

LDD ONELOGIN

WALLIX Deployment Low Level Design <OneLogin>

onelogin

Contacts WALLIX:

Vice President Customer Success	Name : Grégory Rousseau Tél : +33 1 81 69 93 46 E-mail : grousseau@wallix.com
Cybersecurity Senior Consultant Customer Success	Name : Sėti Armel Digbo Bi Tél : +33 6 63 52 20 23 E-mail : sdigbobi@wallix.com
Bastion Managed Services Customer Success	Name : Bruno Marques Tél : +33 1 53 42 13 10 E-mail : bmarques@wallix.com

Date de rédaction : 29/03/2019

Révision 1.0

INTRODUCTION	5
A. OBJECT	5
B. COPYRIGHT NOTICE	5
1 ONELOGIN	6
1.1 ARCHITECTURE	6
1.2 ACCESS MANAGER CONFIGURATION.....	7
2 PROJECT ROADMAP.....	15
3 GLOSSARY	16

Author: Bruno MARQUES

Version Number	Update date	Status	Reason for the change
0.1	29/03/2019	Creation	

INTRODUCTION

a. Object

This document provides the low-level design of the integration of the WALLIX BASTION solution with OneLogin.

b. Copyright notice

This document contains confidential information and/or notices of ownership of WALLIX and may not be disclosed or reproduced, in whole or in part, in any format whatsoever, without the prior written permission of WALLIX. Please contact WALLIX at the address legal@wallix.com to request this prior written permission pursuant to articles L. 122-4 and L. 342-1 of the Intellectual Property Code.

This document is provided "as is" and for information purposes only. WALLIX reserves the right to make changes to this document or to the specifications and descriptions of related products at any time and without notice. In addition, WALLIX does not guarantee the use of this document and assumes no responsibility for any errors. Nor does it undertake to update the information it contains.

Copyright © 2019, WALLIX. All rights are reserved.

WALLIX and its logos are registered trademarks or trade-marks of WALLIX in France and/or other countries. Therefore, any reproduction and/or use without the prior consent of WALLIX will incur the responsibility of the user and constitute a violation punishable by the penalties described in articles L. 335-2, L. 713-2, L. 713-3 and L. 716. -1 of the Intellectual Property Code.

The other marks and names mentioned in this document may be trademarks and/or registered trademarks of their respective holders.

1 ONELOGIN

1.1 Architecture

WALLIX Bastion is a PAM solution*. It is designed as a reverse proxy with the ability to

- Give access permissions based on the user profile and the group.
- Trace the RDP and SSH connections, Applications with audit logs and session records.
- Store the passwords of the target servers in the vault with the possibility to change these passwords or SSH keys.

OneLogin is a cloud-based IAM* provider that designs, develops and sells a UAM* platform to enterprise-level businesses and organizations.

The OneLogin platform is an AMS* that uses SSO* and a cloud directory to enable organizations to manage user access to on-premises and cloud applications. The platform also includes user provisioning, lifecycle management and MFA*.

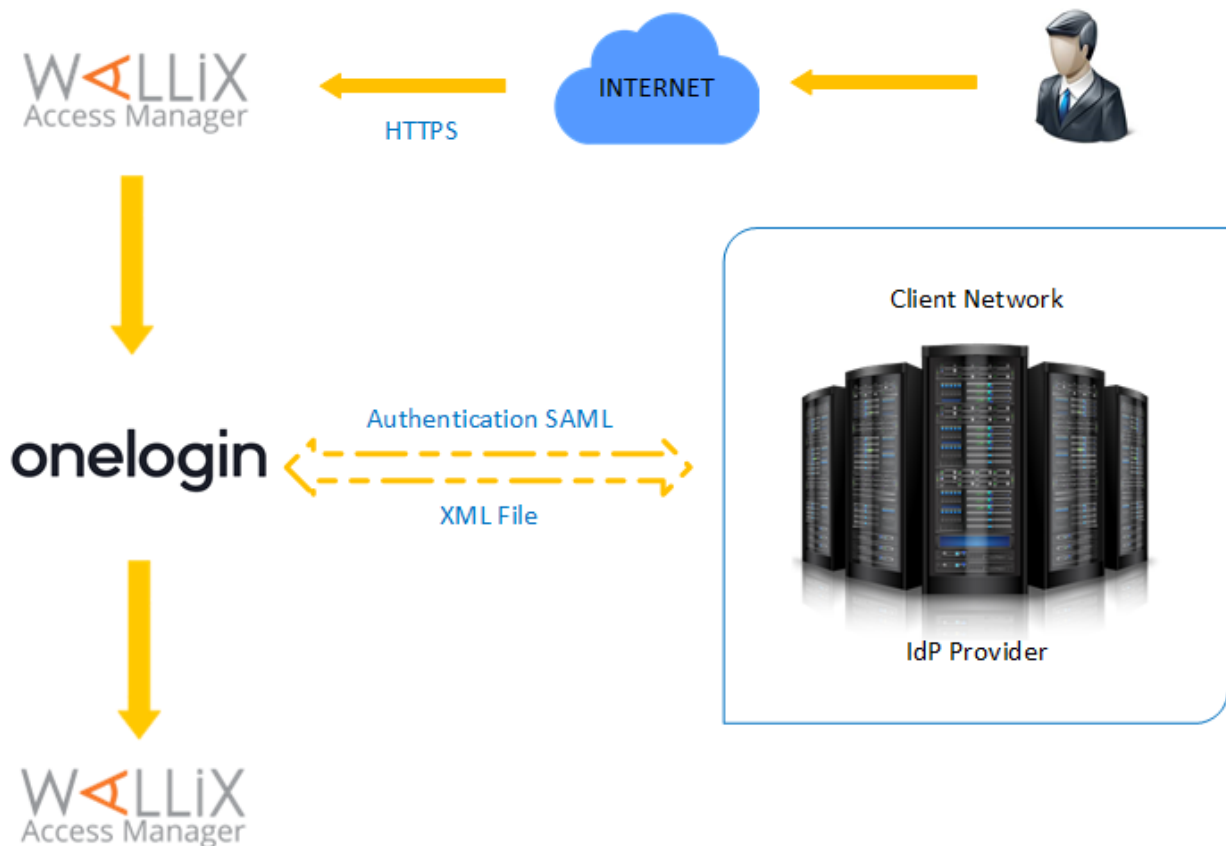


Figure #1: infrastructure model

1.2 Access Manager Configuration

In order to provide the integration of the WALLIX Bastion solution with OneLogin, some parameters are set in the web interface of the AM.

The AM is accessed by HTTPS (global organization).

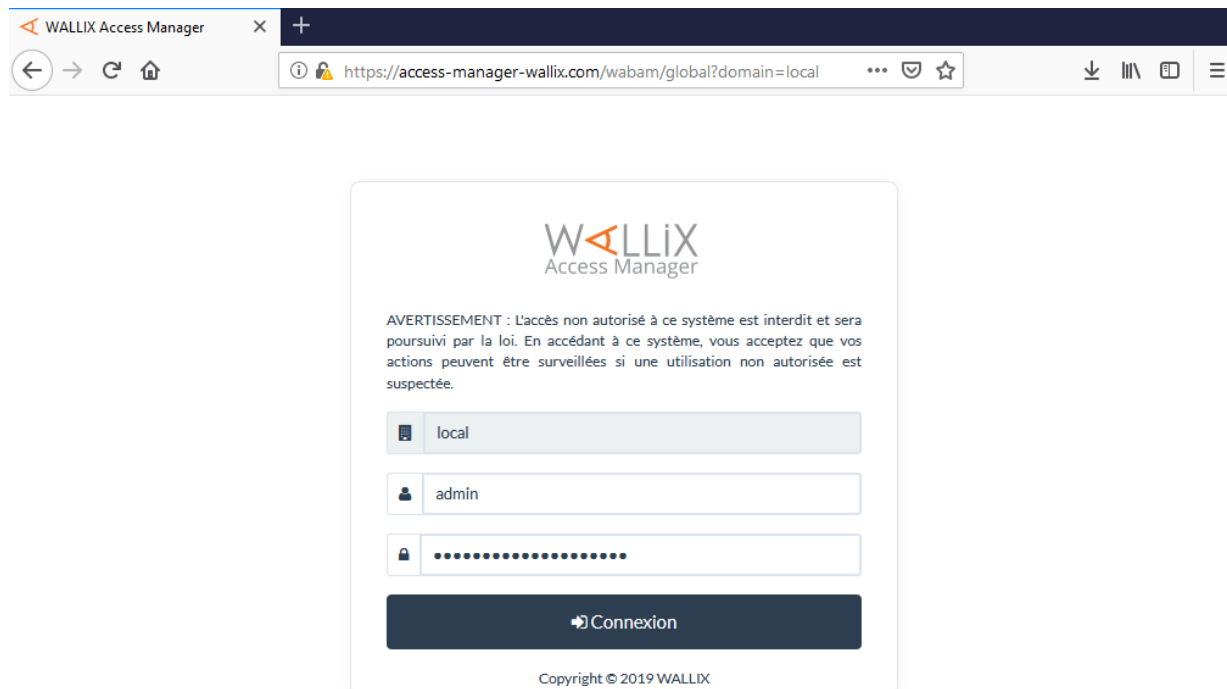


Figure #2: Access Manager Homepage

In the top menu, select “Configurations”, followed by “Organizations”.

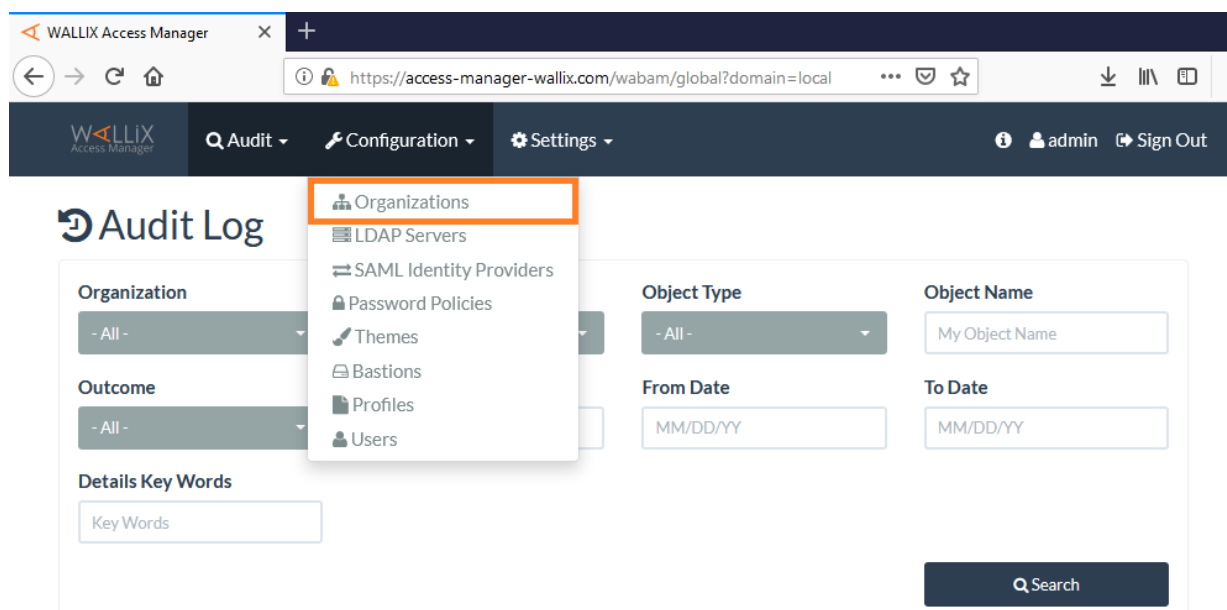


Figure #3: Add organization

Insert a name and an identifier for the organization and submit the form. By default, the option “Local Domain Name” should be set as “local”.

It is also possible to add a CA Certificate for the organization.

Add an Organization

Name*
WALLIX

Identifier*
wallix

Local Domain Name*
local

CA Certificate

Cancel Save

Figure #4: Add organization

Then, it is necessary to add a SAML* Identity Provider. For that, in the top menu, select “Configurations”, followed by “SAML Identity Providers”.

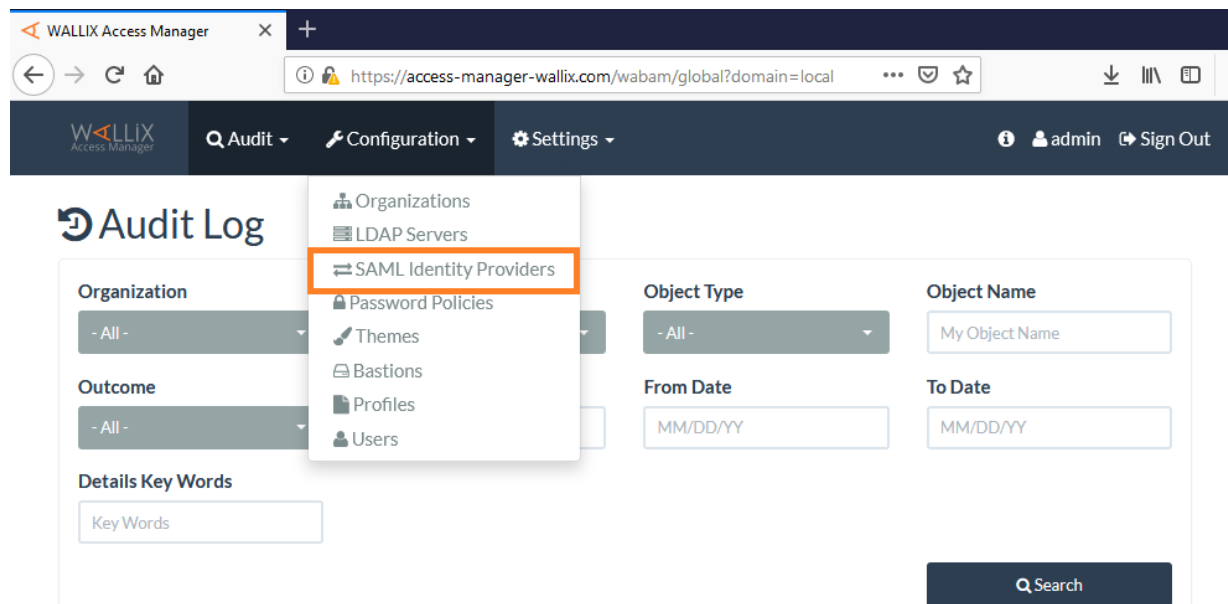


Figure #5: Add SAML Identity Provider

To add a new SAML Identity Provider, click on the button “+Add”.

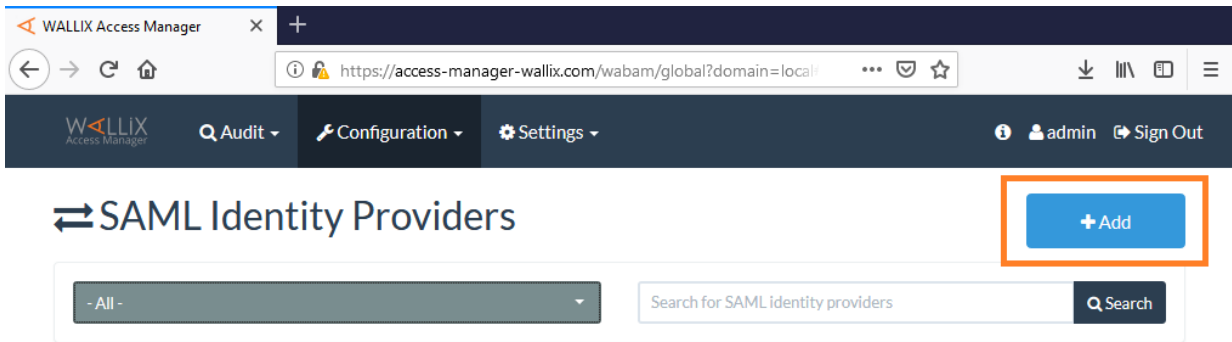


Figure #6: Add SAML Identity Provider


In the *tab* “Service Provider”, insert a name and a WALLIX-AM Entity Id. All the other options could be set as “No”: “Sign Messages”, “Encrypt Messages” and “Signed Response”.

A screenshot of the 'Add an SAML Identity Provider' form. The 'Organization' dropdown is set to 'WALLIX'. The 'Name' field contains 'onelogin-wallix'. The 'Service Provider' tab is selected and highlighted with an orange box. The 'WALLIX-AM Entity Id' field also contains 'onelogin-wallix'. There are three rows of toggle switches: 'Sign Messages' (set to 'No'), 'Encrypt Messages' (set to 'No'), and 'Signed Response' (set to 'No'). To the right, there are two sections for certificates: 'Signing Key & Certificate' and 'Encryption Key & Certificate', each with an 'empty' status and a 'Generate' button. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure #7: SAML Identity Provider – Service Provider

In the *tab* “Identity Provider” several fields are required (“Identity Provider Entity Identifier”, “SSO Binding Type”, “Redirect Binding Uri” and “Redirect Logout Uri”).



These fields are set manually or through the upload of a XML file provided by the customer.

 Add an SAML Identity Provider

Organization
WALLIX


Name*
onelogin-wallix


Service Provider **Identity Provider** Domain




 Fill the form or import metadata file. 

Identity Provider Entity identifier*
https://adfs-test.internal.lan/

SSO Binding Type
Redirect

Redirect Binding Uri* 
https://adfs-test.internal.lan/adfs/ls

Redirect Logout Uri* 
https://adfs-test.internal.lan/adfs/ls


Identity Provider Validation Certificate  
 empty

Cancel Save

Figure #8: SAML Identity Provider – Identity Provider

Once the XML file uploaded, all the fields are automatically updated.

The button “Identity Provider Validation Certificate” turns green in the case of a successful configuration or red in the case of some mismatch field.

 Edit SAML Identity Provider



Organization

WALLIX

Name *

onelogin-wallix

Service Provider Identity Provider Domain


 Fill the form or import metadata file. 

Identity Provider Entity identifier *


https://app-eu.onelogin.com/saml/metadata/27806a5b-0eb3-5cde-bef7-f3ed707d1e83

SSO Binding Type



Redirect


Redirect Binding Uri * 

https://wallix.onelogin.com/trust/saml2/http-redirect/sso/543927

Redirect Logout Uri * 

https://wallix.onelogin.com/trust/saml2/http-redirect/slo/543927

Identity Provider Validation Certificate  







 Delete  Cancel  Save

Figure #9: SAML Identity Provider – Identity Provider

In the *tab* “Domain”, insert a “Domain Name”, set a “Default Profile” and a “Default Language”.

Click over the Attributes in order to edit the “Mapping Attributes”.

 Add an SAML Identity Provider

Organization
WALLIX

Name *
onelogin-wallix

Service Provider Identity Provider **Domain**

Domain Name *
wallix.com

Attributes *
Please Configure


Default Profile
User

Default Language
English

Cancel Save

Figure #10: SAML Identity Provider - Domain

In the configuration of “Mapping Attributes”, at least the “Login” should be set. All the other fields are optional.

 Edit Mapping Attributes

Login *
Login

Display Name Attribute
DisplayName

Email Attribute
email

Language Attribute
preferredLanguage

Profile Attribute
eduPersonAffiliation

Cancel Save

Figure #11: SAML Identity Provider - Domain

The button “Attributes” turns green in the case of a successful configuration.

Add an SAML Identity Provider

Organization
WALLIX

Name*
onelogin-wallix

Service Provider Identity Provider Domain

Domain Name* wallix.com

Attributes*

Default Profile User

Default Language English

Cancel Save

Figure #12: SAML Identity Provider - Domain

Click on the button “Save” and if everything is well configured, a message in the top of the page saying that the SAML Identity Provider has been saved will appear.

WALLIX Access Manager

https://access-manager-wallix.com/wabam/global?domain=local/

WALLIX Access Manager Audit Configuration Settings

SAML Identity Providers

+ Add

- All - Search for SAML identity providers Search

1 - 1 of 1

<input type="checkbox"/>	Organization	Name	Domain Name
<input type="checkbox"/>	WALLIX	onelogin-wallix	wallix.com

Figure #13: SAML Identity Provider - Domain

Now, when accessing to the AM, an automatically redirection will be made to the IdP Provider of the customer, that will allow the user to authenticate in the WALLIX BASTION solution.

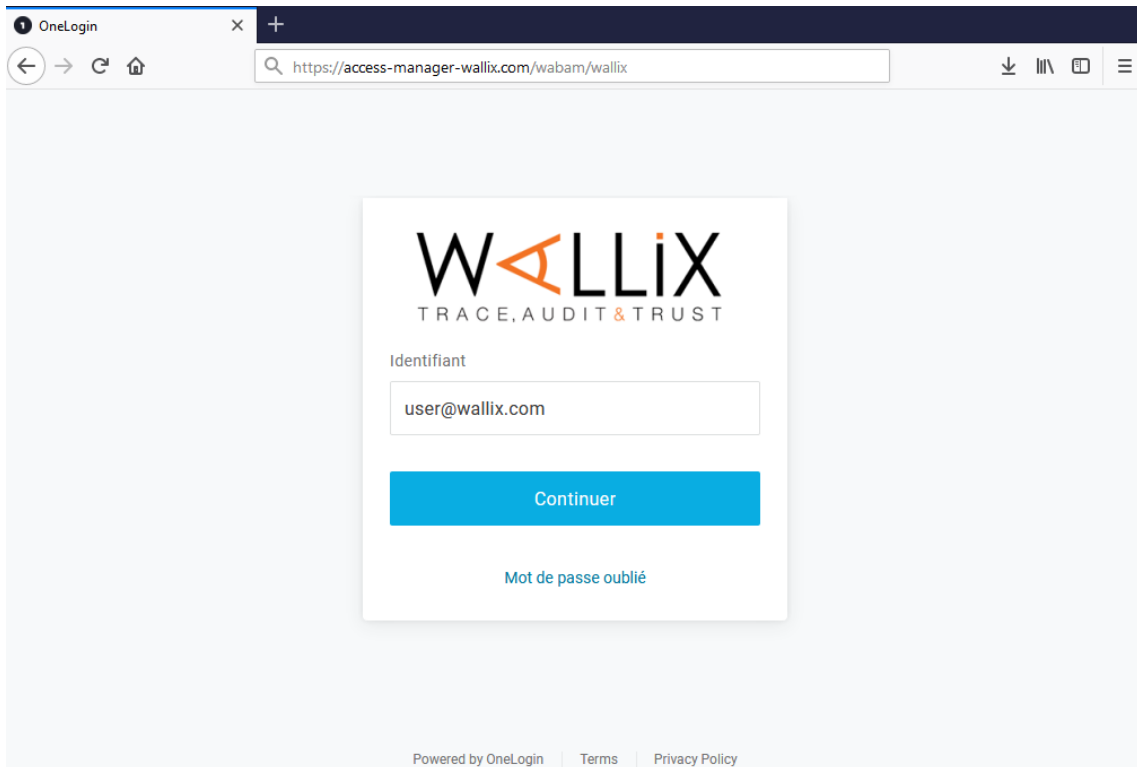


Figure #14: OneLogin Authentication

If the user exists in the Customer IdP Provider and is configured with the right permissions, he is redirected again to the WALLIX AM where he is able to see his list of authorizations.

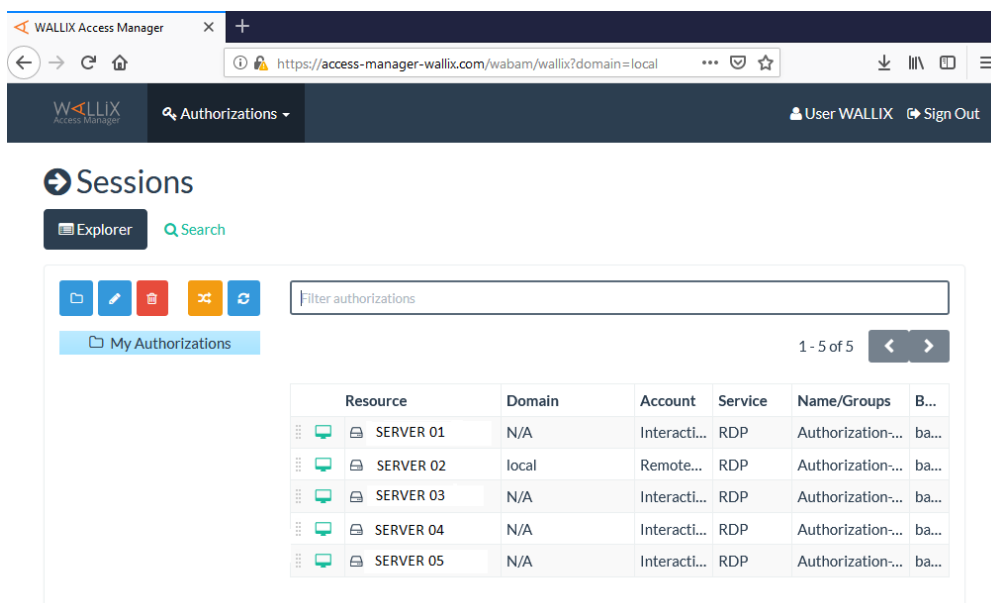


Figure #15: User list of authorizations

2 PROJECT ROADMAP

Phase	Task	Responsible
Access Manager Setup	Configure Organization	WALLIX
	Provide XML File for SAML integration	CUSTOMER
	Configure SAML Identity Provider	WALLIX
Platform Testing	Test redirection from Access Manager to OneLogin	WALLIX
	Authentication through OneLogin	CUSTOMER

3 GLOSSARY

PAM: Management of Privilege Accounts.

IAM: Identity and Access Management

UAM: Unified Access Management

AMS: Access Management System

SSO: Single Sign-One

SAML: Security Assertion Markup Language

MFA: Multi-Factor Authentication

RDP: Remote Desktop Protocol (RDP) is a protocol that allows a user to connect to a server running Microsoft Terminal Services. Customers exist for almost all versions of Windows, and for other operating systems, such as GNU/Linux systems. The server listens by default on TCP port 3389.

SSH: Secure Shell (SSH) is both a computer program and a secure communication protocol. By default, an SSH server listens on the standard TCP Port 22.

LB : Load distribution (in English : Load Balancing) is a set of techniques for distributing a workload between different computers in a group. These techniques allow both to respond to a too large load of a service by distributing it over several Servers, and to reduce the potential unavailability of this service that could cause the software or hardware failure of a single server.

AM: WALLIX Access Manager (Access Manager). WALLIX Access Manager (Access Manager) provides connection services between Web browsers and targets to which users are allowed access. Access to targets is made through WALLIX Bastion appliances. Connections are made using HTML5 clients; Browsers do not require any extension.

Access Manager also allows users with the appropriate rights to view the passwords of the targets in the browser and/or copy them directly to the Clipboard.

Access Manager supports a "multi-tenant" configuration using containers called "organizations".