed from the **Session History** page on the **Audit** menu, in the **Session metadata** area.
- in SIEM messages, if the routing to a SIEM software is configured on WALLIX Bastion.

11.12. Antivirus software or a DLP solution with ICAP

Connections to ICAP servers provided by antivirus software or Data Loss Prevention (DLP) solutions can be configured to verify the validity of files transferred during RDP and SSH sessions. The files which can be verified are those transferred via subprotocols SFTP and SCP (`SFTP_SESSION`, `SSH_SCP_UP`, and `SSH_SCP_DOWN`) during SSH session and from the copy/paste function via the clipboard (`RDP_CLIPBOARD_FILE`) during RDP session.

File verification does not interfere with file transfer. The status returned by the ICAP server is logged:



- in the session metadata displayed from the **Session History** page on the **Audit** menu, in the **Session metadata** area.
- in SIEM messages, if the routing to a SIEM software is configured on WALLIX Bastion.

11.12.1. Configuration of connection to ICAP servers

About this task

An ICAP server can be configured for each protocol (RDP and SSH) and for each transfer direction:

- for the files transferred as an upload operation from client to server (for example, an antivirus software)
- for the files transferred as a download operation from server to client (for example, a DLP solution)

Procedure

1. Go to the **Configuration > Configuration options** page.
2. Click **SSH proxy** or **RDP proxy** to edit the related proxy parameters.
3. In **[icap_server_up]**, configure the ICAP server for files transferred as an upload operation.
 - **Host**: IP address or FQDN of the ICAP server
 - **Port**: port of the ICAP server
 - **Service name**: service name on the ICAP server
 - **Tls**: option to select if TLS is enabled on the ICAP server
4. In **[icap_server_down]**, configure the ICAP server for files transferred as a download operation.
 - **Host**: IP address or FQDN of the ICAP server
 - **Port**: port of the ICAP server
 - **Service name**: service name on the ICAP server
 - **Tls**: option to select if TLS is enabled on the ICAP server
5. Click **Apply**

11.12.2. Enabling file verification

About this task

File verification can be enabled or disabled for RDP or SSH protocol or both. By default, file verification is disabled.

Procedure

1. Go to the **Session management > Connection policies** page.
2. Click the desired connection policy and click **Edit this connection policy**.
3. In the **[file_verification]** section, enable the options depending on your requirements:
 - **Enable up**: to enable the verification of files transferred as an upload operation by the ICAP server. The latter is configured in section **[icap_server_up]** from the configuration options of the related proxy (accessible from **Configuration > Configuration Options > RDP proxy** or **SSH proxy**).
 - **Enable down**: to enable the verification of files transferred as a download operation by the ICAP server. The latter is configured in section **[icap_server_down]** from the configuration options of the related proxy (accessible from **Configuration > Configuration Options > RDP proxy** or **SSH proxy**).
4. For connection policy is defined on the RDP protocol, you can also enable the following parameters:

- **Clipboard text up**: option to select to enable verification of text transferred as an upload operation from the copy/paste function using the clipboard by the ICAP servers. The **Enable up** option must be selected to allow this verification.
 - **Clipboard text down**: option to select to enable verification of text transferred as a download operation from the copy/paste function using the clipboard by the ICAP servers. The **Enable down** option must be selected to allow this verification.
5. Click **Apply**.

11.12.3. Blocking file transfer on invalid verification

About this task

When file verification is enabled from the connection policy defined on the RDP or SSH protocol (refer to [Enabling file verification \(on page 154\)](#)), the transfer of files detected as invalid during verification can be blocked. This action can be carried out when using file copy/paste function on the RDP protocol or during file transfer via SCP or SFTP on the SSH protocol (using FileZilla, OpenSSH, or WinSCP clients).

Procedure

1. Go to the **Session management > Connection policies** page.
2. Click the desired connection policy and click **Edit this connection policy**.
3. In the **[file_verification]** section, enable the options depending on your requirements:
 - **Block invalid file up**: blocks file transfer for an upload operation when files are detected as invalid during verification.
 - **Block invalid file down**: blocks file transfer for a download operation when files are detected as invalid during verification.
4. Click **Apply**.

11.12.4. Enabling file storage on invalid verification

About this task

When file verification is enabled from the connection policy defined on the RDP or the SSH protocol (refer to [Enabling file verification \(on page 154\)](#)), the invalid transferred files can be stored.



Note:

Session recording must be enabled for the authorization defined (refer to [Authorizations \(on page 189\)](#)) to allow the auditor to view and download the transferred files from the "Session History" page on the "Audit" menu.

Procedure

1. Go to the **Session management > Connection policies** page.
2. Click the desired connection policy and click **Edit this connection policy**.
3. In the **[file_storage]** section, for **Store file**, choose the **on_invalid_verification** option.
4. Click **Apply**.

Results

The invalid transferred files can be viewed and downloaded from the "Session History" page on the "Audit" menu, in the "Transferred files" area.



11.13. Configuration of cryptographic algorithms supported on target devices

The cryptographic algorithms supported on target devices can be configured in the pages related to the connection policies for the RDP or SSH protocols as detailed in the following sections.

11.13.1. SSH cryptographic settings on target devices

About this task

The cryptographic algorithms allowed on target devices can be modified. When no algorithm is entered, all algorithms supported by the SSH proxy are allowed on the target devices. By default, no algorithm is listed in the fields to ensure highest compatibility with target servers.



Attention:

The **Advanced options** must only be changed when instructed by the WALLIX support team. An icon representing an exclamation mark on an orange background is displayed near the concerned fields.

Procedure

1. Go to **Session Management > Connection Policies**.
2. Click the relevant SSH connection policy to edit the configuration.
3. Click **Advanced options**.
4. Find the **algorithms** section.
5. Modify the algorithms according to your requirements.
6. Click **Apply** to save the connection policy modifications.

11.13.2. RDP cryptographic settings on target devices

About this task

The cryptographic algorithms allowed on target devices can be modified. By default, no algorithm is listed in the fields to ensure highest compatibility with target servers.

Procedure

1. Go to **Session Management > Connection Policies**.
2. Click the relevant RDP connection policy to edit the configuration.
3. Find the **rdp** section.
4. Modify the algorithms according to your requirements.
 - **Tls min level**: minimum TLS version level supported. By default, no minimum level is set in this field to ensure highest compatibility with target servers.
 - **Tls max level**: maximum TLS version level supported. By default, no maximum level is set in this field to ensure highest compatibility with target servers.
 - **Cipher string**: additional cryptographic algorithms used for TLSv1.2 connections supported by client. By default, no value is specified in this field to apply system-wide configuration corresponding to SSL security level 2. The value **ALL** must be set to support all cryptographic algorithms and ensure highest compatibility with target servers.
 - **Show common cipher list**: option to select to show in log files the list of common algorithms supported by client and server. This option requires to display **Advanced options**.
5. Click **Apply** to save the connection policy modifications.

11.14. Delete a connection policy

About this task



Attention:

You cannot delete a connection policy when it is linked to a device (at the level of the service on the "Devices" page). For more information on how to link a connection policy on a device, refer to [Create a new device \(on page 110\)](#).

If the target account access is not allowed for a profile, then the profile members cannot delete or edit a connection policy.

Procedure

1. Go to the **Session management > Connection policies** page.
2. Select the connection policies that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected connection policies.



12. Targets



Important:

All the IP addresses which can be set on WALLIX Bastion support both IPv4 and IPv6 formats.

Concept overview

The **Targets** menu allows you to create and manage multiple elements of WALLIX Bastion.

Accounts

Target accounts are entities that allow a user to be authenticated to a system and to be granted a defined level of authorization to access resources on that system.

Applications

Application sessions are managed through a standard jump server (based on Windows), on which applications are installed.

Checkout policies

A checkout policy defines the settings concerning the account checkout process.

Clusters

Clusters are groups of jump servers.

Devices

Devices are physical or virtual equipments for which WALLIX Bastion manages the access to sessions or passwords.

Discovery

Discovery is a module which allows the automatic discovery of assets (devices and accounts) on configured networks and Active Directories and provides the ability to onboard the discovered assets.

Domains

A global domain is a management entity grouping multiple target accounts which can be used to authenticate across multiple devices.

A local domain is a management entity grouping multiple target accounts which can be used to authenticate on a single device only.

Password vault

Structure that manages accounts. It allows configuration through policies and it enforces account usage according to these policies.

Groups

Target groups are entities that simplify management of multiple target accounts.

12.1. Target accounts

What are target accounts?

A target account is an entity managed by WALLIX Bastion or by an external password vault that allows a user to be authenticated to a system and to be granted a defined level of authorization



to access resources on that system, for management purposes. An account always belongs to a domain. For more information, refer to [Domains \(on page 173\)](#).

A target account is characterized by the association of the following entities: a device, a service, and an account.

There are three target account types available:

Global account

The account is defined on a global domain and is used to access services on devices in this domain and to manage service accounts.

For more information on the management of service accounts, refer to [Define references for service account management \(on page 162\)](#)

Device account

The account is defined on a device and is only used for accessing a service on this device.

Application account

The account is defined for an application only. In this case, an account to access the jump server (the target device on which the application is running) might be necessary.

12.1.1. Add a target account to a global domain

Procedure

1. Go to **Targets > Accounts > Global accounts**.
2. Click  **Add**.
3. Select the global domain to which you want to add an account.

It is not possible to modify this information after saving the configuration.

4. Provide an **Account name**.

The name is displayed on the session selector and on the account's credential checkout page on the web interface. This name must be unique in the WALLIX Bastion domain.



Important:

When the account is created on a global domain associated with an external password vault linked to the [Bastion plugin \(on page 236\)](#), the name must follow any of the following formats:

```
account_name\\global_domain
account_name\\local_domain\\device
account_name\\local_domain\\application
```

The `account_name` corresponds to the name of an account on the remote WALLIX Bastion. The `global_domain` and `local_domain` correspond respectively to a global and a local domain on the remote WALLIX Bastion. The `device` and `application` correspond respectively to a device and an application on the local domain on the remote WALLIX Bastion.

5. **Optional:** If necessary, modify the prefilled **Account login**.

This is the user name of the remote account. This information is not displayed on the session selector or on the account's credential checkout page on the web interface.



6. Add a **Resource association**.

A resource association is required to create targets for applications and clusters. To associate resources, select a device and a service in the drop-down lists and click **+**. When created, it is possible to delete this association by clicking the - red icon. You can associate as many resources as necessary.

7. **Optional:** Provide a description of the global account.
8. **Optional:** Select a checkout policy to associate with the account.

For more information, refer to [Checkout policies \(on page 183\)](#).

9. **Optional:** Set additional configuration options.
 - Enable or disable the automatic password change for this account.
 - Enable or disable the automatic SSH key change for this account.
 - Set the certificate validity period if the account is defined on a domain associated with a Certificate Authority. If no value is entered in this field, the certificate is valid for an unlimited period.
10. Click **Apply**.

12.1.2. Add a target account to a device

Procedure

1. Go to **Targets > Accounts > Device accounts**.
2. Click  **Add**.
3. Select the device to which you want to add an account.

It is not possible to modify this information after saving the configuration.

4. Select or create a **Local domain**.

It is not possible to modify this information after saving the configuration.

5. Provide an **Account name**.

The name is displayed on the session selector and on the account's credential checkout page on the web interface. This name must be unique in the WALLIX Bastion domain.

6. **Optional:** If necessary, modify the prefilled **Account login**.

This is the user name of the remote account. This information is not displayed on the session selector or on the account's credential checkout page on the web interface.

7. **Optional:** Provide a description of the account.
8. **Optional:** Select a checkout policy to associate with the account.

For more information, refer to [Checkout policies \(on page 183\)](#).

9. **Optional:** Set additional configuration options.
 - Enable or disable the automatic password change for this account.
 - Enable or disable the automatic SSH key change for this account.
10. Click **Apply**.

12.1.3. Add a target account to an application

Procedure

1. Go to **Targets > Accounts > Application accounts**.
2. Click  **Add**.
3. Select the application to which you want to add an account.



It is not possible to modify this information after saving the configuration.

4. Select or create a **Local domain**.

It is not possible to modify this information after saving the configuration.

5. Provide an **Account name**.

The name is displayed on the session selector and on the account's credential checkout page on the web interface. This name must be unique in the WALLIX Bastion domain.

6. **Optional:** If necessary, modify the prefilled **Account login**.

This is the user name of the remote account. This information is not displayed on the session selector or on the account's credential checkout page on the web interface.

7. **Optional:** Provide a description of the account.
8. **Optional:** Select a checkout policy to associate with the account.

For more information, refer to [Checkout policies \(on page 183\)](#).

9. **Optional:** Enable or disable the automatic password change for this account.
10. Click **Apply**.

12.1.4. Define SSH private key for global or device account

You can define the private key for the SSH connection by generating or upload a key.

12.1.4.1. SSH private key generation

Procedure

1. Go to **Targets > Accounts** and select **Global accounts** or **Device accounts** depending on the target account type.
2. Click the name of the target account that you want to edit.
3. Switch to the **SSH private key > Private key generation** tab.
4. Choose the appropriate private key signature system in the list entitled **Private key signature system**.
5. Click **Apply**.

Results

You have the possibility to download the corresponding SSH public key in the OpenSSH or ssh.com format from the **Download SSH public key** button.

You can delete the SSH private key defined for this account by clicking **Delete existing SSH private key**.

12.1.4.2. SSH private key upload

Procedure

1. Go to **Targets > Accounts > Global accounts**.
2. Click the name of the target account that you want to edit.
3. Switch to the **SSH private key > Private key uploading** tab.
4. Drop or upload a file from your computer containing an existing private key (in the OpenSSH or PuTTY key format) in the **Upload SSH private key** section.
5. If there is a passphrase associated to the private key, enter the information in **Passphrase**.
6. Activate **Propagate credential change** to change the SSH private key of the account and instantly propagate it on the target.
7. Click **Apply**.



Results

You have the possibility to download the corresponding SSH public key in the OpenSSH or ssh.com format from the **Download SSH public key** button.

You can delete the SSH private key defined for this account by clicking **Delete existing SSH private key**.

12.1.5. Define references for service account management

About this task

When changing the secret of a service account, the secret used by a service must be updated with the new secret.

Defining references is a way to simplify the process of secret rotation on services. These references are used by WALLIX Bastion to automatically propagate the new secrets to the devices on which the service is deployed.

Procedure

1. Go to **Targets > Accounts** and select the account type.
2. Click the name of the target account that you want to edit.
3. Switch to the **References** tab and click  **Add**.
4. From the **New reference** window, provide the necessary information.
 - the name of the reference
 - a description
 - the global domain on which the WindowsService plugin is selected (for more information, refer to [WindowsService plugin \(on page 231\)](#))
 - one or more devices on which the service is deployed
 - the global domain on which the administrator account is defined
 - the name of the administrator account
5. Click **Apply and close**.

Results

By clicking the link in the **Device status** column, information on the password change status of the service accounts can be viewed.

12.1.6. Associate global domain accounts to a group

About this task

After you create a global domain account, you can add that account to a target group. Setting up target groups simplifies session management or password management.



Tip:

The association can also be managed directly from the group (for more information, refer to [Target groups \(on page 167\)](#)).

Procedure

1. Go to **Targets > Accounts > Global accounts**.
2. Select one or more accounts.
3. Click  **Add to group**.

This opens a pop-up modal to configure information.

4. In **Group**, select an existing group or create a new group by entering a name.
5. **Optional:** Provide a description.
6. In **Target type**, select the relevant target type to create the association.
 - **Account for session management**
 - **Scenario account for session management**
 - **Account for password management**
7. If you selected **Account for session management**, select the desired resource type for the resource association in the **From** drop-down list.
 - **A device and global accounts**
 - **An application and global accounts**
8. If you selected **Account for session management**, select the required device or application.
9. Select the **Service** if required.
10. Select one or more global accounts.
11. Click **Add and continue** to save and associate the account with another group, or **Add and close** to save and close the window.

12.1.7. Associate device or application accounts to a group

About this task

After you create an application account or a device account, you can add that account to a target group. Setting up target groups simplifies session management or password management.



Tip:

The association can also be managed directly from the group (for more information, refer to [Target groups \(on page 167\)](#)).

Procedure

1. Go to **Targets > Accounts** and select **Device accounts** or **Application accounts** depending on the target account type.
2. Select one or more accounts.
3. Click  **Add to group**.

This opens a pop-up modal to configure information.

4. In **Group**, select an existing group or create a new group by entering a name.
5. In **Target type**, select the relevant target type to create the association.
 - **Account for session management**
 - **Scenario account for session management**
 - **Account for password management**
6. In **Local account**, select all the relevant accounts.

The account is displayed in the list as many times as there are services defined on the device to which it belongs. Make sure to select only the relevant accounts for the association to the group.
7. Click **Add and continue** to save and associate the account with another group, or **Add and close** to save and close the window.



12.1.8. Import target accounts

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the #wab1040 account tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(equired) O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_'
Login	Text	R	Free text
Description	Text	O	Free text
Password	Text	O	Free text Authentication can be performed either by password or by a private key or both or none of them. When the import is performed from WALLIX Bastion 6.1: • if this field is empty, then the password is deleted during import • if this field is filled with the [hidden] keyword, then the existing password is not modified. Caution: If there is no existing password for the account, then this field is set at [hidden]. • if this field is filled with a value other than the [hidden]keyword, then the password is updated with this new value Caution: When the import is performed from a WALLIX Bastion whose version is earlier than 6.1 and if this field is empty, then the password is NOT deleted during import.



Field	Type	R(equired) O(ptional)	Possible values
Private key	Text	O	Free text Authentication can be performed either by password or by a private key or both or none of them. When the import is performed from WALLIX Bastion 6.1: • if this field is empty, then the private key is deleted during import • if this field is filled with the [hidden] value, then the existing key is not modified. Caution: If there is no existing key for the account, then this field is set at [hidden]. • if this field is filled with a value other than the [hidden] keyword, then the key is updated with this new value Caution: When the import is performed from a WALLIX Bastion whose version is earlier than 6.1 and if this field is empty, then the key is NOT deleted during import. As the private key is a long length value, it must be entered between quotes for the import.
Passphrase	Text	O	Free text Passphrase for the private key. This field is used when a new private key is specified in the "Private key" field.
Automatically change password	Boolean	R	True or False Default value: False
Automatically change SSH key	Boolean	R	True or False Default value: False
Checkout policy	Text	R	Checkout policy defined



Field	Type	R(quired) O(ptional)	Possible values
Domain	Text	R	For an account on a device:
Device			• domain: local domain of the device • device: name of the device
Application			• resources: related services (optional and must exist on the device)
Resources/Services			For an account on an application:
			• domain: local domain of the application • application: name of the application
			For an account on a global domain:
			• domain: name of the global domain • resources: device on the domain, expressed with the syntax device:protocol(optional)

Example of import syntax for a device, domain, and application:

```
#wab1040 account
my_device_user;device_user_login;description;False;P4sSw0rD;;False;default;
local_domain_1;my_device;;my_domain_user;domain_user_login;description;True;
P4sSw0rD;;False;default;my_global_domain;;device_on_domain:rdpmy_app_user;
app_user_login;description;False;P4sSw0rD;;True;default;local_domain_1;;my_application;
```

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Accounts** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.



12.1.9. Edit a target account

About this task



Attention:

You cannot edit the login, password, SSH private key and checkout policy of a target account on the web interface or via the REST API when the related credentials are being checked out. The credentials must first be checked in using the **Force check-in option** to edit the corresponding fields.

When the global domain account is defined on a domain associated with a Certificate Authority, you can edit the certificate validity period or add it if it was not previously defined. The appropriate format is as follows: [number of weeks]wk[number of days]d[number of hours]h[number of minutes]min[number of seconds]s. However, if this value is edited or defined at this point, the former validity period still applies. The new validity period for the certificate applies at next SSH key change.

Procedure

1. Go to **Targets > Accounts** and select the type of account that you want to edit (**Global accounts**, **Device accounts**, or **Application accounts**).
2. Click the name of the target account that you want to edit.
3. Edit the necessary information.

12.1.10. Delete a target account

About this task



Attention:

If you delete a global account, the associated references are also deleted.

Procedure

1. Go to **Targets > Accounts** and select the type of account that you want to delete (**Global accounts**, **Device accounts**, or **Application accounts**).
2. Select the accounts that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected target accounts.

12.2. Target groups

The **Groups** page on the **Targets** menu allows you to:

- list the declared target groups
- add, import, edit, and delete a group
- view the target accounts included in each group
- configure a group for session management and password management

12.2.1. Create a target group

Procedure

1. Go to the **Targets > Groups** page.
2. Click **Add**.

3. Give the new group a name and provide an optional description to simplify management.
4. Click **Apply** to create the new target group and proceed with further configuration.

12.2.1.1. Configure a target group for a scenario account during SSH session

About this task

This procedure consists in defining, in a group, the target accounts which can be used by a startup scenario when the SSH session is initiated. These accounts are called *scenario accounts*. For more information, refer to [Startup scenario on a target device \(on page 149\)](#).



Note:

At least one local account must exist on the device or one global account must exist on the global domain to manage associations.



Important:

In SSH sessions, you cannot use scenario accounts with authorizations that include an approval workflow. To manage scenario accounts, assign them to a dedicated target group and create a separate authorization for target group without an approval workflow.

Procedure

1. From the **Session management targets** tab, select **Scenario account** from the drop-down list then click **+ Add** to display the resource association creation page.
2. In the **From** field, select the relevant option from the drop-down list:
 - **A device and related local accounts**
 - **A global domain and related accounts**
3. Depending on the previously selected option, select the relevant **Device** or **Global domain** from the drop-down list.
4. Select one or more target accounts.
5. Click **Add and close** to apply the configuration and close the window, or click **Add and continue** to apply the configuration and create another one.

What to do next

You can delete an association by selecting one or more accounts and clicking **Delete association(s)**. You must confirm the permanent deletion of the selected associations.

12.2.1.2. Configure a target group for session management from an account in the vault

About this task

This procedure consists in defining, in a group, the target accounts which can be accessed remotely from an RDP or an SSH client.



Note:

At least one local or global account must exist for the device and the application to manage this association.

At least one service must exist on the device to manage this association.

Procedure

1. From the **Session management targets** tab, select **Account** from the drop-down list then click **+ Add** to display the resource association creation page.
2. In the **From** field, select the relevant option from the drop-down list:
 - **A device and related local accounts**
 - **A device and global accounts**
 - **An application and related local accounts**
 - **An application and global accounts**
3. Depending on the previously selected option, select the relevant **Device** or **Application** from the drop-down list.
4. If necessary, in the **Service** field, select the service which will be used to access the target accounts.
5. Select one or more target accounts.
6. Click **Add and close** to apply the configuration and close the window, or click **Add and continue** to apply the configuration and create another one.

What to do next

You can delete an association by selecting one or more accounts and clicking **Delete association(s)**. You must confirm the permanent deletion of the selected associations.

12.2.1.3. Configure a target group for session management through account mapping

About this task

The following procedure consists in defining, in a group, the targets which can be accessed through account mapping. An access through account mapping can be defined on a resource (device+service or application) when a service is saved on this resource.



Attention:

The **PASSWORD_MAPPING** authentication method must be selected in the connection policy associated with the target to be able to connect to this target using the account mapping mechanism (for more information, refer to [Connection policies \(on page 134\)](#)).

Account mapping with the authentication method **PASSWORD_MAPPING** is not functional if the user authenticates via a method with no password exchange such as:

- Kerberos or X.509 certificate for WALLIX Bastion
- SAML or X.509 certificate for WALLIX Access Manager

Procedure

1. From the **Session management targets** tab, select **Account mapping** from the drop-down list then click **+ Add** to display the resource association creation page.
2. In the **From** field, select the relevant option from the drop-down list:
 - **A device and related services**
 - **Applications**
3. Depending on the previously selected option, select the relevant **Device** from the drop-down list when applicable.
4. Select one or more service or application.
5. Click **Add and close** to apply the configuration and close the window, or click **Add and continue** to apply the configuration and create another one.



What to do next

You can delete an association by selecting one or more accounts and clicking **Delete association(s)**. You must confirm the permanent deletion of the selected associations.

12.2.1.4. Configure a target group for session management through interactive login

About this task

This procedure consists in defining, in a group, the targets which can be accessed through interactive login. An access through interactive login can be defined on a resource (device+service or application) when a service is saved on this resource.



Note:

The **PASSWORD_INTERACTIVE** authentication method must be selected at the connection policy associated with the target level to be able to connect to this target using the interactive login mechanism (for more information, refer to [Connection policies \(on page 134\)](#)).

Procedure

1. From the **Session management targets** tab, select **Interactive login** from the drop-down list then click **+ Add** to display the resource association creation page.
2. In the **From** field, select the relevant option from the drop-down list:
 - **A device and related services**
 - **Applications**
3. Depending on the previously selected option, select the relevant **Device** from the drop-down list when applicable.
4. Select one or more service or application.
5. Click **Add and close** to apply the configuration and close the window, or click **Add and continue** to apply the configuration and create another one.

What to do next

You can delete an association by selecting one or more accounts and clicking **Delete association(s)**. You must confirm the permanent deletion of the selected associations.

12.2.1.5. Configure a target group for password management from an account in the vault

About this task

This procedure consists in defining, in a group, the target accounts for which the password can be checked out or viewed.

Procedure

1. From the **Password management targets** tab, click **+ Add** to display the resource association creation page.
2. In the **From** field, select the relevant option from the drop-down list:
 - **A device and related local accounts**
 - **A global domain and related accounts**
 - **An application and related local accounts**
3. Depending on the previously selected option, select the relevant **Device**, **Global domain**, or **Application** from the drop-down list.



4. Select one or more service or application.
5. Click **Add and close** to apply the configuration and close the window, or click **Add and continue** to apply the configuration and create another one.

What to do next

You can delete an association by selecting one or more accounts and clicking **Delete association(s)**. You must confirm the permanent deletion of the selected associations.

12.2.2. Import target groups

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the `#wab1040 targetsgroup` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(equired) O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_' There can only be a single group name.
Description	Text	O	Free text
Target accounts	Text	O	Selected target accounts for session management. There can be 0 target account, one or several target accounts defined in each category, or one or several target accounts defined in all categories at the same time. A target account can be defined on a global domain (and not on a local domain) Format for target accounts: <code>account@domain@device:protocol</code>
Account mapping	Text	O	Selected account mapping targets Format for account mapping targets: <code>device:protocol</code>



Field	Type	R(equired) O(ptional)	Possible values
Interactive login	Text	O	Selected interactive login targets Format for interactive login targets: device:protocol
Accounts	Text	O	Selected target accounts for password management Format for target accounts: account@domain Or account@domain@device Or account@domain@application
Scenario	Text	O	Selected scenario accounts Format for scenario accounts: account@domain or account@domain@device

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Target groups** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

12.2.3. Edit a target group

Procedure

1. Go to the **Targets > Groups** page.
2. Click the name of the group that you want to edit.
3. Edit the necessary information.

12.2.4. Delete a target group

About this task



Attention:

You cannot delete a target group linked to active authorizations (refer to [Sessions configuration \(on page 248\)](#)).

Procedure

1. Go to the **Targets > Groups** page.
2. Select the target groups that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected target groups.

12.3. Domains

What are Domains?

There are two types of domains: global and local.

Global domain

A global domain is a management entity grouping multiple target accounts which can be used to authenticate across multiple devices. This entity offers the significant advantage of expanding and synchronizing the password change at the same time for all the accounts on the devices associated with the domain.

A global domain can also be associated with a password external vault. In this case, this domain groups accounts which are managed externally through the association of an external vault plugin. As a result, a password change mechanism cannot be applied to the related accounts in WALLIX Bastion.

Local domain

A local domain is a management entity grouping multiple target accounts which can be used to authenticate on a single device only. This entity offers the significant advantage of expanding and synchronizing the password change at the same time for all the accounts associated with the domain.



Note:

Local domains are created through the association with a device or a target account. For more information, refer to [Devices \(on page 110\)](#) and [Target accounts \(on page 158\)](#).

12.3.1. Add a global domain with a local vault

About this task



Note:

The CA public key is transferred to the target device (for a local domain) or the target server (for a global domain) when a password change plugin is set on the concerned domain and the WALLIX Password Manager feature is associated with the license key.

Procedure

1. Go to **Targets > Domains**.
2. Click **Add a global domain**.
3. Give the domain a name in WALLIX Bastion.

The name is used to display accounts and targets on the web user interface or during RDP/SSH sessions

4. Provide the domain real name.



This is the name of the external domain if the created domain is a mapping of an external domain (LDAP, AD, NIS). The domain real name is ignored when password change is performed on Unix-derived targets.

5. **Optional:** Provide a description of this global domain.
6. For the **Vault type**, select **Local**.
7. **Optional:** Define an SSH Certificate Authority (CA) to be associated with the domain for the connection. The CA is represented by a private/public SSH key pair. There are two possibilities:
 - Generate a key: select the appropriate key type and length from the list (RSA 2048 by default).
 - Upload the file containing an existing key (in the OpenSSH or PuTTY key formats) and specify the corresponding passphrase (if any).

For more information, refer to [Associate the domain with an SSH Certificate Authority \(on page 182\)](#).

8. **Optional:** If the chosen password change plugin is WindowsService and the transport protocol defined for this plugin is Kerberos, fill out the Kerberos parameters information.
 - **Kerberos realm:** specify the Kerberos realm
 - **Kerberos KDC:** specify the domain name or the IP address of the KDC server
 - **Kerberos port:** specify the port number of the KDC server. The default port is 88.
9. **Optional:** Activate the password change for the accounts on this domain.

When the option is activated, you must configure the following parameters:

- a. Select the password change policy for this domain. For more information, refer to [Password change policies \(on page 209\)](#).
- b. Select the password change plugin for this domain and fill out the required configuration parameters. For more information, refer to [Password change plugins \(on page 213\)](#).

10. Click **Apply**.

12.3.2. Add a global domain with an external vault

About this task



Attention:

The External Vaults feature must be associated with the license key.

Procedure

1. Go to **Targets > Domains**.
2. Click **Add a global domain**.
3. Give the domain a name in WALLIX Bastion.

The name is used to display accounts and targets on the web user interface or during RDP/SSH sessions

4. Provide the domain real name.

This is the name of the external domain if the created domain is a mapping of an external domain (LDAP, AD, NIS). The domain real name is ignored when password change is performed on Unix-derived targets.

5. **Optional:** Provide a description of this global domain.
6. For the **Vault type**, select **External**.
7. **Optional:** If the chosen password change plugin is WindowsService and the transport protocol defined for this plugin is Kerberos, fill out the Kerberos parameters information.



- **Kerberos realm**: specify the Kerberos realm
 - **Kerberos KDC**: specify the domain name or the IP address of the KDC server
 - **Kerberos port**: specify the port number of the KDC server. The default port is 88.
8. Select the desired plugin from the drop-down list and fill out the required configuration parameters.

For more information on each plugin configuration requirements, refer to [External password vault plugins \(on page 235\)](#).

9. Click **Apply**.

12.3.3. Import global domains

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the `#wab1040 globaldomain` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(quired)/ O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_'
Real name	Text	O	Free text
Description	Text	O	Free text
Admin account	Text	O	An existing account on the domain This field is only taken into account when the domain exists and the account was created on this domain. Empty if an external vault plugin is defined for the domain
Kerberos realm	Text	O	Free text
Kerberos KDC	Text	O	IP address or host name of the KDC
Kerberos port	Integer number	O	Integer number between 1 and 65535 Default value: 88



Field	Type	R(quired)/ O(ptional)	Possible values
Password change policy	Text	R/O Required when the password change is enabled (one of the 4 last fields is entered)	Password change policy defined Empty if an external vault plugin is defined for the domain
Password change plugin	Text	R/O Required when the password change is enabled (one of the 4 last fields is entered)	Password change plugin defined Empty if an external vault plugin is defined for the domain
Password change infos	Text	R/O Required for given plugin types	All the needed arguments for the password change plugin defined Required for given plugins Format: key1=value1 key2=value2 Cisco: host (required), enable_password (required), port (optional) Windows: domain_controller_address (required) Unix: host (required), port (optional), root_password (optional - root password can only be defined if an admin_account was previously selected) Oracle: host (required), port (optional), service_name (required), admin_mode (optional and set as "Normal" by default if not entered). The possible values for the admin_mode field are as follows: "Normal", "SYSDBA", "SYSOPER" and "SYSASM" Empty if an external vault plugin is defined for the domain



Field	Type	R(equired)/ O(ptional)	Possible values
External vault plugin	Text	O	External vault plugin defined Empty if the password change is enabled for the domain
External vault infos	Text	Required when the external vault plugin is defined	All the needed arguments for the external vault plugin defined Format: key1=value1 key2=value2 Bastion: api_url (required), api_key (optional), service_login (optional), service_password (optional) The API URL must start with https:// and end with /api/vX.Y. The minimum API version supported is 2.3. Empty if the password change is enabled for the domain

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Global domains** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

12.3.4. Import local domains

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the #wab1040 localdomain tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:



Field	Type	R(quired) O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_'
Description	Text	O	Free text
Device	Text	R/O	At least one device or an application must be defined
Application	Text	R/O	At least one device or an application must be defined
Admin account	Text	O	An existing account on the domain This field is only taken into account when the domain exists and the account was created on this domain.
Password change policy	Text	R/O Required when the password change is enabled (one of the 4 last fields is entered)	Password change policy defined
Password change plugin	Text	R/O Required when the password change is enabled (one of the 4 last fields is entered)	Password change plugin defined



Field	Type	R(equired) O(ptional)	Possible values
Password change infos	Text	R/O Required for given plugin types	All the needed arguments for the password change plugin defined Required for given plugins Format: key1=value1 key2=value2 Cisco: port (optional), enable_password (required) Windows: no specific parameter to set Unix: port (optional), root_password (optional) For devices: Oracle: port (optional), service_name (required), admin_mode (optional and set as "Normal" by default if not entered). The possible values for the admin_mode field are as follows: "Normal", "SYSDBA", "SYSOPER" and "SYSASM" For applications: Oracle: host (required), port (optional), service_name (required), admin_mode (optional and set as "Normal" by default if not entered). The possible values for the admin_mode field are as follows: "Normal", "SYSDBA", "SYSOPER" and "SYSASM"

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Local domains** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

12.3.5. Add an account to the global or a local domain

Procedure

1. Go to the **Targets > Domains** page.
2. Select the type of domain that contains the domain you want to edit from **Display domain type: Global, Local for a device, or Local for an application**.
3. Click the name of the domain to which you want to add domain accounts.



4. **Optional:** Click **Domain accounts** to expand the list of existing accounts on the domain to ensure yours does not already exist.
5. Click **Add an account** and enter the necessary information.
To add a global domain account, refer to [Add a target account to a global domain \(on page 159\)](#).
To add a device account, refer to [Add a target account to a device \(on page 160\)](#).
To add an application account, refer to [Add a target account to an application \(on page 160\)](#).
6. Click **Apply**.

12.3.6. Edit a global or a local domain

About this task

When the password change is enabled on the domain, the "**Administrator account**" field allows you to select the target account which will be used to change the password on another target account in the event of a password mismatch between WALLIX Bastion and the device. This process is called "*reconciliation*".



Attention:

The administrator account is required on the local domain when using Fortinet FortiGate or IBM 3270 password change plugin. This account must be first added to the domain from the "Domain accounts" area on the domain summary page, after the domain creation step is completed. For more information, refer to [Add an account to the global or a local domain \(on page 179\)](#). After the "Enable password change" option is selected on the domain modification page, select this account from the list in the "Administrator account" field before selecting the plugin in the "Password change plugin" field.

When the global domain is associated with an external vault, the related information is displayed on the domain summary page, from the "External vault plugin" and the "Vault plugin parameters" fields.

If an SSH Certificate Authority is configured for this domain (domain type is "Global" or "Local for a device"), a line with the CA private key type and length is displayed on the domain modification page. It is then possible to:

- delete this key
- replace this key
 - by generating a new one: in this case, select the appropriate key type and length from the list (RSA 2048 by default)
 - by browsing a path to upload the file containing an existing key (in the OpenSSH or PuTTY key formats) and specifying the corresponding passphrase (if any defined)
- download the corresponding public key in the OpenSSH or ssh.com formats on the domain summary page, from the "CA public key" field



Note:

If the CA private key defined for the domain is changed, then the SSH keys for all the accounts on this domain are re-signed with the new Certificate Authority. The CA public key is transferred to the target device (for a local domain) or the target server (for a global domain) when a password change plugin is set on the concerned domain and the WALLIX Password Manager feature is associated with the license key.

For more information, refer to [Associate the domain with an SSH Certificate Authority \(on page 182\)](#).



Procedure

1. Go to the **Targets > Domains** page.
2. Select the type of domain that contains the domain you want to edit from **Display domain type**: **Global**, **Local for a device**, or **Local for an application**.
3. Click the name of the domain that you want to edit.
4. Click **Edit this domain**.
5. Edit the necessary information.
6. Click **Apply**.

12.3.7. Change the passwords for all the accounts on a global domain

About this task



Important:

The **Change passwords** feature is displayed when an administrator account is defined for the domain. The passwords are changed in accordance with the password change policy selected for the domain. For more information, refer to [Password change policies \(on page 209\)](#).

Procedure

1. Go to the **Targets > Domains** page.
2. Select **Global** from **Display domain type**.
3. Click the name of the domain for which you want to change passwords.

The global domain must have the password change option enabled. Verify that the option is enabled from the **Password change** column.

4. **Optional:** Click **Domain accounts** to expand the list of accounts on the domain to ensure all accounts can have a password change.
5. Click **Change passwords** to instantly change the passwords for all the accounts on this domain.
6. Confirm the action to change all password on the domain.

Results

The secret change results can be viewed from the **System > Syslog** page.

If the secret rotation fails, click the **More details** link in the error message to display the list of accounts whose secrets were not changed.

12.3.8. Change the passwords for all the accounts on a local domain

About this task



Important:

The **Change passwords** feature is displayed when an administrator account is defined for the domain. The passwords are changed in accordance with the password change policy selected for the domain. For more information, refer to [Password change policies \(on page 209\)](#).

Procedure

1. Go to the **Targets > Domains** page.
2. Select the type of domain that contains the domain you want to edit from **Display domain type**: **Local for a device**, or **Local for an application**.
3. Click the name of the domain for which you want to change passwords.



The local domain must have the password change option enabled. Verify that the option is enabled from the **Password change** column.

4. **Optional:** Click **Domain accounts** to expand the list of accounts on the domain to ensure all accounts can have a password change.
5. Click **Change passwords** to instantly change the passwords for all the accounts on this domain.
6. Confirm the action to change all password on the domain.

Results

The secret change results can be viewed from the **System > Syslog** page.

If the secret rotation fails, click the **More details** link in the error message to display the list of accounts whose secrets were not changed.

12.3.9. Associate the domain with an SSH Certificate Authority

About this task

A Certificate Authority (or "CA") can be associated with a local domain (type "Local for a device") or a global domain (when the latter is not associated with an external vault). It is then used to certify the SSH keys for the target accounts. A CA is defined by an SSH key pair (a private key and a public one). The CA private key signs the public keys of the target accounts on the domain. These signed public keys are also called "certificates" and are used by the SSH client to allow connection to a target server. The certificates are checked against the CA public key by the target server during connections.

Procedure

1. Copy the CA public key to `/etc/ssh/wallix_ca_user.pub`.
2. Reference the file in the sshd daemon's configuration file using the `TrustedUserCAKeys` keyword.
`TrustedUserCAKeys /etc/ssh/wallix_ca_user.pub`
3. Restart the ssh daemon.

What to do next

When a password change plugin is set on the domain, WALLIX Bastion transfers the CA public key and the subsequent configuration to the target device (for a local domain) or the target server (for a global domain). Furthermore, the public SSH key of the administrator account is not signed. To allow SSH authentication using this account, the public key must be present on the target server (usually in the file `authorized_keys` located in the home directory of the target account).

When a CA is associated with a domain, the public SSH keys for all the target accounts on this domain are automatically signed by the CA. The summary page of an account on a domain which is associated with a CA will allow to download the corresponding signed certificate, instead of an SSH public key. Furthermore, when a user wants to check out the credentials of a target account on a domain associated with a CA, the option to download the certificate is added. The private key alone is not sufficient for authentication.

12.3.10. Revoke the signed certificate for the accounts on the domain associated with a Certificate Authority

Procedure

1. Go to the **Targets > Domains** page.
2. Select the type of domain that contains the domain you want to edit from **Display domain type: Global** or **Local for a device**.
3. Click the name of the domain that you want to edit.



Select a domain which is associated with a Certificate Authority.

4. Click **Domain accounts** to expand the list of accounts on the domain and:
 - Click **Revoke all** to revoke the certificates for all the accounts on the domain.
 - Click **Revoke** revoke the certificate of a specific account.

Results

A revocation list is automatically generated and transferred to the target server to mention that this or these certificates can no longer be used for connection.

12.3.11. Delete a domain

Procedure

1. Go to the **Targets > Domains** page.
2. Select the type of domain that contains the domain you want to delete from **Display domain type: Global, Local for a device, or Local for an application.**
3. Select the domain that you want to delete.
4. Click **Delete.**
5. Confirm the permanent deletion all of the selected domains.

Results

After deleting a global domain, all related global accounts are removed, including discovered global accounts from the **Onboarding** page on the **Discovered items** and **Hidden items** views. For more information on global account onboarding, refer to [Onboard discovered global accounts \(on page 208\)](#).

12.4. Checkout policies

What is a Checkout policy?

A checkout policy defines the settings concerning the account checkout process. It can be selected during the creation or modification of a target account. For more information, refer to [Target accounts \(on page 158\)](#).



Attention:

A default checkout policy called default is configured on WALLIX Bastion. You can edit this policy but you cannot delete it.

During the credential checkout process, the user has access to the following information:

- the login of the account
- the password it is defined for the account either on the local or the remote WALLIX Bastion
- the SSH private key if it is defined for the account either on the local or the remote WALLIX Bastion
- the certificate (that is the signed SSH public key) if the account is defined on a domain associated with a Certificate Authority



12.4.1. Add a checkout policy

Procedure

1. Go to the **Targets > Checkout policies** page.
2. Click **Add**.
3. Give the new checkout policy a name and provide an optional description.
4. Enable or disable the **Enable lock** option.

Enabling account lock during the checkout process stops other users from using the account at the same time.

5. **Optional:** If you enable the **Enable lock** option, you must also:

- a. Configure the **Checkout duration**.
- b. **Optional:** Configure the **Checkout duration extension** to prolong usage.
- c. **Optional:** Configure the **Maximum checkout duration** to limit usage.

If you did not configure **Checkout duration extension**, set to 0.

If you configured both **Checkout duration** and **Checkout duration extension**, set a duration greater than or equal to the sum of both values.

- d. Choose if you want to enable **Change password at check-in** to force password update.

6. Click **Apply**.

Results

You can now select this new checkout policy for any target account.



Tip:

When target accounts are linked to this checkout policy, they are listed on the **Accounts** tab of this checkout policy. From this tab, you can edit or delete the target account.

12.4.2. Delete accounts using a checkout policy

Procedure

1. Go to the **Targets > Checkout policies** page.
2. Click the name the checkout policy that you want to edit.
3. Switch to the **Accounts** tab and click the desired account type (**Global accounts**, **Device accounts**, **Application accounts**).

The page lists all the accounts of this type associated with this checkout policy.

4. Select one or more accounts and click **Delete**.

12.4.3. Edit a checkout policy

About this task

If access to target accounts is not allowed for a profile, then the profile members cannot delete or edit a password checkout policy.

Procedure

1. Go to the **Targets > Checkout policies** page.
2. Click the name the checkout policy that you want to edit.
3. Edit the necessary information.
4. Click **Apply**.

12.4.4. Delete a checkout policy

About this task

If access to target accounts is not allowed for a profile, then the profile members cannot delete or edit a password checkout policy.



Attention:

You cannot delete a password checkout policy if at least one target account is linked to this policy.

Procedure

1. Go to the **Targets > Checkout policies** page.
2. Select the checkout policies that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected checkout policies.

12.5. Protected Users group

Prerequisites

When an AD user is a member of the Protected users group, Windows New Technology LAN Manager (NTLM) connections to a target for this user do not work. The connection must be established using Kerberos.

1. Enter the DNS configuration that must resolve the address for the KDC and the targets from **System > Network > DNS**.
2. Enable Kerberos in connection policies by checking the **Enable kerberos** box in **Session management > Connection policies > RDP**, section **[rdp]**



Note:

In the case of a group of replicated bastions, actions must be performed on the Master and on each of the bastions.



Note:

Missing or incorrect DNS entries can cause issues. To avoid this, ensure that the FQDN of the domain controller is resolved by WALLIX Bastion, and that the FQDN of WALLIX Bastion is resolved by the domain controller (entries can be added to the hosts files of WALLIX Bastion and the domain controller if necessary). Make sure you also use FQDNs when configuring target devices.

Next, a distinction must be made between a target account configured as an account mapping and a target account included in WALLIX Bastion Vault.



12.5.1. Target account configured as account mapping

About this task

When the target account is configured as account mapping, you must configure the primary accounts on the following pages:

- **Configuration > External authentications.** For more information, refer to [External sources management \(on page 91\)](#).
- **Configuration > Authentication domains.** For more information, refer to [External sources management \(on page 91\)](#).

Procedure

Follow the [Connect to an Active Directory server \(on page 53\)](#) procedure with the following requirements.

1. Create Active Directory external authentication.
2. Choose a Kerberos authentication protocol, with a name and domain name identical to the domain (in uppercase).
3. Create the Active Directory authentication domain and map Active Directory groups to WALLIX Bastion groups.

Set the Active Directory domain name to be identical to the domain name in the Kerberos configuration.

12.5.2. Target account in WALLIX Bastion Vault

About this task

When the target account exists in WALLIX Bastion Vault, there is no account mapping. The DOMAIN/REALM must be present in the target account.

For local domain,

1. Got to **Targets > Accounts > Device accounts**.
2. Add or click the relevant device account to edit the configuration.
3. Enter the account name and identifier in the **General** tab. For example, account in the **Account name** field and account@EXAMPLE.DOMAIN in the field **Account login**.

For global domain,

1. Go to **Targets > Domains**.
2. Add or click the relevant domain to edit the configuration.
3. Enter the real name of the domain in **Real name**. For example, EXAMPLE.DOMAIN. To work, the domain must not be present in the account login.

12.6. Setting up an AD authentication silo

About this task

Silos provide a way to define a relationship between accounts in an AD domain (for example: users, computers) and enforce an authentication strategy for the related accounts. Defining this relationship assigns the related accounts to a silo. The main purpose of silos is to prevent privileged user accounts from logging on computers of a lower trust level. By assigning users and computers to a silo, users from the silo will only be allowed to log on computers that are part of the same silo.

The silo to be set up on the AD and then configured in the Bastion contains:



- The trusted target server. For example, `server2019.example.com`
- The privileged user account. For example, `admin-t0`
- The service account of the trusted computer (Bastion). For example, `service-t0`

Procedure

1. [Create a global domain \(on page 173\)](#).

This global domain will manage the global accounts which will be used on AD silo/ the privileged user account and the service account.

2. [Create two global accounts for this global domain \(on page 179\)](#): the first one as a privileged user, the second as a service account.

Give the first global account (privileged user) the name `admin-t0`.

Give the second global account (service account) the name `service-t0`. Give that service account the following a **Account login**: `service-t0$`. Make sure to add the \$ symbol at the end of the service account login to identify this account as a Bastion service account.

3. [Add a Kerberos-Password external authentication \(on page 64\)](#).

The parameter configuration of this external authentication is used by the AD silo feature to initiate the session of the privileged user account on the target for the secondary connection.

4. [Create a new RDP connection policy \(on page 134\)](#). In this new policy, you must:
 - a. Enable **Advanced options**.
 - b. Activate **Enable Kerberos**.
 - c. Fill out **Krb armoring account**, **Krb armoring realm**, **Krb armoring fallback user**, **Krb armoring fallback password**.
5. [Create a device \(on page 110\)](#). For this new device, you must create a **RDP** service where the **Connection policy** matches the RDP connection policy created in the previous step.
6. [Create a target group \(on page 167\)](#) with target accounts for the privileged user and the service account. For this new target group, you must:
 - a. Create an account for the privileged user from **Session management targets > Account** with the **From:A device and global accounts** configuration. Make sure to select the previously created device, the RDP service, and the previously created global account for the privileged user.
 - b. Create an account for the service account from **Session management targets > Scenario account** with the **From:A global domain and related accounts** configuration. Make sure to select the previously created global domain and the previously created global account for the service account.

Results

The AD authentication silo is configured. Create a user group and an authorization using the target group previously configured to allow authorized users to connect to the target. For more information, refer to [Create an authorization \(on page 189\)](#).

12.7. Enabling smart card authentication on targets for RDP protocol

About this task



Note:

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



WALLIX Bastion offers users the possibility to authenticate to Windows targets using the RDP protocol with smart cards connected on the client desktop and the associated PIN code. Refer to the *Release Notes* document to view the list of smart cards compatible with WALLIX Bastion.

Procedure

1. [Create a target device \(on page 110\)](#) or edit a target device.
 - a. Create or edit a **RDP** service from the **Services** tab.
 - b. Enable the **RDP_SMARTCARD** option from the list of proxy options for that RDP service.
2. Go to **Session management > Connection policies**, and edit the **RDP** connection policy.
 - a. Enable the **Force smartcard authentication** option.
 - b. Click **Apply**.

Results

After enabling the **Force smartcard authentication** option, Network Level Authentication (NLA) is disabled. The credentials of a possible associated target account can no longer be used.

13. Authorizations

Authorization is a key object in the Bastion as it allows WALLIX Bastion administrators to give a user group access rights to a target group. Two main rights are available:

- Sessions: enables users to access sessions on targets
- Secrets: enables users to access secrets related to targets

Access rights to sessions and secrets are cumulative, without restriction.



Note:

One authorization can link only one user group to one target group.

It is not possible to create multiple authorizations with the same user group/target group pair.



Important:

Auditor can view current SSH sessions even when the session recording option is not enabled in the authorization defined for the user group and the target group.

13.1. Create an authorization

Procedure

1. Go to the **Authorization > Manage authorizations** page.
2. Click **Add**.
3. Give the authorization an identifiable name.

The name is restricted to 255 characters and cannot contain the following characters:

`\ / : * ? " < > | @ &` and space.

4. Choose the **User group** to which this authorization applies.
5. Choose the **Target group** which the user group is authorized to access.
6. Provide a description of the authorization.

The maximum length of the description is limited to 1,024 characters.

7. Select the **Authorization mode** according to the type of access requested.
8. If you selected **Sessions** or **Sessions and secrets**, select **Protocols/Sub-protocols**.

For more information, refer to [SSH options \(on page 254\)](#) and [RDP options \(on page 252\)](#).

9. Depending on the authorization mode and protocols, you can activate the following options:
 - **Session recording**: enable session recording. The type of recording depends on the protocol to access the device.
 - **Session invite**: allow a user (host) to invite an external user (guest) to join a current RDP or VNC session. When activated, there are two sub-options to choose from:
 - **View only**: the guest can only view the current session.
 - **View and control**: the guest can view the current session and control it using the mouse and keyboard when the host gives them control. The host can regain control of the session at any time.
 - **Critical targets**: indicate if the targets concerned by the authorization are critical. When activated, dedicated notifications can be sent after each access to a target (sessions and/or secrets).



10. Click **Apply** to create the authorization.
11. **Optional:** If you want add an approval workflow to the authorization, switch to the **Approval** tab.

For more information, refer to [Approval workflow configuration \(on page 191\)](#).

13.2. Approval workflow

The approval workflow is a mechanism to manage access to sessions and secrets. When a user wants to access sessions or secrets on a target, they must submit a request to the approvers first. Administrators configure the approval workflow for each authorization to further refine the access to sensitive resources. A different approval workflow can be configured if access is required inside or outside the user's authorized time frame.

There are two mandatory conditions for a user to be the approver of an authorization:

- the **Modify** right for the **Manage Approvals** feature is set in the user profile of all users of the user group (refer to [Permission profiles \(on page 22\)](#))
- the user group must be selected in the **Approvers** section on the **Approval** tab of the authorization page

Approvers can decide to allow or reject the access to a session or the checkout of secrets of a target. A request is approved when the quorum is reached. The quorum is the minimum number of favorable answers required for a particular authorization.



Note:

By default, an approver can approve their own requests. This behavior can be managed through the option **Allow self approvals** from the menu **Configuration > Configuration options > Global**. If this option is cleared, then approvers cannot view their own requests on the **My approval history** page from the **Authorizations** menu. Their requests are viewed only by the other members of the approver group.

Functioning

A user requests an approval either from the "My Authorizations" menu on the WALLIX Bastion web interface (for immediate or future access) or when connecting to an RDP or an SSH client (for immediate access). All the approvers are notified by e-mail. Approvers can then accept or reject a request using the WALLIX Bastion web interface.

The statuses of a valid request (its duration has not expired) can be either of the following:

- a request is marked as "accepted" when the quorum is reached



Note:

When the first approver accepts the request and the start date and time are reached:

- the start date and time of the request are updated with the start date and time of this action
- the end date and time are extended for the requested duration from this action

- a request is marked as "rejected" and dismissed as soon as one approver rejects it. The user is then notified by e-mail of the reason for the rejection.
- a request is "pending" as long as the quorum is not reached and it the request is not rejected.

If the request is no longer valid (the duration expired), the request is marked as "closed" and it is no longer possible for an approver to answer the request. It is also not possible to answer requests that were accepted or rejected.



Note:

A request is also marked as "closed" if one of the following elements is deleted: the requesting user or the concerned target or the concerned authorization.

An "accepted" request automatically switches to the "closed" status if the user did not connect to the target and the timeout defined for the approval is reached.

Each approver can reduce the duration of a request. The duration is incrementally decreased: a subsequent approver, when answering the same request, sees the reduced period and not the original one.

Users can view approval statuses for their requests on the "My Authorizations" menu.

When the quorum is reached, the user is notified by e-mail. The session can then be started or the target credentials can then be accessed for the allocated duration. If the session is disconnected before the end of the duration, the user can start a new session without a new approval as long as the end of the period specified by the duration of the initial approval is not elapsed. To prevent a user to reconnect after the initial session, approvers can cancel a request.

13.2.1. Approval workflow configuration

About this task

Approval workflow is defined during the configuration of authorizations. When this option is configured, a user must submit an approval request to access sessions or secrets for a target.



Important:

If both **No approval required** and **Access blocked** options are enabled in step 3 and step 4, the configuration of the approval workflow is void and cannot be saved.

Procedure

1. Go to the **Approval** tab of an authorization.
2. Enable **Approval workflow**.
3. Select the type of approval during the authorized time frame:
 - **No approval required**: the user has direct access to the sessions or secrets of a target.
 - **Automatic approval**: the approvers are notified of the approval request and the user has direct access to the sessions or secrets of a target.
 - **Approval with quorum**: the number of approvers required to approve a request for access to the sessions or secrets of a target. The number defined for a quorum must be equal to or be less than the number of approvers available in the user group.
4. Select the type of approval outside the authorized time frame:
 - **Access blocked**: access to the sessions and secrets is forbidden.
 - **Automatic approval**: the user has direct access to the sessions or secrets, but approvers are notified of the request to access the target.
 - **Approval with quorum**: the number of approvers required to approve a request for access to the sessions or secrets of a target. The number defined for a quorum must be equal to or be less than the number of approvers available in the user group.



For more information on the configuration of a time frame, refer to [Time frames for target access \(on page 251\)](#).

5. Move one or more user groups from the **Available** column to the **Selected** column to designate them as approvers.

When an approval request is issued by a user who wants to access sessions or secrets, all approvers in the selected groups are notified by e-mail. The e-mail contains a direct link to **My current approvals** page in the **Authorizations** menu where they can answer the request. This feature is available to approvers through the interface dedicated to the **User & audit features** service group.

6. Select the appropriate value for the **Comment** field.

By selecting **Mandatory**, the user and the approvers must provide the reason for the request and request decision.

7. Select the appropriate value for the **Ticket** field.

By selecting **Mandatory**, the user and the approvers must provide a ticket reference during the approval workflow.

8. Define the timeout of the approval in the **Approval timeout** field.

If the user did not connect to the target and this timeout is reached, the status of the **accepted** request is automatically changed to **closed**.

When the approver accepts the request, this value is set as the maximum value in the **Timeout** field of the form. Approvers can reduce this value.

9. **Optional:** Enable the **Single connection** option if users must be authorized access to the session only one time during the duration of the approval.

It does not apply to the checkout of secrets.

10. Click **Apply** to save the configuration.

13.3. Edit an authorization

About this task



Note:

When editing an authorization, it is not possible to edit the **User group** and **Target group** fields.

Procedure

1. Go to the **Authorization > Manage authorizations** page.
2. Click the name of the authorization that you want to edit.
3. Edit the necessary information.
4. Click **Apply**.

13.4. Import authorizations

Before you begin

The CSV file must begin with a line containing the `#wab1040 authorization` tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:



Field	Type	R(quired)/ O(ptional)	Possible values	Default value
Name	Text	R	Name of the authorization created	N/A
Usergroup name	Text	R	User group defined	N/A
Targetgroup name	Text	R	Target group defined	N/A
Sub-protoc ols	Text	R if "Proxy access" = True	Sub-protocol name ⁽¹⁾ There can be one or several sub-protocols	N/A
Critical	Boolean	R	True or False	False
Recorded	Boolean	R	True or False	False
User access	Boolean	R	True or False	False
Proxy access	Boolean	R	True or False	False
Description	Text	O	Free text	N/A
Require approval	Boolean	R	True or False	False
Has comment	Boolean	R	True or False	False False if "Require approval" = False True if "Comment mandatory" = True



Field	Type	R(equired)/ O(ptional)	Possible values	Default value
Comment mandatory	Boolean	R	True or False	False False if "Require approval" = False
Has ticket	Boolean	R	True or False	False False if "Require approval" = False True if "Ticket mandatory" = True
Ticket mandatory	Boolean	R	True or False	False False if "Require approval" = False
Approver groups	Text	R if "Require approval" = True	Approver groups defined There can be one or several approver groups	N/A Empty if "Require approval" = False
Active quorum	Integer number	R	Integer number between -1 and the number of approvers in groups At least one quorum (active or inactive) must be defined and greater than -1	"-1"
Inactive quorum	Integer number	R	Integer number between -1 and the number of approvers in groups At least one quorum (active or inactive) must be defined and greater than -1	"-1"



Field	Type	R(equired)/ O(ptional)	Possible values	Default value
Single connection	Boolean	O	True or False	False False if "Require approval" = False
Approval timeout	Integer number	O	The value is set in minutes.	"0"
Session sharing	Boolean	O	False or view_only or view_control	False

(1) Sub-protocol - one of the following values:

```

RAWTCPIP
RDP, RDP_AUDIO_INPUT, RDP_AUDIO_OUTPUT, RDP_CLIPBOARD_DOWN, RDP_CLIPBOARD_FILE,
RDP_CLIPBOARD_UP, RDP_COM_PORT, RDP_DRIVE, RDP_PRINTER, RDP_SMARTCARD
RLOGIN
SFTP_SESSION, SSH_AUTH_AGENT, SSH_DIRECT_TCPIP, SSH_DIRECT_UNIXSOCK, SSH_REMOTE_COMMAND,
SSH_REVERSE_TCPIP, SSH_REVERSE_UNIXSOCK, SSH_SCP_DOWN, SSH_SCP_UP, SSH_SHELL_SESSION,
SSH_X11
TELNET
VNC

```

Example of a valid authorization syntax:

```

#wab1040 authorization
Group_users1;target_group1;SSH_SHELL_SESSION SFTP_SESSION;False;False;True;True;
description;False;False;False;False;False;False;group_approvers;1;2False;0

```

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.

For more information, refer to [SSH options \(on page 254\)](#) and [RDP options \(on page 252\)](#).

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Authorizations** from the **Data** options.
5. Retrieve the CSV file from your computer.
6. Click **Import**.



Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

13.5. Delete authorizations

Procedure

1. Go to the **Authorizations > Manage authorizations** page.
2. Select the authorizations that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected authorizations.



14. Assets Discovery

What is Discovery?

WALLIX Bastion embeds a specific module to provide continuous automatic discovery of assets on configured networks and Active Directories, and to onboard the relevant discoveries. That module allows you to:

- configure scans
- launch scans manually
- configure an automatic scan launch
- view the results of scan jobs
- view the list of the discovered assets and onboard them in WALLIX Bastion with a configured password change plugin and password change policy

Prerequisites

To view the **Discovery** entries, the following is required:

- The **Enable discovery** option must be activated from the **Configuration > Configuration options > Module configuration** page.
- The **View** right on **Targets & accounts** and the **Modify** right on the **Settings** features with no limitations on target groups must be set in the user profile.

14.1. Configure a network scan for device discovery

About this task



Important:

Canceling a scan can be impossible if the subnet contains a large number of IP addresses. The exact number varies depending on the hardware or virtual machine configuration and the current load of your WALLIX Bastion. As a result, WALLIX recommends to never perform a network scan on a subnet with more than 8,192 IP addresses.

Procedure

1. Go to the **Targets > Discovery > Scan configuration** page.
 2. Click **Add** and click **Network** from the drop-down list.
 3. Give the new scan a name and provide an optional description to simplify management.
 4. Disable the **Enable account discovery** option to ensure that the scan discovers only devices.
 5. Add as many subnets as necessary using the CIDR notation (`<network address>/<number of mask bits>`).
- For example, `192.168.0.15/24`.
6. To create an association, select a protocol from the drop-down list then specify the related port. Click **+ Add field** to create as many associations as necessary. When created, it is possible to delete this association by clicking the  **Remove** icon.
 7. **Optional:** Configure one or more SSH banner filters using regular expressions to ensure that only devices with a banner matching the regular expressions are discovered.
 8. **Optional:** Configure the frequency at which the scan is automatically triggered.



The **Periodicity** field uses the cron syntax with the 5 following fields: `<Minute>`, `<Hour>`, `<Day_of_the_Month>`, `<Month_of_the_Year>`, `<Day_of_the_Week>`, and aliases `@`. If this field remains empty, then no periodicity is set.

For example, if `0 0 * * *` or `@daily` is entered in this field, then the scan job is set to run once a day at midnight.

9. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.
10. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.
11. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.

14.2. Configure a network scan for account discovery

About this task



Important:

Canceling a scan can be impossible if the subnet contains a large number of IP addresses. The exact number varies depending on the hardware or virtual machine configuration and the current load of your WALLIX Bastion. As a result, WALLIX recommends to never perform a network scan on a subnet with more than 8,192 IP addresses.

Procedure

1. [Create a global domain \(on page 173\)](#).
2. [Create at least one administrator account on this global domain \(on page 179\)](#).

This administrator account will discover accounts on new devices.

3. Go to the **Targets > Discovery > Scan configuration** page.
4. Click **Add** and click **Network** from the drop-down list.
5. Give the new scan a name and provide an optional description to simplify management.
6. Activate the **Enable account discovery** option to ensure that the scan discovers devices and related local accounts.
7. Select the global domain previously configured.
8. Select the administrator account related to the global domain previously configured.

You can add a maximum of 5 accounts.

9. Add as many subnets as necessary using the CIDR notation (`<network address>/<number of mask bits>`).

For example, `192.168.0.15/24`.

10. To create an association, select a protocol from the drop-down list then specify the related port. Click **+ Add field** to create as many associations as necessary. When created, it is possible to delete this association by clicking the **-** icon.
11. **Optional:** Configure one or more SSH banner filters using regular expressions to ensure that only devices with a banner matching the regular expressions are discovered.
12. **Optional:** Configure the frequency at which the scan is automatically triggered.

The **Periodicity** field uses the cron syntax with the 5 following fields: `<Minute>`, `<Hour>`, `<Day_of_the_Month>`, `<Month_of_the_Year>`, `<Day_of_the_Week>`, and aliases `@`. If this field remains empty, then no periodicity is set.

For example, if `0 0 * * *` or `@daily` is entered in this field, then the scan job is set to run once a day at midnight.



13. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.
14. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.
15. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.

14.3. Configure an Active Directory scan for device discovery

About this task



Attention:

To perform a relevant Active Directory scan for device discovery, make sure the DNS server is configured in accordance with this scan. The DNS section is accessible from the menu **System > Network**.

Procedure

1. Go to the **Targets > Discovery > Scan configuration** page.
2. Click **Add** and click **Active Directory** from the drop-down list.
3. Give the new scan a name and provide an optional description to simplify management.
4. Deactivate the **Enable account discovery** option to ensure that the scan discovers only devices.

A device must be assigned to an organization to be detected by the **Discovery** feature

5. Select an LDAP external authentication using Active Directory in the drop-down list or click the link under the field to be redirected to the authentication creation page.
6. **Optional:** Modify the LDAP/AD search filter to include additional criteria.

The default query(`objectClass=Computer`) retrieves all the computers from the directory.

7. Add the Distinguished Names (DNs) of the entries in the directory. Click **+ Add field** to add as many DN's as necessary.
8. To create an association, select a protocol from the drop-down list then specify the related port. Click **+ Add field** to create as many associations as necessary. When created, it is possible to delete this association by clicking the **-** icon.
9. **Optional:** Configure one or more SSH banner filters using regular expressions to ensure that only devices with a banner matching the regular expressions are discovered.
10. **Optional:** Configure the frequency at which the scan is automatically triggered.

The **Periodicity** field uses the cron syntax with the 5 following fields: `<Minute>`, `<Hour>`, `<Day_of_the_Month>`, `<Month_of_the_Year>`, `<Day_of_the_Week>`, and aliases `@`. If this field remains empty, then no periodicity is set.

For example, if `0 0 * * *` or `@daily` is entered in this field, then the scan job is set to run once a day at midnight.

11. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.
12. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.
13. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.



14.4. Configure an Active Directory scan for local account discovery

About this task



Attention:

To perform a relevant Active Directory scan for local account discovery, make sure the DNS server is configured in accordance with this scan. The DNS section is accessible from the menu **System > Network**.

An administrator account must be created to discover local accounts on new devices during the Active Directory scan. To do so, create a global domain from the **Domains** page. For more information, refer to [Add a global domain with a local vault \(on page 173\)](#). Then create an account for this global domain. For more information, refer to [Add an account to the global or a local domain \(on page 179\)](#).

Procedure

1. Go to the **Targets > Discovery > Scan configuration** page.
2. Click **Add** and click **Active Directory** from the drop-down list.
3. Give the new scan a name and provide an optional description to simplify management.
4. Activate the **Enable account discovery** option to ensure that the scan discovers devices.
5. For **Type of account to discover**, select **Local accounts** from the drop-down list.
6. For the **Global domain** drop-down list, select the global domain previously configured and for the **Account** drop-down list, select the administrator account previously configured.

A maximum number of 5 administrator accounts can be selected.

7. Select an LDAP external authentication using Active Directory in the drop-down list or click the link under the field to be redirected to the authentication creation page.
8. **Optional:** Modify the LDAP/AD search filter to include additional criteria.

The default query(`objectClass=Computer`) retrieves all the computers from the directory.

9. Add the Distinguished Names (DNs) of the entries in the directory. Click **+ Add field** to add as many DN's as necessary.
10. To create an association, select a protocol from the drop-down list then specify the related port. Click **+ Add field** to create as many associations as necessary. When created, it is possible to delete this association by clicking the **-** icon.
11. **Optional:** Configure one or more SSH banner filters using regular expressions to ensure that only devices with a banner matching the regular expressions are discovered.
12. **Optional:** Configure the frequency at which the scan is automatically triggered.

The **Periodicity** field uses the cron syntax with the 5 following fields: `<Minute>`, `<Hour>`, `<Day_of_the_Month>`, `<Month_of_the_Year>`, `<Day_of_the_Week>`, and aliases `@`. If this field remains empty, then no periodicity is set.

For example, if `0 0 * * * or @daily` is entered in this field, then the scan job is set to run once a day at midnight.

13. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.
14. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.
15. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.



14.5. Configure an Active Directory scan for global account discovery

Procedure

1. Go to the **Targets > Discovery > Scan configuration** page.
2. Click **Add** and click **Active Directory** from the drop-down list.
3. Give the new scan a name and provide an optional description to simplify management.
4. Activate the **Enable account discovery** option to ensure that the scan discovers devices and related local accounts.
5. For **Type of account to discover**, select **Global accounts** from the drop-down list.
6. Select an LDAP external authentication using Active Directory in the drop-down list or click the link under the field to be redirected to the authentication creation page.
7. **Optional:** Modify the LDAP/AD search filter to include additional criteria.

The default query(`objectClass=Computer`) retrieves all the computers from the directory.

8. Add the Distinguished Names (DNs) of the entries in the directory. Click **+ Add field** to add as many DN's as necessary.
9. **Optional:** Configure the frequency at which the scan is automatically triggered.

The **Periodicity** field uses the cron syntax with the 5 following fields: `<Minute>`, `<Hour>`, `<Day_of_the_Month>`, `<Month_of_the_Year>`, `<Day_of_the_Week>`, and aliases `@`. If this field remains empty, then no periodicity is set.

For example, if `0 0 * * *` or `@daily` is entered in this field, then the scan job is set to run once a day at midnight.

10. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.
11. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.
12. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.

14.6. Configure a MS Azure Active Directory scan for device discovery

Microsoft Azure prerequisites

1. Configure Microsoft Azure to give permissions to the discovery service to scan subscriptions for devices. To do so, create an application on the Azure Portal by clicking **Azure Active Directory > + Add [App Registration]**, then enter the name of the application and click **Register**.
2. In the **Certificates & secrets** application page, upload a certificate or create a secret. When created, copy the value which are needed to enter the **Secret** field in WALLIX Bastion **Azure scan parameters**.
3. In the **API permissions** application page, click **+ Add a permission** then on **Azure Data Catalog**. Select the **user_impersonation** permission and click **Add permissions**.
4. In the **Resource groups**, **Subscriptions**, **Virtual Machines**, or **VMSS** pages, click **Access control (IAM) > + Add [Add role assignment]**. In the **Roles** tab, select the **Reader** role. In the **Members** tab, select the application previously created. Click **Select** then on **Review + Assign**. As an example, if the role is assigned to the VMSS, only the VMSS of the related resource group are scanned.



Bastion scan parameters for Azure Active Directory

Procedure

1. Go to the **Targets > Discovery > Scan configuration** page.
2. Click **Add** and click **Microsoft Azure** from the drop-down list.
3. Give the new scan a name and provide an optional description to simplify management.
4. Deactivate the **Enable account discovery** option to ensure that the scan discovers only devices.
5. Select the **Authentication type**, add the **Tenant ID** and **Client ID**.
 - Tenant ID can be retrieved from the **Directory (tenant) ID** field of the application page in Azure AD.
 - Client ID can be retrieved from the **Application (client) ID** field of the application page in Azure AD.
6. Provide the Secret or Certificate and password depending on your authentication type.
 - Secret can be retrieved from the **Value** Secret ID field of the application page in Azure AD.
 - Certificate and Password: The password is mandatory only if the certificate is encrypted.
7. **Optional:** Add one or more Azure AD search filters. For each filter, select a type of filter and a value if needed.
8. To create an association, select a protocol from the drop-down list then specify the related port. Click **+ Add field** to create as many associations as necessary. When created, it is possible to delete this association by clicking the **- Remove** icon.

You can remove an association by clicking **Remove**.

9. **Optional:** Configure one or more SSH banner filters using regular expressions to ensure that only devices with a banner matching the regular expressions are discovered.

You can remove a regular expression by clicking **Remove**.

10. **Optional:** Configure the frequency at which the scan is automatically triggered.

The **Periodicity** field uses the cron syntax with the 5 following fields: `<Minute>`, `<Hour>`, `<Day_of_the_Month>`, `<Month_of_the_Year>`, `<Day_of_the_Week>`, and aliases `@`. If this field remains empty, then no periodicity is set.

For example, if `0 0 * * *` or `@daily` is entered in this field, then the scan job is set to run once a day at midnight.

11. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.
12. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.

You can remove an e-mail address by clicking **Remove**.

13. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.

14.7. Configure a MS Azure Active Directory scan for local account discovery

Microsoft Azure prerequisites

1. Configure Microsoft Azure to give permissions to the discovery service to scan subscriptions for devices. To do so, create an application on the Azure Portal by clicking **Azure Active Directory > + Add [App Registration]**, then enter the name of the application and click **Register**.



2. In the **Certificates & secrets** application page, upload a certificate or create a secret. When created, copy the value which are needed to enter the **Secret** field in WALLIX Bastion **Azure scan parameters**.
3. In the **API permissions** application page, click **+ Add a permission** then on **Azure Data Catalog**. Select the **user_impersonation** permission and click **Add permissions**.
4. In the **Resource groups, Subscriptions, Virtual Machines, or VMSS** pages, click **Access control (IAM) > + Add [Add role assignment]**. In the **Roles** tab, select the **Reader** role. In the **Members** tab, select the application previously created. Click **Select** then on **Review + Assign**. As an example, if the role is assigned to the VMSS, only the VMSS of the related resource groups are scanned.

WALLIX Bastion scan parameters for Azure Active Directory

Procedure

1. [Create a global domain \(on page 173\)](#).
2. [Create at least one administrator account on this global domain \(on page 179\)](#).

This administrator account will discover local accounts on new devices during the Active Directory scan.

3. Go to the **Targets > Discovery > Scan configuration** page.
4. Click **Add** and click **Microsoft Azure** from the drop-down list.
5. Give the new scan a name and provide an optional description to simplify management.
6. Activate the **Enable account discovery** option to ensure that the scan discovers devices and related local accounts.
7. Select the global domain previously configured.
8. Select the administrator account related to the global domain previously configured.
9. If **Enable account discovery** is activated, add the global domains and related accounts.
10. Select the **Authentication type**, add the **Tenant ID** and **Client ID**.
 - Tenant ID can be retrieved from the **Directory (tenant) ID** field of the application page in Azure AD.
 - Client ID can be retrieved from the **Application (client) ID** field of the application page in Azure AD.
11. Provide the Secret or Certificate and password depending on your authentication type.
 - Secret can be retrieved from the **Value** Secret ID field of the application page in Azure AD.
 - Certificate and Password: The password is mandatory only if the certificate is encrypted.
12. **Optional:** Add one or more Azure AD search filters. For each filter, select a type of filter and a value if needed.
13. To create an association, select a protocol from the drop-down list then specify the related port. Click **+ Add field** to create as many associations as necessary. When created, it is possible to delete this association by clicking the - icon.
14. **Optional:** Configure one or more SSH banner filters using regular expressions to ensure that only devices with a banner matching the regular expressions are discovered. When created, it is possible to delete this filter by clicking the - icon.
15. **Optional:** Configure the frequency at which the scan is automatically triggered.

The **Periodicity** field uses the cron syntax with the 5 following fields: **<Minute>**, **<Hour>**, **<Day_of_the_Month>**, **<Month_of_the_Year>**, **<Day_of_the_Week>**, and aliases **@**. If this field remains empty, then no periodicity is set.

For example, if **0 0 * * *** or **@daily** is entered in this field, then the scan job is set to run once a day at midnight.

16. Choose to activate the **Enable periodicity** option to apply the previous scan frequency, or to disable the option to not automatically perform a scan.



17. Add one or more e-mail addresses of recipients you want to notify at the end of the scan.
18. Click **Apply** to save the configuration or click **Apply and launch** to immediately launch the scan.

14.8. Launch a scan manually

About this task



Important:

Canceling a scan can be impossible if the subnet contains a large number of IP addresses. The exact number varies depending on the hardware or virtual machine configuration and the current load of your WALLIX Bastion. As a result, WALLIX recommends to never perform a network scan on a subnet with more than 8,192 IP addresses.

Procedure

1. Go to **Targets > Discovery > Scan configuration** page.
2. Select one or more scans that you want to launch.
3. Click **Launch manually** to immediately launch the selected scans.

14.9. Set a periodic scan launch

Procedure

1. Go to **Targets > Discovery > Scan configuration** page.
2. Click the name of the scan that you want to edit.
3. Under the **Scan periodicity** section, set the frequency at which the scan is automatically triggered in the **Periodicity** field.

This field supports the usual syntax on 5 fields

<Minute><Hour><Day_of_the_Month><Month_of_the_Year><Day_of_the_Week> and aliases @.

For example, if `0 0 * * * or @daily` is entered in this field, then the scan job is set to run once a day at midnight.

List of values are available under this field to define clearly this period using the cron syntax.

4. Activate the **Enable periodicity** option.
5. Click **Apply**.

Results

The scan is automatically launched according to the periodicity.



Tip:

The time at which the next scan job is triggered is displayed in the **Next job** column in the list of the configured scans.

14.10. Scan job information

From the **Targets > Discovery > Scan list** page, displays the list of the scan jobs. Each line provides the following information:

Start date



The job start date and time. Clicking the start date information opens a page with the information for this scan.

The calendar icon allows the display of a date picker to select the desired date.

Type

The type of scan, it can be **Network**, **Active Directory**, or **Microsoft Azure**.

Status

The current job status, it can be **Running**, **Success**, **Cancelled**.

Duration

When the scan is done, this indicates the total duration of the scan.

Devices discovered

When the scan is done, this indicates the total of devices discovered during the scan.

Accounts discovered

When the scan is done, this indicates the total of accounts discovered during the scan.

Scan name

The name of the scan. Clicking the name redirects to the configuration of the scan.

Subnets

The subnets for the Network scan.

Distinguished Names

The Distinguished Names for an Active Directory scan.

14.10.1. Get general information about a scan

About this task

In addition to the main information available on the **Targets > Discovery > Scan list** page, you can access the **General** tab to get more details about a scan.

This tab displays:

- the scan configuration properties
- the number of discovered devices and local accounts
- the number of discovered global accounts matching the analysis filters, if the **Enable account discovery** option is enabled in the scan configuration
- the scan progress status

Procedure

1. Click the start date and time of a scan.
The **General** tab appears with the scan information.
2. Monitor the scan progress and review its information.

14.10.2. View the raw results of a scan

About this task

When a scan successfully completes, the **Raw results** tab lists all discovered resources. The **Discovered accounts** column displays the number of discovered local accounts linked to each discovered device.

When you click on a device, you can:



- view the services associated with the device: protocols, ports, and the latency of each protocol between the device and WALLIX Bastion
- view the local accounts associated with the device and their details, if you enabled the **Enable Account Discovery** option in the scan configuration

Procedure

1. From the **Raw results** page, click the IP address of a device.
A modal window appears.
2. Do one of the following actions:
 - a. Click the **Services** tab.
 - b. Click the **Local accounts** tab.

14.11. Cancel a running scan job

Procedure

1. Go to **Targets > Discovery > Job list** page.
2. Click the **Start date** that corresponds to the running scan you want to cancel.
3. Click **Cancel**.

Results

The job now has the **Cancelled** status.

Canceling a scan can be impossible if the subnet contains a large number of IP addresses. The exact number varies depending on the hardware or virtual machine configuration and the current load of your WALLIX Bastion. As a result, WALLIX recommends to never perform a network scan on a subnet with more than 8,192 IP addresses.

If the scan is impossible to cancel, you must restart the Discovery module by running the following command as root:

```
# systemctl restart wallix-discovery
```

14.12. Onboard discovered resources in WALLIX Bastion

The **Targets > Discovery > Onboarding** page displays the list of the discovered resources. By default, it shows the **Devices / Local accounts** tab with the **Discovered items**.

Aside from onboarding, you can also

- get information on the related jobs by clicking the data in the **First discovery** and **Last discovery** columns: they contain an access link to a dedicated page. The **General** tab displays the scan configuration properties and the number of discovered devices and accounts matching the scan filters. The **Raw results** tab lists all the discovered assets during the job.
- hide irrelevant devices and accounts. To do so, click **Hide** in the blue frame. It is possible to cancel this action by clicking **Cancel** in this frame. Select the devices and accounts to hide by checking the box at the beginning of the lines. Click **Next** in the blue frame. The last step is **Summary**. This step allows you to check all selected devices and accounts you want to hide. It is possible to modify the device selection by clicking **Previous**. Then click **Hide**. The corresponding devices and accounts are then listed on the **Hidden items** view. Hidden devices and accounts can also be onboarded if needed by clicking **Onboard** and by following the previous procedure.
- unhide devices and accounts. Hidden devices and accounts can be displayed again on the **Discovered items** view. To do so, from the **Hidden items** view, click **Unhide** in the blue frame. Select the devices and accounts to unhide by checking the box at the beginning of the lines. Click **Next**. The last step is **Summary**. This step allows you to check all selected devices

and accounts you want to unhide. It is possible to modify the device selection by clicking **Previous**. Then click **Unhide**.

- delete devices and accounts. To do so, click **Delete** in the blue frame. Select the devices and accounts to delete by checking the box at the beginning of the lines. Click **Next**. The last step is **Summary**. This step allows you to check all selected devices and accounts you want to delete. It is possible to modify the device selection by clicking **Previous**. Then click **Delete**. This operation removes the selected devices and accounts from WALLIX Bastion. As an example, it can be relevant to delete devices and accounts which no longer exist and are still displayed in the **Discovered items** or **Hidden items** views. They are displayed again if they are discovered after a new scan.

14.12.1. Onboard discovered devices or local accounts

Procedure

1. Go to the **Targets > Discovery > Onboarding** page.
2. From the **Devices/Local accounts** tab, for **Select your action**, click **Onboard**.
3. Click **+** at the beginning of the line of the device to display the list of accounts related to the device.



Tip:

It is possible to filter the local accounts you want to onboard by entering the **Account login**, **Last login** or **Group** fields. Then click **Search**.

4. Select individual local accounts you want to onboard, or select the device to onboard all of its local accounts.
5. Click **Next**.
6. Select a password change plugin and a password change policy for the local accounts in the **Password change plugin** and **Password change policy** columns.

By default, the password change plugin is set to **Unix** for the devices using SSH services and to **Windows** for the devices using RDP services. The password change policy is set to **default** for each device to apply on all the related local accounts. To disable the password change plugin for local accounts of a device, select **No rotation plugin** in the **Password change plugin** column.

Example of password change plugin and policy choices.

WOLIX

Breadcrumbs: Home > Targets > Discovery > Onboarding > Devices / Local accounts

Devices / Local accounts

Selection Rotation management Summary Next Previous

Select the rotation plugin and policy to apply. Only available if local accounts are selected.

Name	Status	Password change plugin	Password change policy	Host	Services	Discovered accounts	First discovery	Last discovery
[redacted]	To onboard	Unix	default	[redacted]	SSH (+1)	38	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM
Account login	Status	Administrator account	Last login	Groups	First discovery	Last discovery		
✓ root	To onboard	-	04/07/2022, 08:53:05 AM	-	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM		
bin	To onboard	-	-	-	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM		
demon	To onboard	-	-	-	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM		
✓ sys	To onboard	-	-	-	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM		
_apt	To onboard	-	-	-	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM		
mail	To onboard	-	-	-	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM		
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	0	05/09/2022, 05:42:30 PM	05/09/2022, 05:42:30 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	37	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	38	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	38	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	38	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM
[redacted]	To onboard	-	-	[redacted]	SSH (+1)	38	05/09/2022, 05:42:30 PM	05/09/2022, 05:56:14 PM

1 device(s) and 2 account(s) selected

7. Click **Next**.



8. During the **Summary** step, you must verify that your selection is correct. If not, you can click **Previous** to make modifications to your configuration.
9. Click  **Onboard**.

Results

The local accounts are onboarded in WALLIX Bastion and the password change plugin and password change policy configuration is applied. The local accounts can be managed from the **Targets > Accounts** page.

14.12.2. Onboard discovered global accounts

Procedure

1. Go to **Targets > Discovery > Onboarding** page.
2. Switch to the **Global accounts** tab.
3. For **Select your action**, click **Onboard**.
4. Select all of the global accounts you want to onboard.
5. Click **Next**.
6. Click  **Onboard**.

Results

The global accounts are onboarded in WALLIX Bastion. They can be managed from the **Targets > Accounts** page.



Note:

After deleting a global domain, all related global accounts are removed, including discovered global accounts from the **Onboarding** page on the **Discovered items** and **Hidden items** views.



15. Secrets rotation

The secrets rotation section regroups information and procedures for managing target accounts credentials.

What is secret rotation?

Secret rotation involves manually or automatically changing passwords, SSH keys, or both for the accounts that are used to access resources through the WALLIX Bastion. Any changes made are immediately applied to the target accounts.



Tip:

Regularly updating secrets for target accounts helps prevent unauthorized access or misuse of the resource.

WALLIX Bastion offers different ways to manage secrets on target domains:

Password change policies

Available to global and local domains as a local vault type.

The password change policy defines requirements and restrictions concerning secrets (passwords and SSH keys). The purpose of these policies is to ensure that access to your targets complies with your security strategy.

A password change policy must always be coupled with a password change plugin when added to a domain.

Password change plugins

Available to global and local domains as a local vault type.

A password change plugin is an extension for synchronizing the rotation of secrets for targets from WALLIX Bastion to an external vault.

A password change plugin must always be coupled with a password change policy when added to a domain.

Password vault plugins

Available to global domains as an external vault type.

A password vault plugin is an extension that allows WALLIX Bastion to retrieve target secrets from a third-party password vault solution.

Break Glass mechanism

Break Glass is an emergency feature that allows a designated user or group of users to retrieve all the credentials of Bastion targets. This access is highly sensitive and reserved for situations where other administrative access is impossible, allowing for the rapid intervention and resolution of a blocked situation.

15.1. Password change policies

What is a password change policy?

In WALLIX Bastion, a password change policy defines the requirements for target accounts in terms of passwords, SSH keys, or both.



You can create as many custom password change policies as you require. When creating or modifying a global or local domain, you can apply whichever password change policy you want. For more information, refer to [Domains \(on page 173\)](#).

Default password change policy

WALLIX Bastion provides a default password change policy called **default**. It is not possible to edit or delete this policy.

The default password change policy enforces the following:

- No automatic scheduled rotation.
- A minimum length of 16 characters for a password, with at least 1 special character, 1 number, 1 uppercase, and 1 lowercase.
- The RSA SSH key type with a key size of 4096.



Important:

WALLIX Bastion 12.0.6 modifies the default password change policy. Until then, the default policy required at least 8 characters, however, to strengthen security, the new default policy requires at least 16 characters.

Upgrading to WALLIX Bastion 12.0.6 and ulterior versions, or restoring from a version earlier than 12.0.6 renames the former default policy to **default (legacy)**. Domains using the legacy version of the default policy continue to use it. To apply the new default policy, edit each domain using the **default (legacy)** policy and switch to the new **default** policy.

The **default (legacy)** can be edited or deleted if no domains relies on it.

Automatic change warning

WALLIX Bastion initiates a secret rotation for each target account with the automatic change option enabled when:

- the configuration of the password change policy applied to the domain is modified
- a new password change policy is applied to the domain

As a result, you must ensure that the e-mails with the new passwords are sent and can be decrypted. WALLIX recommends to test that process using a single, non-administrator account.

For more information on automatic change, refer to [Automatically trigger secret rotation for one or more target accounts \(with auto-generated secrets\) \(on page 245\)](#).

15.1.1. Add a password change policy

Procedure

1. Go to the **Password management > Password change policies** page.
2. Click **Add**.
3. Give the password change policy a name and an optional description.
4. Set the **Change periodicity**, that is the frequency at which the password change is automatically triggered.

The format follows the cron syntax, `<Minute> <Hour> <Day_of_the_Month> <Month_of_the_Year> <Day_of_the_Week>` and aliases `@`. You can either type the rule directly or use the available drop-down values to create the periodicity rule. For example, if `0 0 * *`



* or @daily is entered in this field, then the password change job is set to run once a day at midnight.

If this field remains empty, then no period of change is set.



Important:

This field must be entered to perform secret rotations using the command line. For more information, refer to [Trigger secret rotation for all target accounts using a same password change policy \(CLI\) \(on page 246\)](#).

It is also used to enable the periodic secret rotations. For more information, refer to [Schedule secret rotation for target accounts on a domain \(on page 212\)](#).

5. Select the policy type.

You can choose between **Password**, **SSH key**, and **Password and SSH key**.

6. If you selected **Password** or **Password and SSH key** as a policy type, you must set the password generation rules.

- the password length, that is, the number of characters the password must contain
- the number of non-alphanumeric ASCII characters (or special characters) which must be present in the password
- the number of lowercase letters which must be present in the password
- the number of uppercase letters which must be present in the password
- the number of digits which must be present in the password
- the characters which must be excluded from the password. When you entered a character in the field, click **+ Add** to add it to the forbidden character list. When a character is added, you can delete it from the list by clicking the **- Remove** red icon.

7. If you selected **SSH key** or **Password and SSH key** as a policy type, you must set the SSH key generation rules.

- select the SSH key type
- specify the key size. The following table summarizes the SSH key types and the corresponding allowed sizes:

Key type	Size allowed
RSA	1024 bits, 2048 bits, 4096 bits, 8192 bits
DSA	1024 bits
ECDSA	256 bits, 384 bits, 521 bits
ED25519	N/A

8. Click **Apply** to save the configuration.



15.1.2. Edit a password change policy

About this task



Attention:

If the target account access is not allowed for a profile, then the profile members cannot delete or edit a password change policy.

Procedure

1. Go to the **Password management > Password change policies** page.
2. Click the name of the password change policy that you want to edit.

You cannot edit the **default** password change policy.

3. Edit the necessary information.
4. Click **Apply**.

15.1.3. Schedule secret rotation for target accounts on a domain

Procedure

1. Go to **Password management > Password change policies**.
2. Click the name of the policy related to the domain you want to modify.

You cannot edit the **default** password change policy.

3. Configure the **Change periodicity** field.
4. Click **Apply**.

15.1.4. Modify the maximum number of parallel secret rotations

About this task



Attention:

WALLIX Bastion performance can be affected by a large number of parallel secret rotations.

Procedure

1. Go to **Configuration > Configuration options > Global**.
2. Enable **Advanced options**.
3. Under the **[main]** section, enter the maximum number of simultaneous secret rotations.
 - Enter an integer for **Credential change thread pool dimension**. This defines the number of parallel secret rotations on a domain.
 - Enter an integer for **Domain thread pool size**. This defines the number of domains that can execute a secret rotation in parallel.

As an example, assume that **Credential change thread pool size** is 50 and **Domain thread pool size** is 2. In this scenario, one domain can perform 50 secret rotations simultaneously, and two domains can perform rotations at the same time, for a total of 100 simultaneous secret rotations.

4. Click **Apply**.



15.1.5. Delete a password change policy

About this task



Attention:

If the target account access is not allowed for a profile, then the profile members can neither delete nor edit a password change policy.

Procedure

1. Go to the **Password management > Password change policies** page.
2. Select the password change policies that you want to delete.

You cannot delete the **default** password change policy.

3. Click **Delete**.
4. Confirm the permanent deletion all of the selected password change policies.

15.2. Password change plugins

What is a password change plugin?

In WALLIX Bastion, password change plugins provide the ability to manage and synchronize secret updates with an external server. Most plugins rely on the following process to update a target account secrets:

1. WALLIX Bastion connects as the target account or executes commands as the target account to try and change its own secret.
2. If the first operation fails, WALLIX Bastion uses the reconciliation account to either connect or execute the command to change the secret of the target account.

Defining a reconciliation account is optional. However, WALLIX Bastion cannot define the new secret of a target account if the former secret is unknown. As a result, WALLIX recommends to always provide a reconciliation account.

Plugin matrix

The following table illustrates the main characteristics for each plugin available by default on WALLIX Bastion. For more information on how to configure the plugin on a domain, refer to the documentation dedicated that plugin.



Note:

If you require a plugin that is not on this list, contact the WALLIX Support team.

Plugin name	Plugin version	Target product name	Supported target versions	Domain type	Target type
Check Point Gaia (on page 215)	1.0.0	All Check Point products using Gaia OS	All LTS versions supported	Local	Device



Plugin name	Plugin version	Target product name	Supported target versions	Domain type	Target type
Cisco (on page 216)	1.0.2	All Cisco products using Cisco IOS	All LTS versions supported	Global and Local	Device
Cisco Nexus (on page 216)	1.0.0	Cisco Nexus product line	All LTS versions supported	Global and Local	Device
Citrix ADC (on page 217)	1.0.0	Citrix ADC product line	All LTS versions supported	Global and Local	Device and Application
Dell iDRAC (on page 217)	1.1	All Dell products with iDRAC	All LTS versions supported	Global and Local	Device
F5 BIG IP (on page 218)	1.0.0	F5 BIG IP product line	All LTS versions supported	Global and Local	Device
Fortinet FortiGate (on page 218)	1.0	Dedicated to FortiGate product line	All LTS versions supported	Global and Local	Device
HP ILO (on page 219)	1.0.0	All HP products with ILO	All LTS versions supported	Global and Local	Device
IBM 3270 (on page 220)	1.0.0	All IBM products supporting the TN3270 protocol	All LTS versions supported	Local	Device
IBM AIX (on page 222)	1.0.0	All products using IBM AIX	All LTS versions supported	Global and Local	Device
Juniper SRX (on page 223)	1.0	Dedicated to Juniper SRX product line	All LTS versions supported	Global and local	Device
LDAP (on page 223)	1.1	All products implementing the Open LDAP standard, Free IPA solution	All LTS versions supported	Global and Local	Device



Plugin name	Plugin version	Target product name	Supported target versions	Domain type	Target type
MySQL (on page 224)	1.0.3	-	All LTS versions supported	Global and Local	Device and Application
Oracle (on page 225)	1.0.2	Dedicated to Oracle database product line	All LTS versions supported	Global and Local	Device and Application
Palo Alto PANOS (on page 225)	1.1	Dedicated to the PAN-OS product line	PAN-OS 8, PAN-OS 9, and PAN-OS 10	Global and local	Device
Ultra VNC (on page 226)	1.0.0	Ultra VNC application	All LTS versions supported	Global and Local	Device
Unix (on page 227)	1.2.1	Debian, Ubuntu, CentOS, Red Hat	All LTS versions supported	Global and Local	Device
VMWare ESX (on page 228)	1.0.0	VMware ESX, ESXi product line	All LTS versions supported	Global and Local	Device
Windows (on page 228)	2.0.1	Dedicated to Windows, Windows server, and AD	All LTS versions supported	Global and Local	Device
WindowsService (on page 231)	2.0	All Windows services available from the Windows panel (%windir%\system32\services.msc) dedicated to service account	All LTS versions supported	Global and Local	Device

15.2.1. Check Point Gaia plugin

There are no parameters to configure for this plugin.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

Specific plugin information



There is no host key shared with proxies.

15.2.2. Cisco plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Device hostname or IP address.

Port

Device port number.

SSH default port: 22.

Enable password

[Mandatory] Privilege elevation password of the "enable" command.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is a user with "superuser" privileges / administrator account set for a device.

Specific plugin information

There is no host key shared with proxies.

15.2.3. Cisco Nexus plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Device hostname or IP address.

Port

Device port number.

SSH default port: 22.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an administrator account allowed to launch the specific password change commands.



Specific plugin information

There is no host key shared with proxies.

15.2.4. Citrix ADC plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] System hostname or IP address.

Port

System port number.

SSH default port: 22.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an administrator account allowed to launch the specific change password commands.

Specific plugin information

There is a host key shared with proxies.

15.2.5. Dell iDRAC plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Device hostname or IP address.

Port

Device port number.

SSH default port: 22.

Index

[Mandatory] index of the privileged account. By default, it corresponds to index 2.

iDRAC version

[Mandatory] Device version. By default, it corresponds to Dell iDRAC8.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description



An administrator account is not required on domain.

The administrator account is a root user with "Administrator" account privileges.

Specific plugin information

There is no host key shared with proxies.

15.2.6. F5 BIG IP plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] System hostname or IP address.

Port

System port number.

SSH default port: 22.

Group name

Devices group name (for Sync)

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an administrator account allowed to launch the specific change password commands.

Specific plugin information

There is a host key shared with proxies.

15.2.7. Fortinet FortiGate plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Device hostname or IP address.

Port

Device port number.

SSH default port: 22.

Configuration

Character string referring to the section of the configuration.

Only the "System admin" configuration is supported.



Additional information about the plugin

Type of supported rotation

Password, SSH key (on local domain only)

Administrator account description

An administrator account is not required on domain.

The administrator account is an account with the `super_admin` account profile.



Attention:

The administrator account is required on the local domain for this plugin. This account must be first added to the domain from the "Domain accounts" area on the domain summary page, once the domain creation step is completed. For more information, refer to [Add an account to the global or a local domain \(on page 179\)](#).

Once the **Enable password change** option is selected on the domain modification page, select this account from the **Administrator account** list before selecting the Fortinet FortiGate plugin in the **Password change plugin**.

Specific plugin information

There is a host key shared with proxies.

15.2.8. HP ILO plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Device hostname or IP address.

Port

Device port number.

SSH default port: 22.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an administrator account allowed to launch the specific password change commands.

Specific plugin information

There is a host key shared with proxies.



15.2.9. IBM 3270 plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Port

[Mandatory] System port number (3272 over TLS default port: 623).

Scenario

[Mandatory] Scenario labeled in plain text played by the plugin to change passwords.

This scenario includes the following commands and also accepts comments and empty lines:

- `EXPECT` : expects to receive a specific character string at a given offset which must be absolute, starting from line 1 in the upper part of the terminal
- `IF EXPECT/ELSE/FI` : expects to receive a specific character string at a given offset which must be absolute, starting from line 1 in the upper part of the terminal. If the string is found, the condition in the `TRUE` block element is executed. Otherwise, the condition in the `ELSE` block element is executed if the latter exists.
- `MOVE_TO` : moves the cursor to a given position starting from line and column 1 in the upper part of the terminal (for example, command `MOVE_TO:5:18` moves the cursor to line 5 column 18)
- `PUT` : writes a specific character string at the cursor position
- `SEND_ENTER` | `SEND_PF3` | `SEND_PF4` | `SEND_PF5` | `SEND_PF6` | `SEND_PF7` | `SEND_PF8` : these commands send the specific key (for example, `ENTER` or `PF7`) to the terminal
- `LOG_ERROR` : writes the message specified as a parameter into the error logs
- `LOG_SCREEN` : writes the whole 3270 terminal screen and cursor position into the error logs
- `QUIT` : ends the session. The password is considered as unchanged.

The following variables are interpreted at runtime:

- `$admin_login` : sends the administrator user name
- `$admin_password` : sends the administrator password
- `$account` : sends the target account name for which the password is being changed
- `$old_password` : sends the old password
- `$new_password` : sends the new password. The password is considered as changed if the script for the scenario is successfully executed.

Scenario example: An AS/390 emulator with 3270 capabilities can be found at <http://www.canpub.com/teammpg/de/sim390/>

```
#####
# Script for MUSIC AS/390 emulator
# with TN3270 support

#####

####
# Welcome screen
EXPECT:16:Multi-User System for
SEND_ENTER
```



```
#####
# Login screen
EXPECT:3:MUSIC Userid:
PUT:$account
MOVE_TO:5:18
PUT:$old_password
SEND_ENTER

#####
# Login errors
IF EXPECT:7:Password incorrect
    LOG_ERROR:Bad password !
    QUIT
FI

IF EXPECT:7:Userid is not authorized
    LOG_SCREEN
    LOG_ERROR:Bad username
    QUIT
FI

#####
#
EXPECT:1:Userid last signed
SEND_ENTER

#####
# Change password
EXPECT:12:Change password
PUT:7
SEND_ENTER

EXPECT:17:Enter your current MUSIC sign-on password
PUT:$old_password
SEND_ENTER

EXPECT:19:Enter a new MUSIC sign-on password
PUT:$new_password
SEND_ENTER

EXPECT:23:Please enter the new password again
PUT:$new_password
SEND_ENTER

#####
# End of changing password
IF EXPECT:4:SELECT OPTION
    PUT:X
ELSE
    # Quit with an error
    LOG_ERROR>Password has not been changed
    # Print the terminal screen to syslog
    LOG_SCREEN
    QUIT
FI

# End of script. If reached, password has been successfully changed
```

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is a user allowed to change passwords.

**Attention:**

The administrator account is required on the local domain for this plugin when the variables `$admin_login` and `$admin_password` are specified in the scenario. This account must be first added to the domain from the "Domain accounts" area on the domain summary page, once the domain creation step is completed. For more information, refer to [Add an account to the global or a local domain \(on page 179\)](#). Once the "Enable password change" option is selected on the domain modification page, select this account from the list in the "Administrator account" field before selecting the IBM 3270 plugin in the "Password change plugin" field.

Specific plugin information

There is no host key shared with proxies.

15.2.10. IBM AIX plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] System hostname or IP address.

Port

System port number.

SSH default port: 22.

Root password

Password to connect as "root".

The root account may not be able to connect to the target to perform the password change via SSH under certain circumstances, for security reasons. In this case, the plugin will refer to the administrator account set for the domain to connect to the target and then use the root password via the "su" command.

When reconciliation is needed, the authentication with password or SSH key is attempted for the administrator account.

Additional information about the plugin**Type of supported rotation**

Password, SSH key

Administrator account description

An administrator account is not required on domain if the user has a password command access.

The administrator account is an administrator account with "sudo", "passwd", "pwdadm" rights.

Specific plugin information

There is a host key shared with proxies.



15.2.11. Juniper SRX plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Port

Device port number.

SSH default port: 22.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an "admin" user with "super-user" privileges.

Specific plugin information

There is no host key shared with proxies.

15.2.12. LDAP plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory] Server hostname or IP address.

Port

[Mandatory] Server port number.

Default port: 389.

Encryption

[Mandatory] Encryption protocol to use: STARTTLS (default value), TLS, or None.

Active Directory

Option to select if the password change is associated with Active Directory.

Network timeout

Maximum time period expressed in seconds for connection attempt to the server.

Administrator Bind DN | Administrator password

Bind DN and password of the administrator allowed to connect to the LDAP or Active Directory. These parameters are required.

For example, for LDAP Bind DN: `CN=administrator, DC=mycompany, DC=com`

For example, for Active Directory Bind DN: `administrator@mycompany.com`

**Attention:**

If an administrator account is set on the domain for this plugin, then the parameters of this account are used to connect to the LDAP or Active Directory. Those defined in the **Administrator Bind DN** and **Administrator password** fields are then not considered.

This account must be first added to the domain from the "Domain accounts" area on the domain summary page, once the domain creation step is completed. For more information, refer to [Add an account to the global or a local domain \(on page 179\)](#). Once the "Enable password change" option is selected on the domain modification page, select this account from the list in the "Administrator account" field prior to select the LDAP plugin in the "Password change plugin" field.

Password attribute

[Mandatory] Password attribute required for password change. It corresponds to the LDAP attribute **userPassword** by default.

User DN format

[Mandatory] Syntax of the user DN used to specify the account concerned by password change. By default, it corresponds to the string `CN=${USER},DC=dev,DC=example,DC=com` where parameter `${USER}` will be replaced by the user name. This format is also used for the administrator account which may be set on the domain for this plugin.

Custom parameters

Additional custom attributes to be specified for password change. These parameters may be required by the server and depend on its configuration. Each `parameter=value` pair must be labeled on a single line.

Additional information about the plugin**Type of supported rotation**

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is a user allowed to change passwords.

Specific plugin information

There is no host key shared with proxies.

15.2.13. MySQL plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Database hostname or IP address.

Port

Database port number.



Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is a superuser account with full privileges.

Specific plugin information

There is no host key shared with proxies.

15.2.14. Oracle plugin

This plugin allows you to change the Oracle database password.

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] Database hostname or IP address.

Port

Database port number

Service name

[Mandatory] Database service name (SID).

Admin mode

Connection mode for the administrator account. The relevant mode can be selected from the list of values. This parameter is set to implement reconciliation. When reconciliation is implemented, the password is changed and the locked account is released.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is a user with the "ALTER USER" system privilege.

Specific plugin information

There is no host key shared with proxies.

15.2.15. Palo Alto PANOS plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Port

Server port number.



SSH default port: 22.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an administrative account with superuser privileges.

Specific plugin information

There is no host key shared with proxies.

15.2.16. Ultra VNC plugin



Important:

The Ultra VNC plugin is incompatible with the default password change policy. That is because the VNC protocol only permits an 8-character password, but the default password change policy enforces 16 characters. To prevent password truncation, create a password change policy with an 8-character limit and link it to domains using the Ultra VNC Plugin. For more information, refer to [Password change plugins \(on page 213\)](#) and [Domains \(on page 173\)](#).

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] System hostname or IP address.

Port

System port.

SSH default port: 22.

Connection Account

Account used for SSH connection.

Account Password

Password for SSH account.

Path of setpasswd.exe

Full path of setpasswd.exe in unix format. For example: /drives/c/Program Files/uvnc bvba/UltraVNC/setpasswd.exe

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.



The administrator account is a Windows local administrator.

Specific plugin information

Prerequisite: a Cygwin or an SSH connection to the Windows server hosting Ultra VNC is necessary.

There is a host key shared with proxies.

15.2.17. Unix plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] System hostname or IP address.

Port

System hostname or IP address.

SSH default port: 22.

Root password

Password to connect as "root".

The root account may not be able to connect to the target to perform the password change via SSH under certain circumstances, for security reasons. In this case, the plugin will refer to the administrator account set for the domain to connect to the target and then use the root password via the "su" command.

When reconciliation is needed, the authentication with password or SSH key is attempted for the administrator account.

Additional information about the plugin

Type of supported rotation

Password, SSH key, SSH CA certificate.



Important:

Rotation for Unix targets requiring both SSH key and password authentications is not supported.

Administrator account description

An administrator account is not required on domain.

The administrator account is an account with the right to execute sudo, passwd commands.

Specific plugin information

There is a host key shared with proxies.



15.2.18. VMWare ESX plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory only for a global domain] System hostname or IP address.

Port

System port.

SSH default port: 22.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is an administrator account allowed to launch the specific change password commands and with shell access.

Specific plugin information

There is a host key shared with proxies.

15.2.19. Windows plugin

Parameters

The following configuration is required when adding the plugin to a domain.

Password Change Method

The following methods are available:

- **Samba**: for global and local domains. Use the 139 and 445 ports.
- **Kerberos (recommended)**: for global domains. Use the 88 and 464 ports.
- **WinRM**: for global and local domains. Use the 5985 and 5986 ports.

Depending on the selected method, the remaining parameters can be mandatory or optional.

Port

Only for the **WinRM** method. Optional.

The server port.

Kerberos realm

Only for the **Kerberos (recommended)** method.

The Kerberos realm name.

Kerberos configuration file

Only for the **Kerberos (recommended)** method.

The path to the Kerberos configuration file which contains the information for the domain. For more information on the configuration file, refer to [Kerberos configuration file \(on page 229\)](#).

Domain controller address

Only for the **WinRM** and **Samba** methods on global domains.

The domain controller hostname or IP address.

Kerberos configuration file

For the plugin to function with the Kerberos method, you must add a Kerberos configuration file for the domain in WALLIX Bastion. The default file can be retrieved at the following location: `/opt/wab/share/plugins/cred_chg/windows/krb5_realm.conf`.



Warning:

Do not modify the default Kerberos configuration file.

Do not store new Kerberos configuration files in the same directory as the Windows plugin (`/opt/wab/share/plugins/cred_chg/windows/`).



Tip:

WALLIX recommends to create a dedicated Kerberos configuration file for each domain.

You must duplicate the default file to ensure you have a new configuration file to modify. Store the duplicated file somewhere available to the `wabuser` account. For example, WALLIX recommends the following location: `/var/wab/etc`. Also ensure that the file has at least the following permissions:
`-r--r----- wabuser wabuser`.

In the new Kerberos configuration file, you must replace the following information with the expected values:

- `<REALM>` with the Kerberos realm name. For example `ACME.COM`.
- `<KDC_SRV>` with the domain name or IP address of the KDC server. For example, `ad01.acme.com`.
- `<KPASSWD_SRV>` with the domain name or IP address of the administration server. For example, `ad01.acme.com`.



Attention:

The `[domain_realm]` section of the configuration file may be ignored for standard configurations where domain and realm are the same (one in uppercase, the other in lowercase). If this is your situation, you can erase the section from the duplicated configuration file.

If your situation is not standard, for example if domain and realm do not match, replace `<DOMAIN>` with the FQDN of the domain. For example, if your domain is `mycompany.com` and realm is `ACME.COM` replace `<DOMAIN>` and `<REALM>` with their appropriate values in the duplicated configuration file.



```
default_realm = <REALM>

[libdefaults]

    default_tgs_encrypes = aes128-cts-hmac-sha256-128 aes256-cts-hmac-sha384-192
aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 camellia256-cts-cmac
camellia128-cts-cmac
    default_tkt_enctypes = aes128-cts-hmac-sha256-128 aes256-cts-hmac-sha384-192
aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 camellia256-cts-cmac
camellia128-cts-cmac
    permitted_enctypes = aes128-cts-hmac-sha256-128 aes256-cts-hmac-sha384-192
aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 camellia256-cts-cmac
camellia128-cts-cmac
    clockskew = 300
    kdc_timesync = 1
    ccache_type = 4
    forwardable = false
    proxiable = false

[realms]
<REALM> = {
    kdc = <KDC_SRV>:88
    admin_server = <KPASSWD_SRV>:88
}

[domain_realm]

.<DOMAIN> = <REALM>
<DOMAIN> = <REALM>
```

Reconciliation account specificity

To allow the automatic secret change feature to perform correctly:

- on a standalone Windows Server, the privileged account must be included in the local administrator group.
- on a Windows Server configured with AD, the privileged account must have the "Reset password" right set for the other accounts on the domain.



Targets prerequisites

! Attention:

To ensure automatic secret rotation in WALLIX Bastion work correctly, especially with the rotation at check-in is enabled, set the default minimum password age in Windows password policy to 0.

- On a standalone Windows Server, change the minimum password age in the Windows security settings for local accounts at the local policy level. Go to **Local Security Policy > Account Policies > Password Policy > Minimum password age**.
- On a Windows Server with Active Directory, change the minimum password age in the Windows security settings at the group policy for accounts on domains level. Go to **Group Policy Management Editor > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy > Minimum password age**.

As all commands are executed remotely, you must disable the "Deny access to this computer from the network" local policy. Go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > User rights Assignments**.

To avoid any timeout error when performing password change on a target under Windows Server 2012, WALLIX recommends to enable the `Netlogon Service(NP-In)` rule in the Windows firewall advanced settings.

User Account Control (UAC) can sometimes interfere with password change, WALLIX then recommends to enable the "`LocalAccountTokenFilterPolicy`" registry key to remotely change the passwords. You can follow those instructions: [LocalAccountTokenFilterPolicy procedure](#)

Additional information about this plugin

Type of supported rotation

Password

Administrator account description

An administrator account is not required on domain.

The administrator account is the local administrator account or domain account with the "Reset password" right set for the other accounts on the domain.

Specific plugin information

There is no host key shared with proxies.

15.2.20. WindowsService plugin

The WindowsService password change plugin is used to configure the rotation of the service account password in AD/LDAP and to manage the propagation of the new password to the concerned device(s) for all services using the service account, with only one configured global domain. It is not necessary to specify the name of the service for which password is changed. For more information on how to configure secret rotation for Windows service accounts in a global domain, refer to [Configure secret rotation for Windows service accounts in a global domain \(on page 233\)](#).

**Attention:**

To allow full operation of the password change process on a Windows service, the installation of PowerShell 3.0 or later and the activation of WinRM are required on the Windows server.

Parameters

The following configuration is required when adding the plugin to a domain.

Host

[Mandatory] Server hostname or IP address.

Port

[Mandatory] Server port number.

Default port: 389.

Encryption

[Mandatory] Encryption protocol to use: **STARTTLS** (default value), **TLS**, or **None**.

Active Directory

[Optional] Enable if the password change is associated with Active Directory.

Network timeout

Maximum time period expressed in seconds for connection attempt to the server.

Administrator Bind DN and Administrator password

[Mandatory] Bind DN and password of the administrator allowed to connect to the LDAP or Active Directory.

For example, for LDAP Bind DN: `CN=administrator, DC=mycompany, DC=com`

For example, for Active Directory Bind DN: `administrator@mycompany.com`

**Attention:**

If an administrator account is set on the domain for this plugin, then the parameters of this account are used to connect to the LDAP or Active Directory. Those defined in the **Administrator Bind DN** and **Administrator password** fields are then not considered.

This account must be first added to the domain from the "Domain accounts" area on the domain summary page, once the domain creation step is completed. For more information, refer to [Add an account to the global or a local domain \(on page 179\)](#). Once the "Enable password change" option is selected on the domain modification page, select this account from the list in the "Administrator account" field prior to select the LDAP plugin in the "Password change plugin" field.

Password attribute

[Mandatory] Password attribute required for password change.

The default value is the LDAP attribute `"userPassword."`

User DN format



[Mandatory] Syntax of the user DN used to specify the account concerned by password change.

By default, it corresponds to the string `CN=${USER},DC=dev,DC=example,DC=com` where parameter `${USER}` will be replaced by the user name. This format is also used for the administrator account which may be set on the domain for this plugin.

Custom parameters

These parameters may be required by the server and depend on its configuration.

Additional custom attributes to be specified for password change. Each `parameter=value` pair must be labeled on a single line.

Transport

[Mandatory] Relevant transport protocol for the propagation: **Kerberos** (default value), **CredSSP**, or **NTLM**.



Attention:

If the transport protocol defined for this plugin is Kerberos, then the fields **Kerberos realm**, **Kerberos KDC** and **Kerberos port** must be specified on the global domain page of the administrator account selected during the definition of the reference. For more information, refer to [Add a global domain with a local vault \(on page 173\)](#).

Restart rotated services after propagation

[Optional] It is not recommended to restart Windows services because the credentials are updated after propagation,. However, if restarted, Windows properly manages all the service dependencies.

Additional information about the plugin

Type of supported rotation

Password

Administrator account description

An administrator account is required on domain.

The administrator account is an administrator account with Remote Management (WinRM) enabled.

Specific plugin information

There is no host key shared with proxies.

15.2.20.1. Configure secret rotation for Windows service accounts in a global domain

About this task



Tip:

For more information on Windows Service accounts, refer to the [official Microsoft documentation](#)

The WindowsService password change plugin is used to configure the rotation of the service account password in AD/LDAP and to manage the propagation of the new password to the concerned devices for all services using the service account, with only one configured global domain. It is not necessary to specify the name of the service for which password is changed.



The WindowsService plugin secures standalone managed service accounts (SMSA), which are the most common form of service accounts.

The WindowsService plugin supports the following Windows service account formats:

- `service_account_name@domain_address`
- `domain_name\service_account_name`
- `.\service_account_name` (it is not recommended to use this format)



Procedure

1. [Create a global domain with a local vault \(on page 173\)](#) and configure **WindowsService** as a password change plugin.
2. For the domain administrator account (the account used to propagate secrets following secret rotation), disable automatic secret changes.
 - a. Go to the **Targets > Accounts > Global account** page.
 - b. Click the name of the administrator account to edit its information.
 - c. Deactivate the **Automatic password change** and **Automatic SSH key change** options.
 - d. Click **Apply**.
3. Configure a service account (account on which the password is changed).

It is possible to manually configure a service account (for more information, refer to [Add a target account to a global domain \(on page 159\)](#)) and to add as many service accounts related to the global domain as necessary.



Note:

The **Automatic password change** and **Automatic SSH key change** options must be selected.

To manage secret rotation on a larger number of service accounts, it is recommended to use the WALLIX Bastion discovery feature (refer to [Assets Discovery \(on page 197\)](#)).

4. Configure references.

The configuration of references simplifies the secret rotation on services. References are the way for the Bastion administrator to reference the device where a service account (saved as a global account) is used by at least one service. For more information, refer to [Define references for service account management \(on page 162\)](#).

- a. Go to the **Targets > Accounts > Global accounts** page.
- b. Select the service account previously configured.
- c. Switch to the **References** tab.
- d. Click  **Add** and provide the following information:
 - **Name**
 - **Global domain**: select the global domain previously configured.
 - **Devices**: select the devices related to the services using the service account. If the device is not created, add a device from the **Targets > Devices** page. For more information, refer to [Create a new device \(on page 110\)](#).
 - **Administrator account**: select the global domain and the related administrator account previously configured.
- e. Click **Apply and close**.

15.3. External password vault plugins

What is a password vault plugin?

WALLIX Bastion offers a modular approach that guarantees password management is both flexible and secure, allowing for a seamless integration and management of credentials across different systems. There are two possible sources for external vault plugins:

- **Vault Solutions:** leverage vault solutions such as CyberArk Enterprise Password Vault, HashiCorp Vault, and Thycotic Secret Server.
- **Remote Bastion:** leverage the password vault of another WALLIX Bastion. This approach allows one Bastion in a cluster to manage user sessions on targets and access to target accounts credentials. This includes tasks like secret rotation (target account passwords and SSH keys) and setting checkout policies.

**Note:**

External vault accounts are mapped into the local Bastion through global domains, which act as containers.

Multiple domains can link to the same external vault.

**Attention:**

This page is only displayed when the External Vaults feature is associated with the license key. If you cannot access the feature, contact an administrator with access to the license to verify if the feature is included in your package.

15.3.1. Bastion plugin

The Bastion plugin enables one WALLIX Bastion to access the password vault of another WALLIX Bastion. While the credentials are managed and stored by the original Bastion, the plugin allows the other Bastion to access these credentials and sessions. This is achieved through the original Bastion's REST API, which creates a secure communication channel. This channel allows for the checkout or check-in of account credentials and can extend the checkout duration, depending on the original Bastion's policies.

**Important:**

When using a Master/Slaves HA Database Replication architecture with the password change at check-in feature, all Slaves must have a Bastion plugin connected to the Master.

**Tip:**

To separate password and session management without an external solution, WALLIX recommends dedicating one Bastion to password management and configuring the Bastion plugin on another Bastion used for sessions.

Configuration details

The following configuration is required when adding the plugin to a global domain.

API URL

[Mandatory] The URL of the REST API to access the vault. The minimum supported API version is 2.3.

This URL must:



- start with `https://`
- end with `/api/vX.Y` where X and Y stand for the version number

API key

[Optional] The key to connect to the REST API.

This key must be generated on the remote WALLIX Bastion.

Force use of service account

[Optional]

Activating this option forces WALLIX Bastion to attempt to connect with the service account to the REST API.

Deactivating this option forces WALLIX Bastion to attempt to connect with the credentials of the authenticated user before trying with the service account.

Service account login

[Optional] The login of the service account to connect to the REST API. This login must correspond to the user name of an account on the remote WALLIX Bastion.

Service account password

[Optional] The password of the service account to connect to the REST API.

15.3.2. CyberArk Enterprise Password Vault plugin

Configuration details

This plugin allows access to the password vault of the CyberArk Enterprise Password Vault privilege management solution using the REST API Web Service.

The following configuration is required when adding the plugin to a global domain.

API URL

[Mandatory] The URL of the REST API to access the vault.

This URL must

- start with `https://`
- end with `/PasswordVault`

Safe name

[Mandatory] The name of the container in the CyberArk Enterprise Password Vault privilege management solution which stores the secrets.

Service account login

[Optional] The login of the service account to connect to the REST API. This login must correspond to the user name of an account in the CyberArk Enterprise Password Vault privilege management solution.

Service account password

[Optional] The password of the service account to connect to the REST API.

Maximum checkout duration in minutes

[Optional] The maximum duration for credentials checkout, expressed in minutes. If this duration is reached, the system automatically performs a check-in.



Entering 0 disabled the automatic check-in feature.

15.3.3. HashiCorp Vault plugin

This plugin allows access to the vault of the HashiCorp Vault secret management solution using the REST API Web Service.

Configuration in the HashiCorp Vault secret management solution

The following parameters must be set for the vault secret engine:

- **Secret Engine Type:** Key/Value (KV)
- **Engine version:** Version 1

The secret data is structured as follows in the solution:

1. Vault root

└─ 2. Name of the secret engine
└─ 3. Account name in WALLIX Bastion
└─ Login (field login)
└─ Password (field password)
└─ SSH certificate (field ssh_certificate)
└─ SSH key (field ssh_key)
└─ Other account name in WALLIX Bastion
└─ Login (field login)
└─ Password (field password)
└─ SSH certificate (field ssh_certificate)
└─ SSH key (field ssh_key)

Each secret engine is associated with a domain.

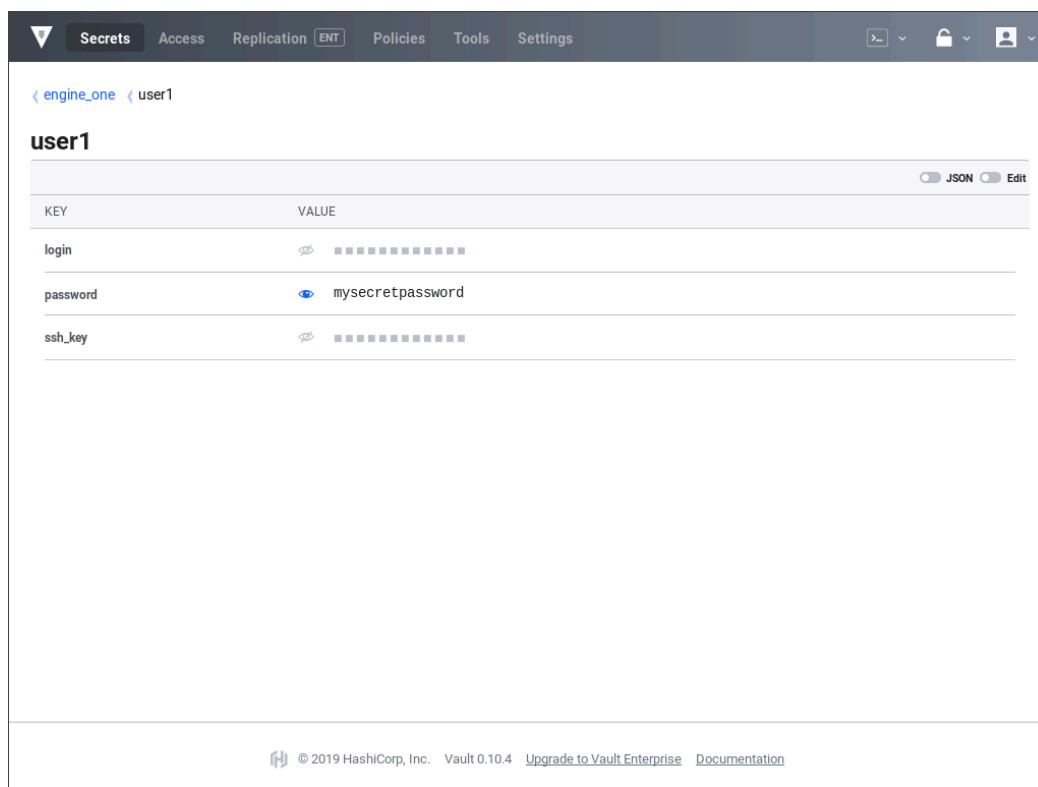
Account data in the solution is UTF-8-encoded.

The login and at least one credential (password or SSH key) are required.

The SSH key must be entered in the OpenSSH or PEM formats. The certificate corresponds to the content of a signed public key which can be downloaded from the web interface of WALLIX Bastion.

Example of secret data

The following is an example of secret data for account `user1` in engine `engine_one` in HashiCorp Vault secret management solution.



Configuration details in WALLIX Bastion

The following configuration is required when adding the plugin to a global domain.

API URL

[Mandatory] The URL of the REST API to access the vault.

Secret engine path

[Mandatory] The access path to the vault secret engine.

Secret path

[Mandatory] Path to the secret directory in the vault secret engine

Engine version

[Mandatory] The version of the Key/Value secret engine.

Token

[Optional] The token to access the vault through the Token authentication method.

Username

[Optional] The login of the account to access the vault through the `Userpass` authentication method. This login must correspond to the user name of an account in the HashiCorp Vault secret management solution.

Password

[Optional] The password of the account to access the vault through the `Userpass` authentication method.

PKCS#12 file

[Optional] The PKCS#12 file to provide the private and public keys to access the vault through the TLS Certificate authentication method.

PKCS#12 file passphrase



[Optional] The passphrase to unlock the keys provided through the PKCS#12 file for the TLS Certificate authentication method.

Role name

[Optional] The name of the role associated with the Certificate Authority (CA) on the server of the HashiCorp Vault secret management solution.



Note:

Mapping occurs between the account name in the WALLIX Bastion solution and the secret name in the HashiCorp Vault secret management solution. The account name must correspond to the secret name in the HashiCorp Vault secret management solution. If the secret name entered is `user1`, this same name must be assigned to the account name.

It is possible to create an account login from the **Targets > Accounts > Global accounts** page and set a password for it, without affecting data mapping between the two solutions.

15.3.4. Thycotic Secret Server plugin

This plugin allows access to the vault of the Thycotic Secret Server secret management solution using the REST API Web Service. This plugin allows checkout and check-in operations on passwords and SSH keys of the target accounts. However, it does not allow to extend the checkout duration for the credentials.

Some features in the Thycotic Secret Server secret management solution are not supported by WALLIX Bastion. As a result, the secrets managed by accounts enabling at least one of the following features cannot be accessed:

- DoubleLock protection is set
- an approval is required
- a comment is required

Configuration details in WALLIX Bastion

The following configuration is required when adding the plugin to a global domain.

API URL

[Mandatory] The URL of the REST API to access the vault.

This URL must:

- start with `https://`
- end with `/SecretServer`

Service account login

[Optional] The login of the service account to connect to the REST API. This login must correspond to the user name of an account in the Thycotic Secret Server secret management solution.

Service account password

[Optional] The password of the service account to connect to the REST API.

Login field



[Mandatory] The name of the field storing the account login in the Thycotic Secret Server secret management solution. This name is case-sensitive and contains **Username** as a default value.



Attention:

If no service account is used, the user must then provide a password when authenticating via RDP or SSH proxies or the web interface to access the vault of the Thycotic Secret Server secret management solution. As authentications through X.509 certificate, SSH key, or Kerberos ticket do not work in this context, it is required to define a service account.

Workflow to access the vault

The workflow to access the vault and retrieve the secret of an account is as follows:

- If the user authenticated using a login and a password, these credentials are used to access the server of the Thycotic Secret Server secret management solution.
- If the user authenticated without providing a password (Kerberos ticket, SSH key, X.509 certificate, etc.), the service account is used to retrieve the secret. In this case, the service account must have at least the same rights as the user.
- If none of these methods work, it is impossible to access the vault and retrieve a secret.

15.3.4.1. Retrieving an account secret in Thycotic Secret Server

To retrieve the secret (that is, the password or the SSH key) of an account in the Thycotic Secret Server secret management solution, the account must be mapped into WALLIX Bastion through a global domain acting as an external vault account container.

The search is done through the specification of the secret ID number of the external vault's account in the **Login** field of the target account in WALLIX Bastion. This target account is then used to map the account in the vault of the Thycotic Secret Server secret management solution.

Find the account

For example, search for account whose secret ID corresponds to 26. On Thycotic Secret Server solution interface, the parameters of the account are as follows:



The URL in the screenshot shows that the secret ID of the concerned account is 26.

Provide the plugin parameters in WALLIX Bastion

On WALLIX Bastion web interface, the parameters defined for the Thycotic Secret Server plugin are as follows:

The value in **Login field** corresponds to the field name storing the account login in the Thycotic Secret Server secret management solution, that is **Username**.

In this example, the value of the account login stored in the **Username** field is `root`, as shown on the previous screenshot.

Parameters for target account

On WALLIX Bastion web interface, the parameters defined for the target account are defined as follows:

The **Account name** field contains the target account name which is displayed on the selector of the proxy client, that is `SSH_root`.

The **Account login** field includes the secret ID number 26 to map the account in the Thycotic Secret Server solution and retrieve the corresponding secret.

15.4. Configure automatic secret rotation for a domain

Procedure

- Configure a [password change policy \(on page 209\)](#).
- Configure the [Domain \(on page 173\)](#) with the following requirements:
 1. Activate the **Enable password change** option.
 2. For **Administrator account**, pick the target account used to modify the secrets on this domain's target accounts if the WALLIX Bastion and the device do not match. This operation is called *reconciliation*.
 3. In the **Password change policy** field, select the policy previously created.
 4. In the **Password change plugin** field, select the relevant plugin and enter the related parameters. For more information, refer to [Password change plugins \(on page 213\)](#).
- Configure the [target accounts \(on page 158\)](#) with the following requirements:
 1. Enable the **Automatic password change** option to activate the secret change of this account.
 2. Enable the **Automatic SSH key change** option to activate the SSH key change of this account.



Note:

WALLIX recommends to disable the automatic secret change on the administrator account related to the domain.



15.5. Configure automatic secret rotation for a target account at check-in

Procedure

1. Go to the **Targets > Checkout policies** page.
2. Click the name of the checkout policy that you want to edit.
3. Activate the **Enable lock** option.
4. Configure the following fields:
 - a. Configure the **Checkout duration**.
 - b. **Optional:** Configure the **Checkout duration extension** to prolong usage.
 - c. **Optional:** Configure the **Maximum checkout duration** to limit usage.

If you did not configure **Checkout duration extension**, set to 0.

If you configured both **Checkout duration** and **Checkout duration extension**, set a duration greater than or equal to the sum of both values.

5. Enable the **Change password at check-in** option.
6. Click **Apply**.

15.6. Manually trigger secret rotation for a target account (with user-generated secrets)

About this task

You can manually launch the account password, SSH private key change, or both, for one of the following types: global domain account, device account, and application account. The credentials are changed:

- in accordance with the password change policy selected for the domain. For more information, refer to [Password change policies \(on page 209\)](#).
- when the checkout policy allows the password change at check-in. For more information, refer to [Checkout policies \(on page 183\)](#).



Important:

The manual credential change is only possible for accounts belonging to a domain on which the password change option is enabled.

Procedure

1. Go to the **Targets > Accounts** page.
2. Select the desired account type from the drop-down list.
3. Click the name of the target account that you want to edit.
4. Depending on the information you want to change,
 - on the **Password** tab: enter and confirm the new password of the account and enable **Propagate credential change**.
 - on the **Private key uploading** page of the **SSH private key** tab: upload the new key and enable **Propagate credential change**.
5. Click **Apply** to launch the credential change for the account.



Results

A message indicates if the secret change failed or if it is successful. If successful, the credentials are instantly changed on WALLIX Bastion and propagated on the related targets.

15.7. Manually trigger secret rotation for one or more target accounts (with auto-generated secrets)

Procedure

1. Go to **Targets > Accounts**.
2. Select the type of account that you want to edit (**Global accounts**, **Device accounts**, or **Application accounts**).
3. Select one or more target accounts and click **Automatic credential change**.

Only accounts for which **Password change on domain** is enabled can be selected.

4. Select the **Credential types**.
5. Verify the list of the selected accounts.
6. Click **Apply and close** to apply the configuration.

Results

A message confirms the secret change on the selected target accounts.

What to do next



Note:

If secret rotation fails on accounts, click the **More details** link in the error message. The list of the concerned accounts is displayed.

15.8. Automatically trigger secret rotation for one or more target accounts (with auto-generated secrets)

About this task

You can launch the automatic password and SSH private key change for one or more accounts of the following types: global domain account, device account, and application account. The credentials are automatically changed:

- in accordance with the password change policy selected for the domain. For more information, refer to [Password change policies \(on page 209\)](#).
- when the checkout policy allows the password change at check-in. For more information, refer to [Checkout policies \(on page 183\)](#).

Before you begin

The automatic credential change is only possible for accounts belonging to a domain on which the password change option is enabled.

Procedure

1. Go to the **Targets > Accounts** page.
2. Select the desired account type from the drop-down list.
3. Select the target accounts which belong to a domain enabling the credential change.
4. Click **Automatic credential change**.
5. Select the credential types you want to change and the relevant accounts in the new window.
6. Click **Apply and close** to launch the automatic credential change for the accounts.



Results

After this change is launched, the credentials are instantly changed on WALLIX Bastion and propagated on the related targets.

15.9. Trigger secret rotation for all target accounts using a same password change policy (CLI)



Important:

Before launching the rotation using the command line, ensure that **Change periodicity** is specified for the password change policy related to the domain of the target account. For more information, refer to [Add a password change policy \(on page 210\)](#).

With `root` privileges, it is possible to trigger a secret rotation for all the target accounts whose domain uses a specific password change policy. You can do so by running the following command line and replacing `<POLICY_NAME>` with the applicable value.

```
sudo -u wabuser /opt/wab/bin/WABChangeAccountCred <POLICY_NAME>
```

15.10. "Break Glass" mechanism

What is the "Break Glass" mechanism?

WALLIX Bastion can administer credential updates for targets, rendering credentials unknown to users. However, this might present problems if an issue arises and the history of credentials updates is absent. For instance, if WALLIX Bastion is unavailable or if you need to retrieve previous passwords after restoring a backup file. As a result, WALLIX Bastion offers a "break glass" feature that allows a user to obtain credentials for the target groups gathered in the Bastion. Credentials includes the login, common name (cn), passwords, and SSH keys.

There are two versions of the mechanism available:

- The standard mechanism, which sends an encrypted archive by e-mail.
- The alternative mechanism, which stores the credentials in a directory or a remote storage.



Notice:

The alternative mechanism is available from the WALLIX Support team upon request.

15.10.1. Standard "Break Glass" mechanism

About this task

With the standard "Break Glass" mechanism, WALLIX Bastion sends an e-mail to designated users for both events:

- Automatically, every night at 2:34 a.m. in the time zone of WALLIX Bastion. Users receive an encrypted e-mail containing the list of all the credentials gathered for target groups, depending on the scope of the limitations set for their profile.
- When a target account is automatically or manually modified, depending on the password change and checkout policies linked to the account. For more information, refer to



[Automatically trigger secret rotation for one or more target accounts \(with auto-generated secrets\) \(on page 245\)](#) and [Manually trigger secret rotation for a target account \(with user-generated secrets\) \(on page 244\)](#).

Notifications about successive credential changes at check-in and notifications that were not received due to network issues are compiled and e-mailed within 15 minutes.

Procedure

1. Create a user profile with the **Credential recovery** feature right set to **Execute**, or ensure that one exists.
2. Apply this profile to all users that must receive the credential updates e-mails.
3. Ensure that all relevant users have a GPG key defined.
 - As a full privilege administrator, from **Users > Accounts**, you can edit each relevant user account, add a GPG key, and apply the modification to their user account.
 - As a user, from the **My preferences > GPG key** tab, you can upload the GPG key and apply the modifications to your profile.
4. Ensure that automatic credential updates are correctly set up.
 - For a checkout policy, linked accounts must have the **Automatic password change** or **Automatic SSH key change** or both options activated.
 - For a domain, the **Enable password change** must be activated with an administrator account defined and a password change policy or password change plugin configured.

Results

The standard "Break Glass" mechanism is up and running.

The e-mail containing the list of all credentials can be decrypted using a PGP-compatible tool. You must decrypt the attachment separately and then to use a tool compatible with the CSV or JSON format, when the attached file contains an extension of this type.



Trouble:

GPG keys have an expiry date. If users no longer receive e-mails, they must check that their key is not expired.

What to do next

If you must remove a user from the list of recipients, you must change their profile. Administrators also have the ability to forcibly remove GPG keys, however this is not advised because users can add GPG keys again.

15.10.2. Alternative "Break Glass" mechanism

About this task



Notice:

The alternative mechanism is available from the WALLIX Support team upon request.

The alternative "Break Glass" mechanism sends a list of passwords stored in the Bastion Vault to the remote storage daily, eliminating the need for the e-mail subsystem. Like for the standard mechanism, files containing passwords are encrypted in GPG. The alternative "Break Glass" mechanism can also send a file with only the password for an account for which a password is changed in real-time.

16. Sessions configuration



Important:

All the IP addresses which can be set on WALLIX Bastion support both IPv4 and IPv6 formats.

16.1. Restrict sessions use



Note:

In the context of an RDP session, you can enable the **Allow rt without recording** option accessible from **Configuration > Configuration options > RDP proxy > audit** section to view the current RDP session for which the session recording option has not been enabled in the authorization defined for the user group and the target group.

By enabling the **Enable osd 4 eyes** option accessible from **Configuration > Configuration options > RDP proxy > client** section, a message is displayed to the user to inform them that the session is being audited as soon as the auditor starts viewing the RDP session in real-time.

16.1.1. User authorizations on sessions

From the **Sessions** page in the **My authorizations** menu, the user can view the list of targets to which they are authorized to access.

The display of icons, and consequently the access to the file to establish a connection, depends on the parameters set for the connection and file types related to RDP and SSH according to the operating system via **Configuration > Configuration options > GUI (Legacy)**, in the following fields: **Rdp connection links** and **Ssh connection links**.

The icons are also displayed if the required subprotocol is authorized in the authorization but also in the service of the device for SSH-type protocols.

When the authorization concerns a Universal Tunneling service, only the WALLIX-PuTTY application allows the user to download or open the file to establish the connection (filename suffix `.puttywab`).



Note:

In a load balancing process, it is possible to specify the WALLIX Bastion's FQDN or IP address to which the user is redirected to when accessing a target via **Configuration > Configuration options > GUI (Legacy)**:

- in the field **Connection file fqdn standard**: when the target is accessed by downloading the configuration file
- in the field **Connection file fqdn otp**: when the target is instantly accessed with one-time password method.



16.1.1.1. Restrict SSH session files

The downloadable file type on Windows platforms for SSH sessions can be selected from **Configuration > Configuration options > GUI (Legacy)**, then select the appropriate value in **Ssh windows filetype**.

To use the .puttywab files on Windows, the WALLIX-PuTTY application has to be downloaded and installed by clicking the **WALLIX-PuTTY** button displayed in the **My authorizations** tab in the **My preferences** page. This button is only displayed when the workstation is running under Windows and when the user is authorized to connect to at least one SSH target. 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.

16.1.1.2. Specific options for RDP sessions

The **RDP configuration file** button displayed in the **My authorizations** tab in the **My preferences** page is used to download an RDP configuration file. The user can then save the file to establish a connection to an application in interactive mode via the RDP client selector. This button is only displayed when the user is authorized to connect to at least one application.

The RemoteApp mode is enabled by default when accessing applications (as defined via **Targets > Applications**). This parameter can be enabled or disabled via the **Rdp remote app mode** option located in **Configuration > Configuration options > GUI (Legacy)**. For more information on RemoteApp mode, refer to [Configure the application launch using RemoteApp mode \(on page 124\)](#).



Attention:

The RemoteApp sessions of a user connected simultaneously on one or several applications are split by default when displayed from the **Current sessions** and **Session history** pages under the **Audit** menu). If the **Rdp enable sessions split** option (accessible from **Configuration > Configuration options > GUI (Legacy)** under the **main** section) is deselected, it may be possible to get an overlay view of these sessions.

The client Remote Desktop Connection (MSTSC) connected to Windows Server 2008 or 2012 does not allow several RemoteApp programs to share the same RDP session. There will be as many RDP sessions created as the number of RemoteApp programs launched.

Display issues related to the Microsoft client were reported when using RemoteApp mode and multiple monitors. Dysfunctions occur when the primary monitor is not located in the upper left part of the virtual screen. The recommended workaround is to locate the primary monitor in the upper left part of the virtual screen. For more information on virtual screens, refer to the [official Microsoft documentation](#).

On the other hand, to allow glyphs support between iOS client and the RDP proxy and thus display text properly on the selector when accessing sessions from mobile devices, the **Bogus ios glyph support level** option is selected by default. This parameter can be managed via **Configuration > Configuration options > RDP proxy** under the **client** section.

Moreover, as the support of Unicode character set for keyboard event is necessary to operate the Remote Desktop Connection client under iOS, the **Unicode keyboard event support** option is selected by default. This parameter can be managed via **Configuration > Configuration options > RDP proxy** under the **globals** section.

As the keyboard behavior for VNC sessions depends on the target server environment, options allow to declare this environment and allow the corresponding behavior. These options can be managed



under the **vnc** section on the configuration page related to the connection policy for the VNC protocol. This page can be accessed from **Session management > Connection policies**:

- when the **Server unix alt** option is selected
 - on a Unix environment, the target server can receive any Unicode character sent by the client
 - on a Windows environment, the target server forbids any Unicode character but allows special characters using AltGr+€ key combination
- the **Server is macos** option must only be selected to support the keyboard specificities related to old versions of Apple Mac OS VNC servers. The French PC keyboard (FR) is supported for the connection to a VNC target on a Macintosh environment if this keyboard is installed and selected on the target server.

16.1.2. External ticketing system script for approval workflow

A script can be called to manage approvals in an external ticketing system when the approval request is created, and also at the beginning and end of each session in the request duration period.

This script must be loaded into the `/usr/local/bin` directory (empty by default on WALLIX Bastion) for which the **wabuser** user has the right to run this script. To load a file into this directory, the user must be connected with **root** privileges.

To use the script, the access path must be entered from the **Configuration > Configuration options > Global** page in the **Ticketing interface path** field.

The script is then called systematically, even if a no ticket number is specified in the **Ticket** field. When the script writes on the standard output a ticket number (expected in the `ticket=1234` format), WALLIX Bastion takes into account this number and not the one specified in the **Ticket** field.

Specificity for secrets

When a password change is in progress, it is not possible to check out secrets and display the credentials of the relevant account. In this case, an error message is displayed notifying the user that the account is temporarily unavailable for the 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. For more information, refer to [Checkout policies \(on page 183\)](#).

The **Check out remotely** option is performed as a standard checkout. As a result, the user does not know whether the secret is local to the Bastion or comes from an external vault.

Specificity for sessions

When this script is called, it receives as a parameter the path to a file providing all the session information.

Example of information provided in the file during the approval request creation:

```
[request]
user=johndoe
target=target1@local@repo:SSH
date=2017-09-22 10:12:19
duration=300
ticket=1234
comment=I have to install patches
session_id=
session_start=0
```



```
session_end=0  
target_host=
```

Example of information provided in the file at the beginning of the session:

```
[request]  
user=johndoe  
target=target1@local@repo:SSH  
date=2017-09-22 10:12:00  
duration=300  
ticket=1234  
comment=I have to install patches  
session_id=15ea8a529008635d5254006c3e07  
session_start=2017-09-22 10:12:29  
session_end=0  
target_host=host1.mydomain.lan
```

Example of information provided in the file at the end of the session:

```
[request]  
user=johndoe  
target=target1@local@repo:SSH  
date=2017-09-22 10:12:00  
duration=300  
ticket=1234  
comment=I have to install patches  
session_id=15ea8a529008635d5254006c3e07  
session_start=2017-09-22 10:12:30  
session_end=2017-09-22 10:12:34  
target_host=host1.mydomain.lan
```

16.1.3. Time frames for target access

The periods during which a user can connect to targets are determined by the time frames defined in WALLIX Bastion.

A time frame is linked to one or more user groups. For more information, refer to [User groups \(on page 43\)](#).



Attention:

A default time frame called `allthetime` is configured in WALLIX Bastion. It allows users to connect to targets on any day and at any time. This time frame cannot be deleted.

The time reference used is the local time of WALLIX Bastion.

16.1.3.1. Add a time frame

Procedure

1. Go to the **Configuration > Time frames** page.
2. Click  **Add**.
3. Give the time frame a name and an optional description.
4. Choose if you want to disable the automatic disconnection at the end of the time period.
5. Add one or more time periods.



- **Weekly schedule:** configure a time period and define the times and days of the week during which users can connect to targets during the defined period.
 - **Date range:** configure the start date, end date, and times of the period during which users can connect to targets without interruption.
6. Click **Apply**.

16.1.3.2. Edit a time frame

Procedure

1. Go to the **Configuration > Time frames** page.
2. Click the name of the time frame that you want to edit.
3. Edit the necessary information.
4. Click **Apply**.

16.1.3.3. Delete a time frame

About this task



Attention:

You cannot delete a time frame linked to a user group.

Procedure

1. Go to the **Configuration > Time frames** page.
2. Select the time frames that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected time frames.

16.1.4. RDP options

The following options, which mainly determine the authorized actions for the session, are provided for the RDP protocol:

Option	Definition
RDP_AUDIO_INPUT	allows audio recording from the client to the RDP session
RDP_AUDIO_OUTPUT	allows audio playback from the session to the RDP client
RDP_CLIPBOARD_DOWN	allows data transfer using the clipboard from the session to the RDP client
RDP_CLIPBOARD_UP	allows data transfer using the clipboard from the client to the RDP session
RDP_CLIPBOARD_FILE	allows file transfer from the copy/paste function using the clipboard RDP_CLIPBOARD_FILE must be associated with RDP_CLIPBOARD_UP to transfer a file using the clipboard from the client to the RDP session RDP_CLIPBOARD_FILE must be associated with RDP_CLIPBOARD_DOWN to transfer a file using the clipboard from the session to the RDP client



Option	Definition
RDP_COM_PORT	allows use of local serial and parallel ports in the remote session
RDP_DRIVE	allows use of local drives in the remote session
RDP_PRINTER	allows use of local printers in the remote session
RDP_SMARTCARD	allows use of local smartcards in the remote session

Each of these subprotocols is covered by a specific authorization on WALLIX Bastion.

If you do not have rights for the appropriate subprotocol, you are not authorized to transfer data using the clipboard or use your local drive in the remote session.

16.1.5. Restrictions for RDP pattern detection

What is a Restriction?

You can define *restrictions* in the configuration user groups or target groups. A restriction is an action which applies when certain character sequences are detected in:

- RDP keyboard flows (the data analyzed is the data entered by the user)
- the window title bars (the data analyzed is the data displayed on the screen)



Attention:

Character sequence detection is only enabled for data sent by the client to the server.

To add a restriction, from the user group or target group configuration, click the **Restrictions** tab then click  **Add** to display the dedicated creation window. The relevant actions must be selected in the **Action** field and the corresponding rules must be defined in the **Rules** field.

Types of restrictions

There are two types of actions that can be defined for a restriction:

- **Kill** causes the session disconnection
- **Notify** sends a notification

Rules

The list of patterns applied is the sum of those present in the user groups and the target groups. The linked action is the most restrictive: if the **Kill** action is in one of the groups, then this action is selected.

The rules must be entered as regular expressions, with one expression per line. The pattern detection is case-sensitive.



Expression prefix	Match
\$kbd:	Only matches keyboard input.
\$ocr: or no prefix	Only matches the title bars of active windows (and not those of the inactive windows).
\$kbd-ocr: Or \$ocr-kbd:	Matches keyboard input and title bars of active windows.

Examples

To ensure files are not deleted from the command prompt (cmd.exe), the expressions you can provide are the following:

```
$kbd:del\s+.*
$kbd:erase\s+.*
```

To forbid opening the command prompt itself:

```
$ocr:Command Prompt
$ocr:.*\cmd.exe
```

The following prefixes provide basic string searching:

- \$content: searches for a string
- \$exact-content: searches for an entire string. It becomes content: when it is used with \$kbd:.
- \$regex: searches for a regular expression. This is the default behavior.
- \$exact-regex: searches for a regular expression formed with ^pattern\$

The supported separator characters are - and ,.

For example: \$content,ocr:abc.exe matches all windows containing abc.exe. , is not considered as a regular expression character. - is the separator character for \$ocr: and \$kbd:.



Attention:

If you choose to kill the session when a specific window title bar is displayed, users will not be able to reconnect until this window is closed or its title changed because their sessions will be killed again immediately.

16.1.6. SSH options

The following options, which mainly determine the channels authorized for the session, are provided for the SSH protocol:

Option	Definition
SFTP_SESSION	bi-directional transfers files via SFTP protocol (SFTP session)



Option	Definition
SSH_AUTH_AGENT	allows agent authentication forwarding (multi-hops auth-agent) SSH_AUTH_AGENT must be associated with SSH_SHELL_SESSION or SSH_REMOTE_COMMAND (at least one of the two)
SSH_DIRECT_TCPIP	allows direct TCP/IP port forwarding (from client to server)
SSH_DIRECT_UNIXSOCK	allows direct Unix socket forwarding (from client to server)
SSH_REMOTE_COMMAND	runs remote commands
SSH_REVERSE_TCPIP	allows reverse TCP/IP port forwarding (from server to client) SSH_REVERSE_TCPIP must be associated with SSH_SHELL_SESSION
SSH_REVERSE_UNIXSOCK	allows reverse Unix socket forwarding (from server to client) SSH_REVERSE_UNIXSOCK must be associated with SSH_SHELL_SESSION
SSH_SCP_DOWN	transfers files from a target device (SCP download from server to client)
SSH_SCP_UP	transfers files to a target device (SCP upload from client to server)
SSH_SHELL_SESSION	starts a shell session
SSH_X11	displays X11 applications running on a target device SSH_X11 must be associated with SSH_SHELL_SESSION or SSH_REMOTE_COMMAND (at least one of the two)

Each of these subprotocols is covered by a specific authorization on WALLIX Bastion.

If you do not have rights for the appropriate subprotocol, you are not authorized to start a remote shell session or transfer a file.



Important:

For SCP security reasons, do not use SSH_SCP_UP or SSH_SCP_DOWN subprotocols without SSH_SHELL_SESSION (refer to CVE-2020-15778 for additional information). As an alternative, you can also use SFTP_SESSION.



Note:

Some clients also need the `SSH_SHELL_SESSION` option to list the directories when they are used in SCP mode.

`SSH_SHELL_SESSION`, `SSH_REMOTE_COMMAND`, `SSH_SCP_UP`, `SSH_SCP_DOWN`, and `SFTP_SESSION` allow the opening of session channels. By default, only one session channel can be open during an SSH connection (or session). Only the administrator can allow the opening of several session channels.

16.1.7. Restrictions for SSH pattern detection

What is a Restriction?

You can define *restrictions* in the configuration user groups or target groups. A restriction is an action which applies when certain character sequences are detected in the upward flow from SSH proxy. The data analyzed is the data entered by the user.



Attention:

Character sequence detection is only enabled for data sent by the client to the server.

To add a restriction, from the user group or target group configuration, click the **Restrictions** tab then click **Add** to display the dedicated creation window. The relevant actions must be selected in the **Action** field and the corresponding rules must be defined in the **Rules** field.

Types of restrictions

There are two types of actions that can be defined for a restriction:

- **Kill** causes the session disconnection
- **Notify** sends a notification

Rules



Note:

A set of allowed commands can be defined as regular expressions for remote command execution for subprotocol `SSH_REMOTE_COMMAND`. For more information, refer to [Patterns of allowed commands for subprotocol SSH_REMOTE_COMMAND \(on page 259\)](#).

The list of patterns applied is the sum of those present in the user groups and the target groups. The linked action is the most restrictive. If the **Kill** action is in one of the groups, this action is selected.

The rules must be entered as regular expressions, with one expression per line. Additionally, pattern detection is case-sensitive.

For example, to prevent files from being deleted, the expressions you can provide are the following:

```
unlink\s+.*
rm\s+.*
```



16.1.7.1. Warning for Kill actions

By default, the **Kill** action disconnects the session at first detection. However, it is possible to define a detection count with blocking and warning before the session disconnection. This can be done in **Configuration > Configuration options > SSH proxy** by entering a positive integer in the **Warning count** field. This value is 0 by default.

For example, if the value is 5, the user is warned five times upon detection (while preventing execution of the command) before disconnecting the session at the sixth detection.



Attention:

By default, the keyboard inputs not displayed on the terminal (for example, passwords) are not logged in WALLIX Bastion, unless the option **Log all kbd** is enabled on the configuration page for the related connection policy. However, a malicious user can force the display permanently during the session using the following command:

```
stty -echo
```

In such a case, the session can then be disconnected by defining the following **Kill** rule in the **Restrictions** tab of the **Groups** page:

16.1.7.2. File transfers and data download

For subprotocols `SFTP_SESSION`, `SSH_SCP_UP`, and `SSH_SCP_DOWN`, it is possible to set a pattern based on the file size to detect transfer of large files. The syntax is as follows: `$filesize:>X` where `X` is the size expressed in bytes.

For subprotocols `SSH_SHELL_SESSION`, `SSH_REMOTE_COMMAND`, `TELNET`, and `RLOGIN`, it is possible to set a pattern based on the definition of a limit for downloading data from the server to the client's desktop. The syntax is as follows: `$downsize:>X` where `X` is the maximum data amount size expressed in bytes.

In both case, a trailing letter (such as `m`, `k`, `g`) can be specified to provide a scaling factor as described in the following table:

Table 6. Scaling factor

Letter	Scaling factor
k	1 000
m	1 000 000
g	1 000 000 000
K	1024 (2^{10})
M	1 048 576 (2^{20})
G	1 073 741 824 (2^{30})



16.1.7.3. Detections of Cisco IOS commands

Cisco routers under IOS are restrictive for command inputs, but support auto completion and partial input when command prefixes are unambiguous. As a result, it is necessary to use a specific extension of the rules syntax to ban or allow certain commands in the most exhaustive way on such a system.



Attention:

A target having this type of detection rules is considered as a Cisco IOS device. Do not use it for another kind of device such as Linux/Unix or you risk a malfunction.

This syntax extension can be used with subprotocols SSH_SHELL_SESSION, RLOGIN or TELNET (according to the kind of connection), for any kind of action.

Two modes are available:

- White list of commands: only the listed commands are allowed. The syntax to use in the **Rules** field is as follows: `$acmd:[command list]`
- Black list of commands: any commands are allowed except those in the list. The syntax to use in the **Rules** field is as follows: `$cmd:[command list]`

The command list is delimited by square brackets, each command being separated by a comma. For example: `[enable, show kerberos, access-template, configure terminal]`

A command can contain a `:` separator to indicate the end of the unambiguous prefix. The command itself must not contain any `:` character. For example for the commands "enable", "show kerberos", "access-template", and "configure terminal" the list would be: `[en:able, sh:ow kerb:eros, access-t:emplate, conf:igure t:erminal]`

Example of white list:

```
$acmd:[en:able, sh:ow kerb:eros, access-t:emplate, conf:igure t:erminal]
$acmd:[sh:ow]
```

Example of black list:

```
$cmd:[en:able, sh:ow]
```

In case of multiple declarations, all lists of the same kind are merged.

If both white and black lists are declared together, detection will be done from the white list where commands from the black list have been removed.

By default, implicitly, the commands `alias` and `prompt` are added to a black list and the command `exit` is added to a white list.

Example of detection using the white list: `[w:here, sh:ow ke:rberos, co:nnect]`.

Table 7. Cisco IOS Detection with white list

Input	Detection
show	Yes
show kerb	No
sh ke c	No

Table 7. Cisco IOS Detection with white list (continued)

Input	Detection
show kron schedule	Yes
show ip arp	Yes
config t	Yes
where	No
w	No
alias show display	Yes
exit	No

Example of detection using the black list: [w:here, show ke:rberos, co:nnect]

Table 8. Cisco IOS Detection with black list

Input	Detection
show	No
show kerb	Yes
sh ke c	Yes
show kron schedule	No
show ip arp	No
config t	No
where	Yes
w	Yes
alias show display	Yes
exit	No

16.1.7.4. Patterns of allowed commands for subprotocol SSH_REMOTE_COMMAND

A set of allowed commands can be defined as regular expressions for remote command execution. A command mismatch will then be detected.

The syntax is as follows: \$allow:<re_1>.

Commands matching the regular expression <re_1> are allowed. The others are detected.

If several expressions prefixed with allow are defined, a command matching one of them is allowed.

The following sequence:

```
$allow:<re_1>
$allow:<re_2>
...
$allow:<re_n>
```

can also be specified as follows:

```
$allow:<re_1> |<re_2>| ... |<re_n>
```



Rules defined as standard regular expressions are also checked. As a result, a rule defined as an allowed regular expression and a standard regular expression is detected and the corresponding action is performed.

Example of detection for rule: \$allow:abc

Table 9. Commands

Input	Detection
abc	No
cde	Yes

Examples of detection for rules:

```
$allow:abc  
$allow:ps.*
```

Table 10. Commands

Input	Detection
abc	No
cde	Yes
ps aux	No
ps aux grep eggs	No
ls	Yes

Examples of detection for rules:

```
$allow:abc  
$allow:ps.*  
ps.*\|
```

Table 11. Commands

Input	Detection
abc	No
cde	Yes
ps aux	No
ps aux grep eggs	Yes
ls	Yes

16.1.8. Import restrictions for target groups and user groups

About this task



Important:

The update of existing data when importing a .csv file overwrites old data.



It is possible to import the restrictions defined during the creation or modification of user groups or target groups. These restrictions define the actions to apply when certain character sequences are detected in the upward flow from proxies (refer to [Restrictions for SSH pattern detection \(on page 256\)](#) and [Restrictions for RDP pattern detection \(on page 253\)](#)).

The CSV file must begin with a line containing the #wab1040 restriction tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(equired) O(ptional)	Possible values
Group name	Text	R	[aA-zZ], [0-9], '-', '_' There can only be a single group name
Group type	Text	R	Target / User
Restriction action	Text	R	"Kill" / "Notify"
Restriction rule	Text	R	Regular expressions, with one expression per line There can be rules on both user groups and target groups on the same file
Restriction sub-protocol	Text	R	Name of the subprotocol



CAUTION:

A user is allowed to export restrictions if at least the **View** right for the **Targets & accounts** feature is set in their profile (refer to [Permission profiles \(on page 22\)](#)).

If only the **View** right for the **Targets & accounts** feature is set in the profile, the user can export restrictions on target groups only.

If the **View** right for the **Users** feature is also set in the profile, then the user is able to export the restrictions defined on the user groups they are allowed to view (depending on the limitations set for the profile. For more information, refer to [Permission profiles \(on page 22\)](#)).

If only the **View** right for the **Users** feature is set in the profile, the user cannot export any restriction.

Procedure

1. Go to the **Import/Export > CSV** page.
2. Select the **Field separator** from the dropdown list.
3. Select the **List separator** from the dropdown list.
4. Select **Restrictions** from the **Data** options.



5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

16.2. Session invite



Restriction:

The Session Invite feature is compatible with Access Manager 5 and above.

What is Session invite?

The Session invite feature allows a privileged user (the host) to share their current session with an external user (the guest). The guest is a user who does not have an associated user account in WALLIX Access Manager or WALLIX Bastion. Session invite can only be performed through WALLIX Access Manager and is supported by RDP and VNC sessions. Only one external user can be invited to join a current session.



Important:

The Session invite feature is not supported by the WALLIX One PAM SaaS offer.

Session invite is not available for SSH sessions and application targets.

Session sharing and remote control of an RDP session is not supported in the host's and guest's sessions.

Workflow

The right to invite an external user to a session is granted by an administrator of WALLIX Bastion in an authorization (for more information on authorizations, refer to [Authorizations \(on page 189\)](#)).

When the host is connected to a session through WALLIX Access Manager, they can invite their guest and generate an invitation link. The host must share this link with their guest. It is up to both users to find the best way to communicate during the shared session.

By copying the invitation link in a browser, the guest joins the session through WALLIX Access Manager. They do not need to authenticate to the shared session. Indeed, the link provided by the host is sufficient to access the session and thus allows the host to invite a person to join their session without having to register them and manage their rights in WALLIX Bastion.



Attention:

A guest is an unknown user in WALLIX Bastion. Any malicious action by a guest in a sensitive session is the responsibility of the administrator who set the **Session invite** option in the authorization and the host who shared the invitation link.

An invitation is:



- pending until the guest joins the session
- ongoing when the host and guest share the session
- expired when one of the following conditions is met:
 - the expiration date of the invitation link is reached
 - the host cancels the sharing
 - the host terminates the session
 - the invitation link was used by the guest and they have left the session

The host can cancel the sharing when the invitation is pending to make the invitation link invalid and when the shared session is ongoing, which disconnects the guest.

The guest's session is linked to the session of the host. That means when the host closes their session or when their session is closed due to a timeout, the guest's session is automatically closed. No timeout can be configured for the guest's session.

All events occurring during the shared session between the host and their guest are logged under the host's session ID (the guest will be a temporary user with a unique ID) and the session control owner is listed for each event. These logs can be exported to an external SIEM where all metadata is associated with the host session. New fields specific to the Session invite feature were added:

- `[control_owner]`: the identifier of the user controlling the session ("`[HOST-NAME]`" or "`[GUEST-NAME]`")
- `[mode]`: the type of the shared session ("`view-only`" or "`view-control`")

When recording an RDP session, both guest and host sessions are recorded.

16.2.1. Customize expiry for session invite

About this task

For security reasons, the invitation link has an expiration date and time. You can adjust this expiry delay to fit your requirements.

Procedure

1. Go to the **Configuration > Configuration options > Global** page.
2. Under the **[main]** section, set a value for **Session Invite request timeout**.

This value defines maximum amount of time during which the guest is allowed to join the host's session. When this time is reached, the invitation link to join the current session expires.

By default, this option is set to 600 seconds.

3. Click **Apply**.

16.3. Transparent mode configuration for RDP and SSH proxies

What is Transparent mode?

The transparent mode allows the proxy to intercept network traffic for a target even when the user specifies the target's address directly, instead of using the WALLIX Bastion address.

Workflow

To use the transparent mode, the network must be configured in a way that the RDP or SSH traffic going to the targets is first redirected to a WALLIX Bastion user network interface. It can be achieved using routing rules. WALLIX Bastion then acts as a gateway. The proxy intercepts the traffic sent to the TCP port 3389 (for RDP and VNC protocols). Any traffic not destined to WALLIX Bastion but



intercepted by the WALLIX Bastion on any other port (other than 3389) is lost. The proxy picks up automatically the target by looking at the destination IP address of the connection. When only a single target is identified by the address, the connection is performed automatically without the display of the selector. In the other cases, the selector displays the list of targets matching this address.

Configuration

This mode can be enabled from **Configuration > Configuration Options**:

- on the **RDP proxy** configuration page by selecting **Enable transparent mode** under the **[globals]** section
- on the **SSH proxy** configuration page by selecting **Enable transparent mode** under the **[main]** section

It is also possible to define a set of targets belonging to a subnet. This is achieved by entering a subnet instead of an IP address in the "**Device host**" field during the creation of the device, from the "**Devices**" page, by using a CIDR notation (`<network address>/<number of mask bits>`). For more information on this configuration, refer to [Create a new device \(on page 110\)](#).

If the destination IP address of the connection corresponds to several targets and at least of one of these is defined by an IP address (or FQDN), then the targets defined by subnets are ignored. When only a single target is identified by the address, the connection is performed automatically without the display of the selector.

Once the RDP or SSH transparent mode is enabled, the following parameters can be set to control the proxy behavior:

- The option "**Auth mode passthrough**" (accessible from **Configuration > Configuration Options > SSH proxy** for SSH or **Configuration > Configuration Options > RDP proxy sesman** for RDP) enables or disables authentication delegation. The latter prevents WALLIX Bastion from performing the authentication when it receives a connection request. The request is then forwarded directly to the target and WALLIX Bastion authorizes the connection if the authentication by the target is successful. It allows to deploy WALLIX Bastion in an environment where only the target knows the credentials. This is the case for some configurations of VMware Horizon View for instance.
- The **Default login** field (accessible from **Configuration > Configuration Options > SSH proxy** for SSH or **Configuration > Configuration Options > RDP proxy sesman** for RDP) allows to specify WALLIX Bastion user different from the RDP or SSH identity. In this case, the sessions and their records will be associated to this WALLIX Bastion user. The RDP or SSH identity information is registered in the target field when available.

16.4. KeepAlive function for the proxies

The KeepAlive function allows to keep a session open even if there is no network traffic between WALLIX Bastion and the client or the target server. A message is then sent by WALLIX Bastion to the client or the target server to keep the connection between them.

16.4.1. Enabling KeepAlive function for connection between the RDP proxy and the RDP client

About this task

This function is enabled when the time interval between two KeepAlive messages is set.

**Attention:**

Modify the KeepAlive function only when instructed by the WALLIX support team.

Procedure

1. Go to **Configuration > Configuration options** and click **RDP proxy**.
2. Under the **[globals]** section, for **RDP keepalive connection interval**, define the interval between two KeepAlive messages.

The value is expressed in milliseconds. By default, it is set to 0 which disables the functionality.

3. Click **Apply**.

16.4.2. Enabling KeepAlive function for connection between the SSH proxy and the SSH client

About this task

This function is enabled when the time interval between two KeepAlive messages is set.

**Attention:**

Modify the KeepAlive function only when instructed by the WALLIX support team.

Procedure

1. Go to **Configuration > Configuration options** and click **SSH proxy**.
2. Enable **Advanced options**.
3. Under the **[main]** section, for **Client keepalive**, define the interval between two KeepAlive messages.

The value is expressed in seconds. By default, it is set to 120 which means there is a 2 minutes interval between two KeepAlive messages.

4. Click **Apply**.

16.4.3. Enabling KeepAlive function for connection between the SSH proxy and the SSH target server

About this task**Attention:**

Modify the KeepAlive function only when instructed by the WALLIX support team.

Procedure

1. Go to **Session management > Connection policies**.
2. Click the name of the existing policy you want to update and click **Edit this connection policy**.
3. Enable **Advanced options**.
4. Under the **[session]** section, configure the following options:

- **Server keepalive type**: enable the sending of the KeepAlive message to the server and choose the packet type to send. By default, it is set to `none` which disables the functionality.
 - **Server keepalive interval**: enter the interval in seconds between two KeepAlive messages when the **Server keepalive type** option is enabled. By default, it is set to `0` which disables the functionality.
5. Click **Apply**.

16.5. Session probe mode with the WALLIX BestSafe agent



Note:

The interaction is supported from WALLIX BestSafe Enterprise version 4.0.0.

When the agent WALLIX BestSafe is deployed on a Windows target, it can interact with the session probe to improve its collection of session metadata.

Event logging

The session probe receives notifications of all events detected or generated by the WALLIX BestSafe agent deployed on Windows targets. These notifications are then transferred and logged to WALLIX Bastion through the session metadata and the SIEM messages.

Detection of outbound connections

The session probe automatically creates a monitoring rule from the WALLIX BestSafe agent to be notified of outbound connections. When a notification is received from the agent, the session probe responds according to the rules (**allow**, **deny**, or **notify**) set in the **Outbound connection monitoring rules** field.

The initial operation is always provided on Windows targets on which the WALLIX BestSafe agent is not deployed.

For more information about outbound connection detection, read [About outbound connection monitoring rules \(on page 145\)](#).

Detection of process launching

The session probe automatically creates a privilege rule from the WALLIX BestSafe agent to be notified when processes are launched. When a notification is received from the agent, the session probe responds according to the rules (**allow**, **deny**, or **notify**) set in the **Process monitoring rules** field.

The initial operation is always provided on Windows targets on which the WALLIX BestSafe agent is not deployed.

16.5.1. Enabling the interaction with the WALLIX BestSafe agent

About this task

The session probe is enabled by default on the configuration page related to the connection policy for the RDP protocol. By default, the interaction with the WALLIX BestSafe agent is disabled.

Procedure

1. Go to **Session management > Connection policies**.
2. Click **RDP** and click **Edit this connection policy**.



3. Enable **Advanced options**.
4. In the **session probe** section, activate **Enable bestsafe interaction**.
5. Click **Apply**.



17. Infrastructure strategy

17.1. Clusters

What are Clusters?

A cluster is a group of jump servers. The use of a cluster in place of a single device allows application load sharing and High-Availability. The jump server used to run an application is selected in two steps. WALLIX Bastion firstly sorts the servers, beginning with the one that has the fewest open sessions, and then tries to connect to each server until it succeeds.

17.1.1. Add a cluster

Procedure

1. Go to the **Targets > Clusters** page.
 2. Click **Add a cluster**.
 3. Give the new cluster a name and optionally add a description.
 4. Manage the targets in the cluster,
 - To add target accounts: double-click the name of a target account from the **Available target accounts** column to move it to the **Selected target accounts** column. You can also perform a multi-selection by clicking several target accounts from the **Available target accounts** column and clicking > to move them to the selection.
 - To remove target accounts: double-click the name of a target account from the **Selected target accounts** column to put it back in the **Available target accounts** column. You can also perform a multi-selection by clicking several target accounts from the **Selected target accounts** column and clicking < to remove them from the selection.
- You can search for a target account by name in the search field.
5. Click **Apply**.

17.1.2. Import clusters

About this task



Attention:

The update of existing data when importing a .csv file overwrites old data.

The CSV file must begin with a line containing the #wab1040 cluster tag. That first line must not be modified. If this line is modified, the file can no longer be imported into WALLIX Bastion. Each subsequent line must be formed as follows:

Field	Type	R(equired) O(ptional)	Possible values
Name	Text	R	[aA-zZ], [0-9], '-', '_'
Description	Text	O	Free text

Field	Type	R(equired) O(ptional)	Possible values
Targets	Text	R/O	Target accounts defined: at least one target account or one account mapping target or one interactive login target must be defined. There can be 0 target, one or several targets defined in each category, or one or several targets defined in all categories in the cluster.
Account mapping	Text	R/O	Account mapping targets defined: at least one target account or one account mapping target or one interactive login target must be defined. There can be 0 target, one or several targets defined in each category, or one or several targets defined in all categories in the cluster.
Interactive login	Text	R/O	Interactive login targets defined: at least one target account or one account mapping target or one interactive login target must be defined. There can be 0 target, one or several targets defined in each category, or one or several targets defined in all categories in the cluster.

Procedure

1. Go to the **Targets > Clusters** page.
2. Click **Import CSV file**.
3. Select the **Field separator** from the dropdown list.
4. Select the **List separator** from the dropdown list.
5. Retrieve the CSV file from your computer.
6. Click **Import**.

Results

After the .csv file is imported, a summary report is displayed. This report lists the number of elements which were created and updated in the WALLIX Bastion database, but also the rejected data. In case of rejection, the corresponding error is mentioned.

17.1.3. Edit a cluster

Procedure

1. Go to the **Targets > Clusters** page.
2. Click the name of the cluster that you want to edit.
3. Edit the necessary information.
4. Click **Apply**.

17.1.4. Delete clusters

Procedure

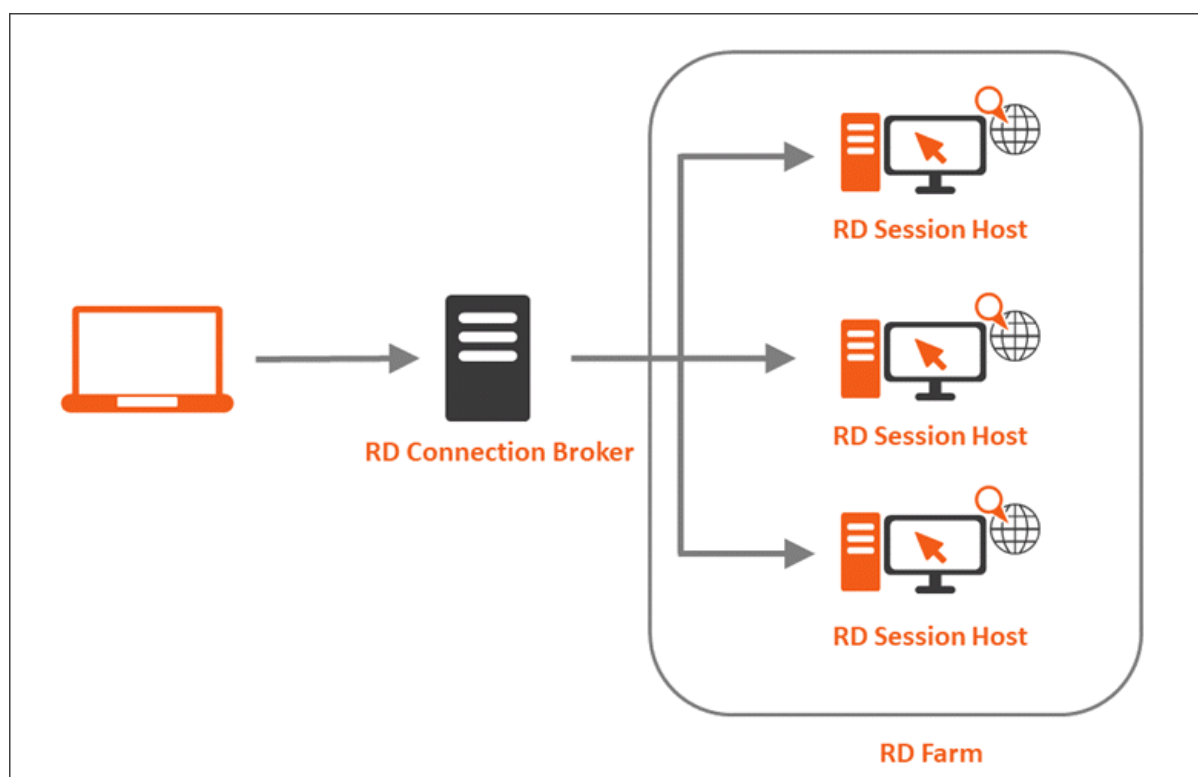
1. Go to the **Targets > Clusters** page.
2. Select the clusters that you want to delete.
3. Click **Delete**.
4. Confirm the permanent deletion all of the selected clusters.

17.2. Load balancing with Remote Desktop Connection Broker

Remote Desktop Connection Broker (RD Connection Broker) is a role service on Windows Server 2012 and 2016 operating systems providing the ability to:

- allow users to reconnect to their existing sessions in a load-balanced RD Session Host server farm
- enable you to evenly distribute the session load among RD Session Host servers in a load-balanced RD Session Host server farm
- provide users access to virtual desktops hosted on RD Virtualization Host servers and to RemoteApp programs hosted on RD Session Host servers through RemoteApp and Desktop Connection.

Load balancing



Prerequisites

WALLIX Bastion supports Remote Desktop Connection Broker with the following configuration:

- at least one server must have access to the role service RD Connection Broker
- at least one server must have access to the role service RD Licensing
- at least one server must have access to the role service RD Web Access



- role services RD Connection Broker, RD Licensing and RD Web Access can share the same server
- several servers must have access to the role service RD Session Host



CAUTION:

We recommend not installing the role service RD Session Host on a server having access to the role service RD Connection Broker.

RD Connection Broker cannot be used with a WALLIX Bastion cluster as a result of interferences between both services. We strongly recommend giving priority to RD Connection Broker in the context of load balancing.

It is not necessary to choose among Remote Desktop or RemoteApp collections when resources are accessed via the WALLIX Bastion web interface. Indeed, WALLIX Bastion uses RemoteApp collections for all connections.

RD Connection Broker must be set on RD Session Host servers. This can be performed locally (on each RD Session Host) with Local Group Policy Editor (gpedit.exe).

The values to edit are located on the following subfolders:

- Local Computer Policy
- Computer Configuration
- Administrative Templates
- Windows Components
- Remote Desktop Services
- Remote Desktop Session Host and
- RD Connection Broker

These values are as follows:

- Join RD Connection Broker
- Configure RD Connection Broker farm name
- Configure RD Connection Broker server name
- Use RD Connection Broker load balancing

Configuration

RD Connection Broker must be declared on WALLIX Bastion as a target. To reach directly RD Connection Broker (and not one of the RD Session Host), the field "**Load balance info**" must be specified at the level of the RDP connection policy, via **Session Management > Connection Policies**.

This field must be entered with the information retrieved from the **loadbalanceinfo:s:** field in the .rdp file saved from the Work Resources page on RD Web Access (`https://<ip-rd_web_access>/rdweb/`).

For example: `tsv://MS Terminal Services Plugin.1.Sessions.`

For more information on connection policies, refer to [Connection policies \(on page 134\)](#).

18. Universal Tunneling (RAW TCP/IP)

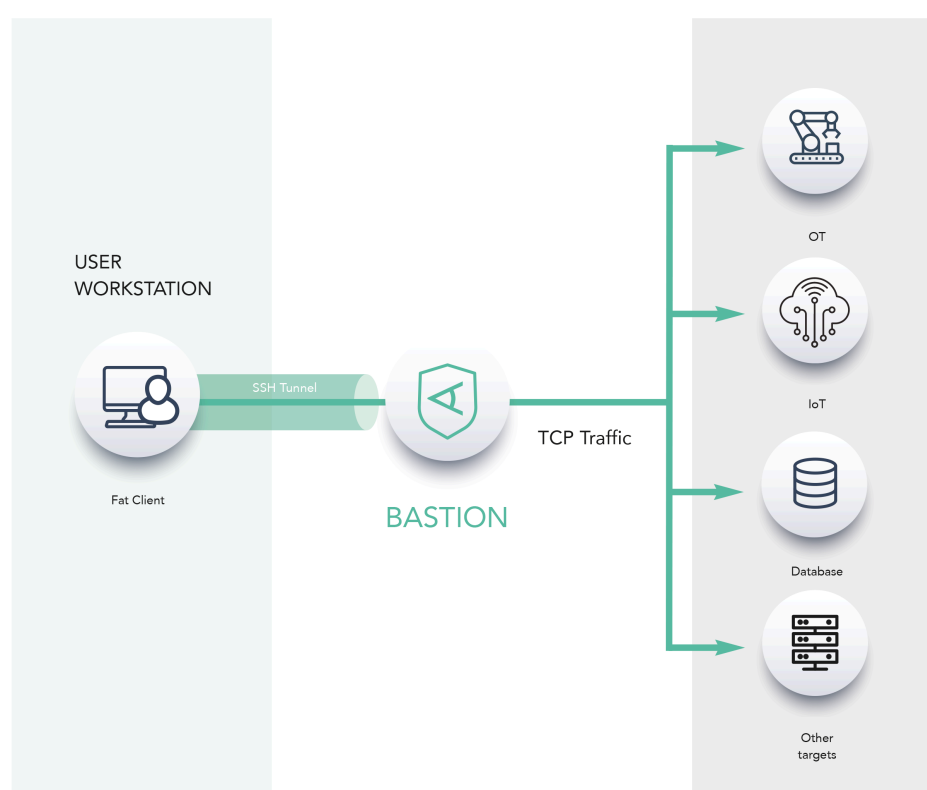
What is Universal Tunneling?

Universal Tunneling (or 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)

Universal Tunneling can manage all application protocols based on TCP for the transport layer in the Open Systems Interconnection model (OSI model). An SSH tunnel is used between the workstation of the user 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, Windows 11
- any Linux distribution with OpenSSH

The targets must have a port open on the network for a TCP-compatible protocol.



Auditing

The Universal Tunneling session can be recorded. The recording of a Universal Tunneling session consists of a PCAP file containing all the traffic exchanged between the user's client and the target through the session. This PCAP file can be analyzed with a packet analyzer such as Wireshark, a free and open-source tool.

To facilitate the analysis:

- the client address of each packet is filled in with the IP of the system from which the tunnel was established (the IP of the user's workstation, or the IP of the Access Manager in the case of a session initiated from WALLIX Access Manager)
- the remote address of each packet is filled in with the IP of the target or with the NAT IP of the configured option (refer to [Multi-tunneling \(on page 273\)](#)).

If the data transmitted above the TCP layer is encrypted between the user and the target, this data appears encrypted in the PCAP file.

18.1. Seamless connection

What is Seamless connection?

The Seamless connection option allows 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. To this end, a temporary network interface is created on the workstation of the user using the target's IP. Traffic sent over this interface is redirected to the SSH tunnel.

If the Seamless connection option is disabled, traffic is redirected to the local address: the user must define a local access port and configure the fat client to redirect traffic to the local address (127.0.0.1) on the local port defined. Traffic is redirected through the SSH tunnel. This mode does not require any specific privileges from the user.

Configuration



Attention:

The Seamless connection option is only available with user workstations running under Windows XP, Windows 7, Windows 8, Windows 10, and Windows 11.

This mode requires workstation the user to be in the "Network Configuration Operators" group. The use of WALLIX-PuTTY is required and is automatically activated when this option is enabled.

The Seamless connection option is located in **Targets > Devices**, for each RAW TCP/IP service associated with a device, in the **Services** tab.

18.2. Multi-tunneling

What is Multi-tunneling?

The Multi-tunneling option allows the user to access as many IPv4 network interfaces as configured by the WALLIX Bastion administrator in the RAW TCP/IP service in one session. Interfaces can differ by IP or port. As a result, they can belong to a single real device or to several real devices. The Multi-tunneling option can be used to manage up to 50 interfaces for RAW TCP/IP service.



In audit, all flow forwarded are assigned to the correct interfaces into the PCAP file. It is possible to determine the different flows by their corresponding IP address and destination port. Each interface can receive up to 100 kb/s of data in parallel with the other interfaces.

Configuration



Important:

Opening multiple Multi-tunneling sessions in parallel is not recommended.



Note:

WALLIX-PuTTY version 0.74.15 or later must be used to make Multi-tunneling sessions work properly.

The Multi-tunneling option is located in **Targets > Devices**, for each RAW TCP/IP service associated with a device, in the **Services** tab. The Multi-tunneling option automatically enables the **Seamless connection** option. For more information, refer to [Seamless connection \(on page 273\)](#).

18.3. NAT

About this task



Note:

The *Multi-tunneling* option is not compatible with Network Address Translation (NAT).

If the target is behind a NAT (Network Address Translation) solution, you must add a specific connection policy (for more information, refer to [Add a connection policy \(on page 134\)](#)) with the following configuration:

Procedure

1. Select **RAWTCPIP** in the **Protocol** field.
2. Enable and specify the fields in the **nat_redirection** section.



Note:

By enabling this option, the target address of each packet matches the IP address of the NAT in the PCAP file.

18.4. Configuration to access an IT or OT target

About this task

To allow a user to access an IT or OT target with a fat client, perform the following steps:



Procedure

1. Add a device with a RAW TCP/IP service whose port is the opened port on the target that is usually accessed by the fat client. For more information, refer to [Create a new device \(on page 110\)](#).

If the target is the MySQL database exposed on `192.168.0.1:3306` and accessible from a MySQL client, the IP address of the device is `192.168.0.1` and the port of the RAW TCP/IP service is `3306`.

If the target is a Siemens Programmable Logic Controller exposed on `192.168.0.1:102` and accessible from a Siemens Totally Integrated Automation Portal (TIA Portal), the IP address of the device is `192.168.0.1` and the port of the RAW TCP/IP service is `102`.

2. Add the new device to a target group for session management through interactive login. For more information, refer to [Create a target group \(on page 167\)](#).
3. Add a new authorization so that a user group can access the target group. For more information, refer to [Authorizations \(on page 189\)](#). Configure the authorization as follows:
 - a. Select **Sessions** in **Authorization mode**.
 - b. Select **RAWTCPIP** in **Protocols/Subprotocols**.
 - c. If the generation of a PCAP file is necessary, enable **Session recording**.
4. If the target is behind a NAT (Network Address Translation) solution, a specific connection policy must be configured. For more information, refer to [Multi-tunneling \(on page 273\)](#).

19. Monitor WALLIX Bastion activity

From the **Dashboards > Administration** page, it is possible to generate charts from statistical data defined on the **Connection data** tab, or to obtain a detailed view of the numerical data in the form of indicators on the **Connection indicators** tab.



Note:

The dashboard is only available in English.

The data viewable from this dashboard corresponds mostly to user connections to WALLIX Bastion (primary connections) and target connections (secondary connections).



Note:

Only users whose profile has **Administration** as a selected dashboard can view the **Dashboards > Administration > page**. By default, users with the default **product_administrator** or **operation_administrator** profile can access this menu entry. For more information on user profiles, refer to [Permission profiles \(on page 22\)](#).

Connection data

The **Connection data** tab allows the user to generate charts based on the data entered in the filter areas displayed at the top of the page:

- The **Time filter** area allows the user to define the period of time for which they want to view the data. By default, this period corresponds to the last 7 days and can be edited by clicking the **Last week** value under **Time range**. A window is then displayed: it is possible to select a predefined period on the **Defaults** tab or to define a date range or a number of days before the current date on the **Custom** tab. It is then necessary to click **OK** to generate the charts corresponding to this period.
- The **User group filter** area allows the user to restrict the display in the charts by selecting one or more user groups, according to the selected period of time.
- The **Target group filter** area allows the user to restrict the display in the charts by selecting one or more target groups, according to the selected period of time.

Each filter area displays an icon on the top right indicating the number of corresponding active filters. It is possible to click this icon to view the active filters under the **Applied filters** section in a dedicated window. This window can also display the unset filters under the **Unset filters** section. A click on each type of filters in these sections redirects to the corresponding filter area at the top of the page to edit and/or add one or more criteria.

When the relevant data is entered in the filter areas, a set of charts is displayed on the page and the following actions are possible:

- highlight the desired data by clicking the legend entry above the chart
- display the numerical data for a given day by hovering the mouse pointer over the chart
- edit the filters by clicking the icon on the top right of the chart.

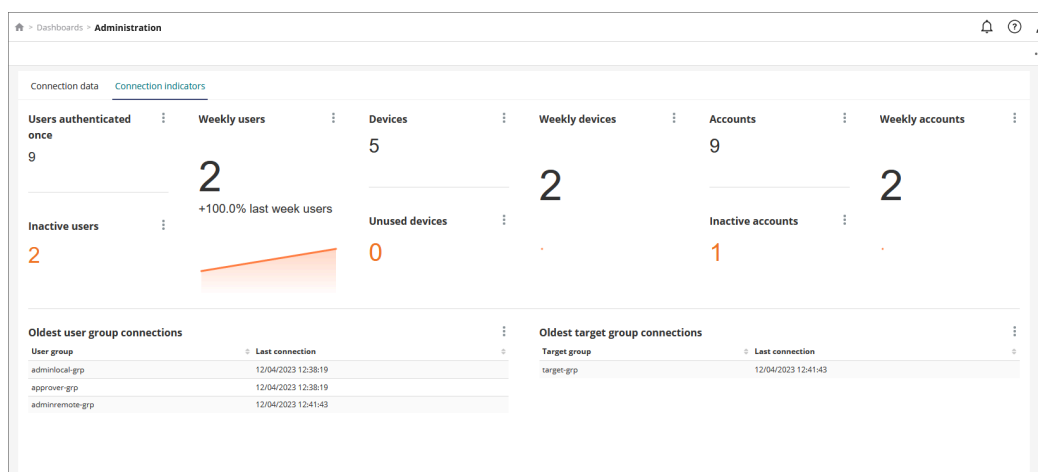


Connection indicators

The **Connection indicators** tab provides a view of the numerical data in the form of indicators, including:

- the number of users connected over the defined period, the number of devices and accounts declared and managed in WALLIX Bastion
- the number of users connected, devices and accounts used for sessions over the last 7 days compared to the previous week
- the number of users who were inactive for 180 days and the number of devices and accounts which were never used for sessions.

A tabular view presents also the oldest connections by user groups and by target account groups.



Data options

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

- Sort table values by ordering a column alphabetically or not ()
- View filters applied to the board ( 1)



- **Force refresh:** instantly refresh the data of the board. The time stamp of the last refresh is also indicated.
- **Enter fullscreen:** display the full screen view of the board. It is possible to return to the condensed view by clicking the “Minimize chart” icon.
- **Download as image:** download the data of the board as a JPG file.
- **Export to CSV:** download the data of the board as a CSV file.
- **Export to Excel:** download the data of the board as a XLSX file.



20. Annex

20.1. 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

A

- Active Directory
 - Authentication domain 55
 - Configuration 53
 - External authentication 53
 - Group mappings 56
 - Password reset 57
- Application Driver 132
 - browser extension 133
 - configuration
 - automatic deployment 130
 - manual deployment 132
 - parameter list 127
- Authentication
 - LDAP/AD users
 - Bind password 63
 - Kerberos Password 64
 - Kerberos Ticket 63
 - RADIUS 65
 - SSH Certificate 68
 - SSH Key 67
 - TACACS+ 66
 - X.509 Certificate 69
 - Local users
 - Password 85
 - PingID 90
 - RADIUS 88
 - SSH Key 87
 - TACACS+ 89
 - X.509 Certificate 87
 - protocols 48
- Authentication domain
 - AD 55
 - Deletion 99
 - Edition 98
 - Import 92
 - LDAP 59
 - OIDC 78
 - SAML 73, 76
- Authentication protocols
 - Local users 85
- Authorization
 - protocols 48

B

- Break Glass 209
 - alternative 247
 - mechanism 246
 - standard 246
- Browser extension
 - Application Driver 133

C

- CIDR

- notation 263

Communication

- Banner message 100
- Connection message 100
- Notification 105, 108, 108, 109
- Connection policies 134

D

- Dashboards
 - administration 276
- discovery 205, 205
- DNS 145

E

- Entra ID
 - Group mapping 77
- External authentication
 - AD 53
 - Add Kerberos Password authentication 64
 - Add Kerberos Ticket authentication 63
 - Add RADIUS authentication 65
 - Add TACACS+ authentication 66
 - Deletion 99
 - Edition 98
 - LDAP 58
 - OIDC 77
 - SAML 72, 75

G

- GPG Key
 - Deactivate notification 109
- Group mapping
 - Entra ID 77
- Group mappings
 - AD 56
 - Import 96
 - LDAP 61
 - OIDC 79
 - SAML 74

H

- HA Database Replication 236

L

- latency 205
- LDAP
 - Authentication domain 59
 - Configuration 57
 - External authentication 58
 - Group mappings 61

M

- Microsoft
 - Azure AD 76
 - Entra ID 76
 - monitoring 145

N

- Notification
 - Add 108
 - Change language for notification e-mails 109
 - Change notification triggers 109
 - Change recipients list 109
 - Delete 109
 - Disable 109
 - Template 105
 - Create 108
- Notifications 101
 - Deactivate missing GPG key warning 109
 - E-mail sender 108
 - List 101

O

- OIDC
 - Authentication domain 78
 - External authentication 77
 - Group mappings 79

P

- Password change plugins 209, 213
 - Check Point 215
 - Cisco 216, 216
 - Citrix 217
 - Dell 217
 - F5 218
 - Fortinet 218
 - HP 219
 - IBM 220, 222
 - Juniper 223
 - LDAP 223
 - MySQL 224
 - Oracle 225
 - Palo Alto 225
 - Ultra VNC 226
 - Unix 227
 - VMware 228
 - Windows 228, 231, 233
- Password change policies 209, 209, 212
 - Create 210
 - Delete 213
 - Edit 212, 212
 - Periodicity 212
- Password vault plugins 209, 235
 - Bastion 236
 - CyberArk 237
 - HashiCorp 238
 - Thycotic 240
- Permission profile
 - create 37
 - custom 37, 38, 38, 42, 43
 - default 34
 - delete 43
 - edit 42
 - export 38
 - import 38
- Permission profile

- details
 - configuration 23
- Protected group 185

R

- RAW TCP/IP 272
- RDP connections 146, 148
- RDP session 252, 253
- Reconciliation
 - definition 180
- restrictions 253, 256
- round-robin 145

S

- SAML
 - Authentication domain 73
 - External authentication 72, 75
 - Group mappings 74
- scan 205
- Screen resolution 148
- script execution 132
- Secondary authentication 146
- Secret rotation 209
 - Automatic 243, 244, 245
 - Check-in 244
 - Manual 244, 245, 246
- Session administration 153, 185, 252, 253, 254, 256
- Session invite 262
- Session management 134
- session probe 145
- SSH session 256
- subnet 263

T

- Transformation rule 135, 136

U

- Universal Tunneling 272
- User accounts
 - Azure AD 74
 - Directory Services 52
 - Entra ID 74
 - Local 80
 - Authentication protocols 85
 - Create 81
 - Delete 91
 - Edit 90
 - Export 91
 - Import 82
 - Unlock 90
 - OIDC 77
 - SAML 71
- User authentication 12
 - Kerberos 14
 - Login and password 13
 - OIDC 13
 - SAML 13
 - X.509 certificate 13
- User profile

<i>Introduction</i>	22
<i>User session</i>	
<i>RDP</i>	153, 185
<i>SSH</i>	254
<i>Users</i>	
<i>Account details</i>	47
<i>Authentication methods</i>	48
<i>Communication</i>	100
<i>Groups</i>	43
<i>Identities</i>	48
<i>Profiles</i>	22



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