LDD ONELOGIN

WALLIX Deployment Low Level Design <OneLogin>

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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 : Séti 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

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

Author: Bruno MARQUES

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

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

INTRODUCTION

a. Object

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

b. Copyright notice

© WALLIX Group 250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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*.

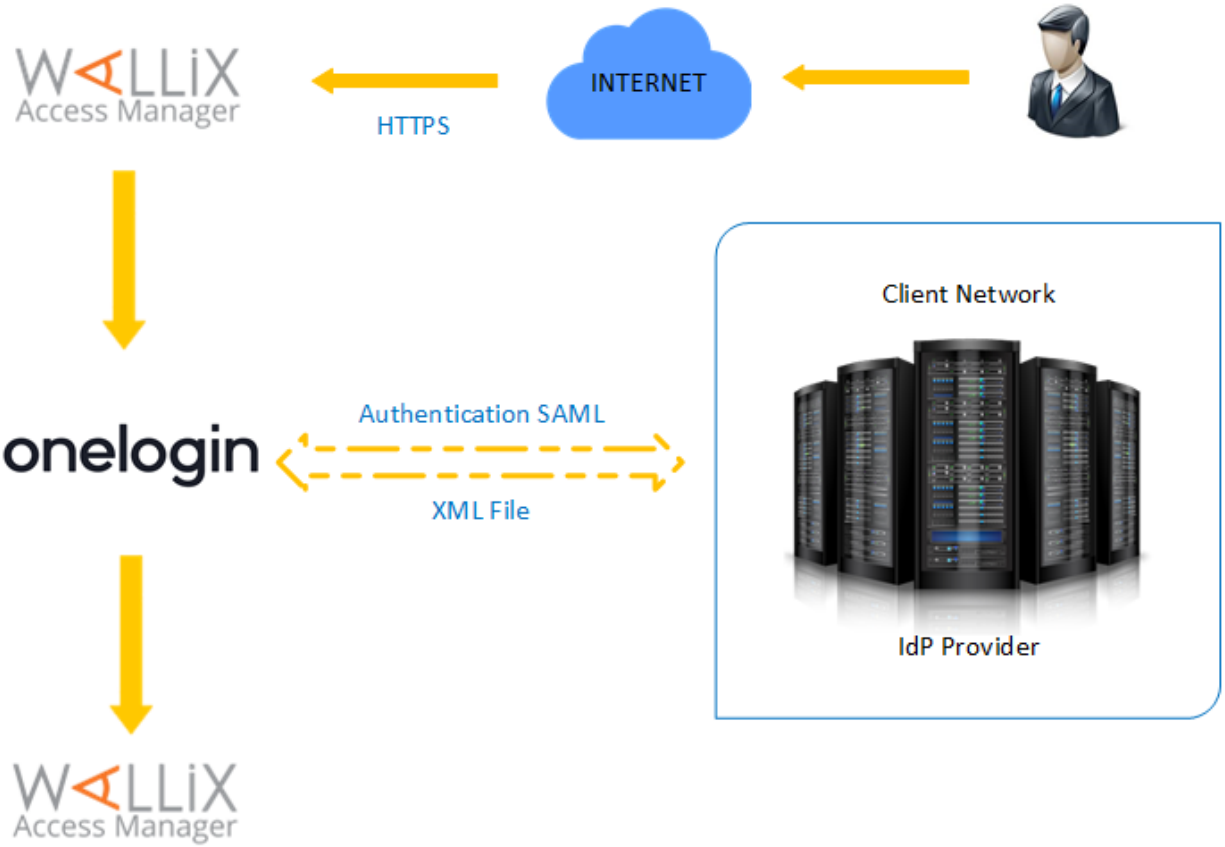

Figure #1: infrastructure model

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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”.

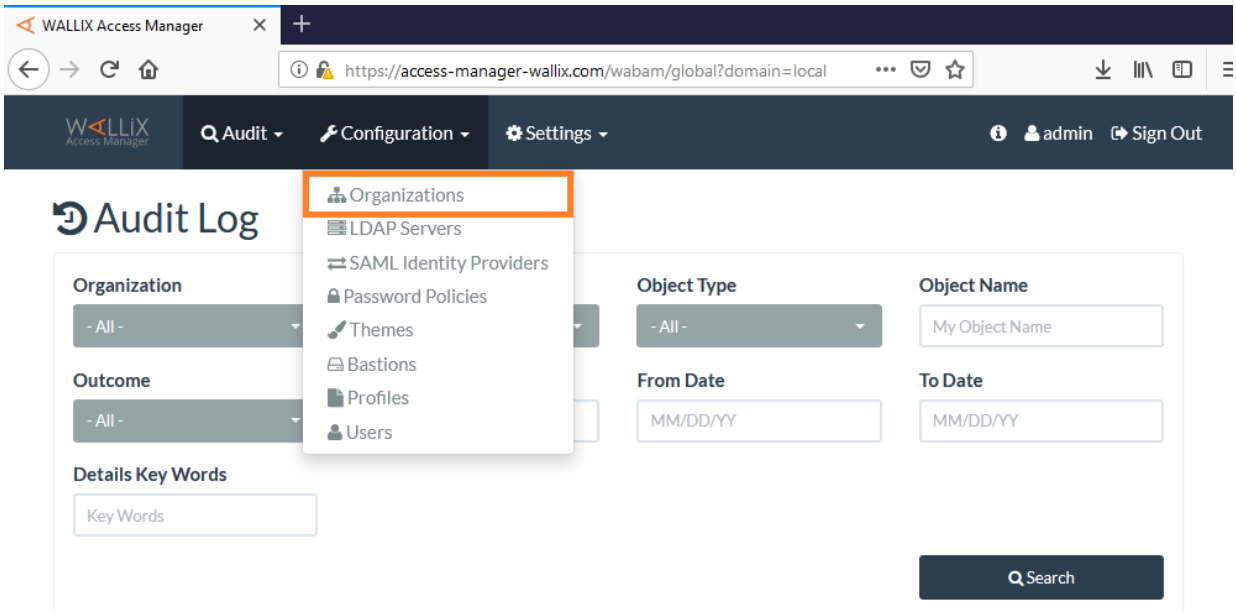

Figure #3: Add organization

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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.

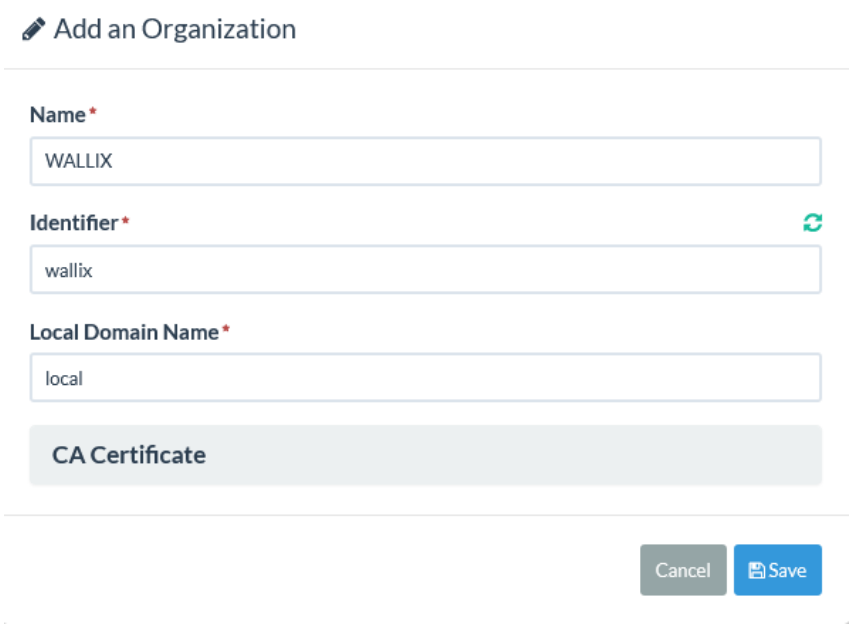

Figure #4: Add organization

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

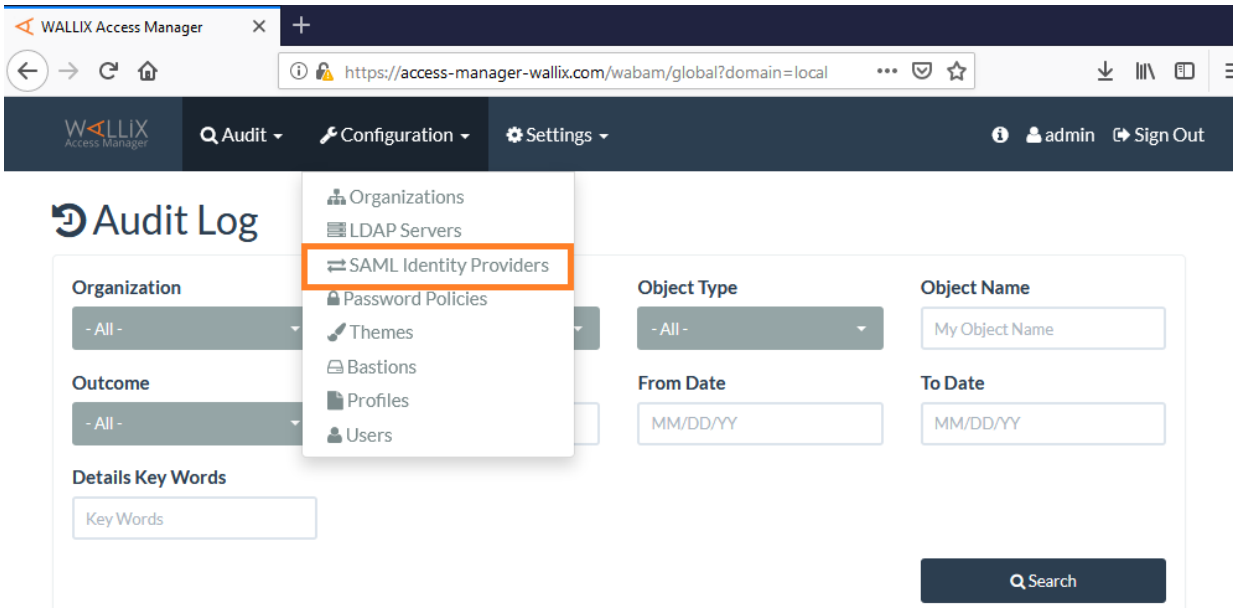

Figure #5: Add SAML Identity Provider

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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

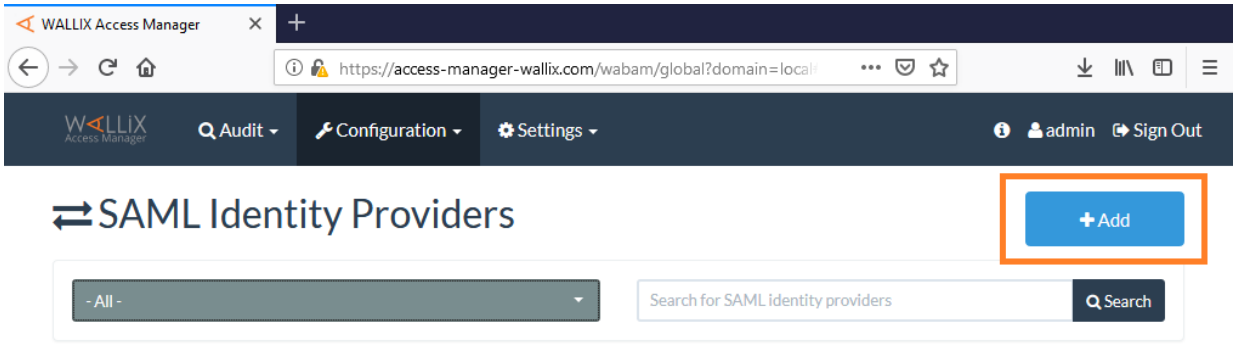

Figure #6: Add SAML Identity Provider

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”.

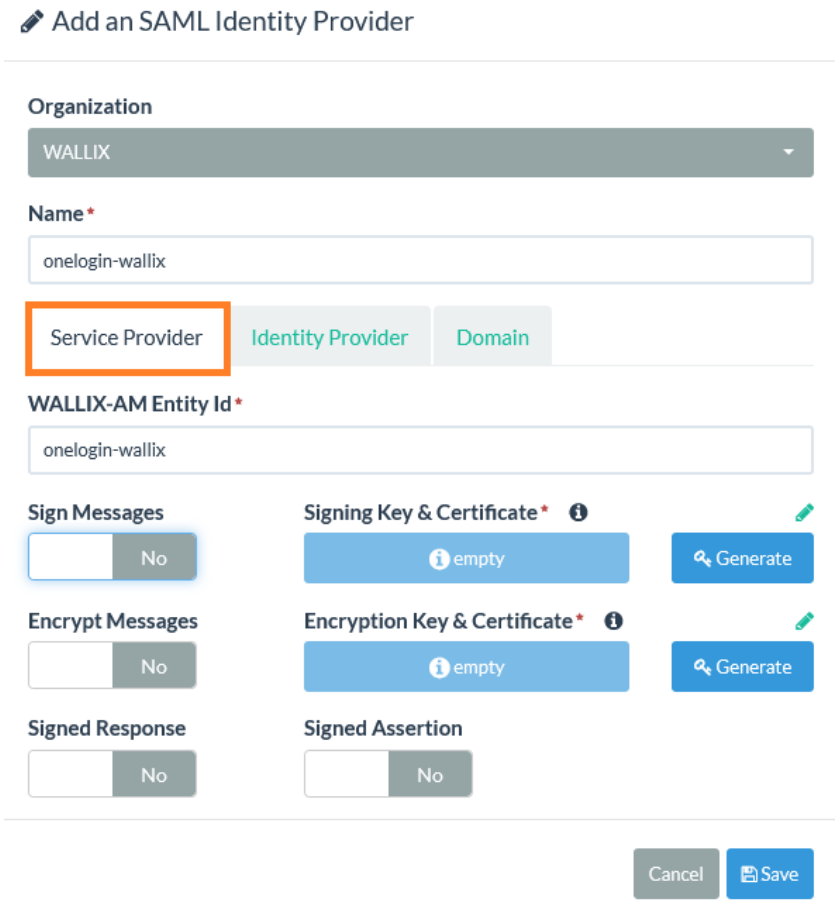

Figure #7: SAML Identity Provider – Service Provider

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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

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

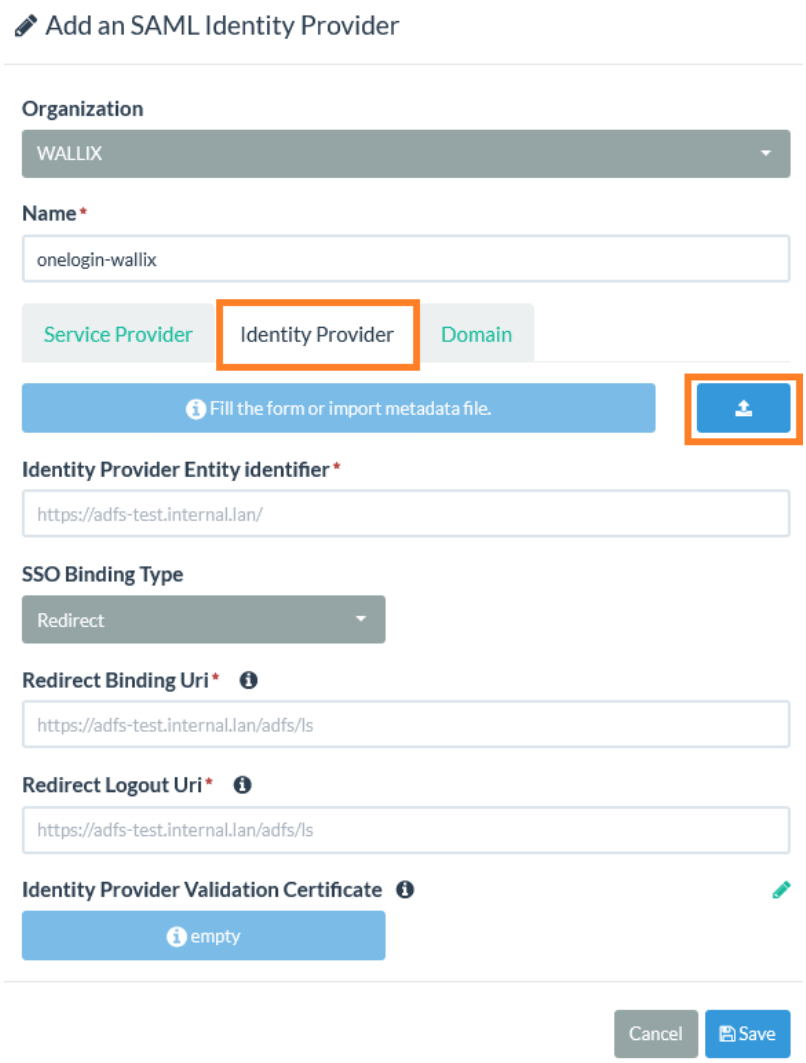

Figure #8: SAML Identity Provider – Identity Provider

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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.

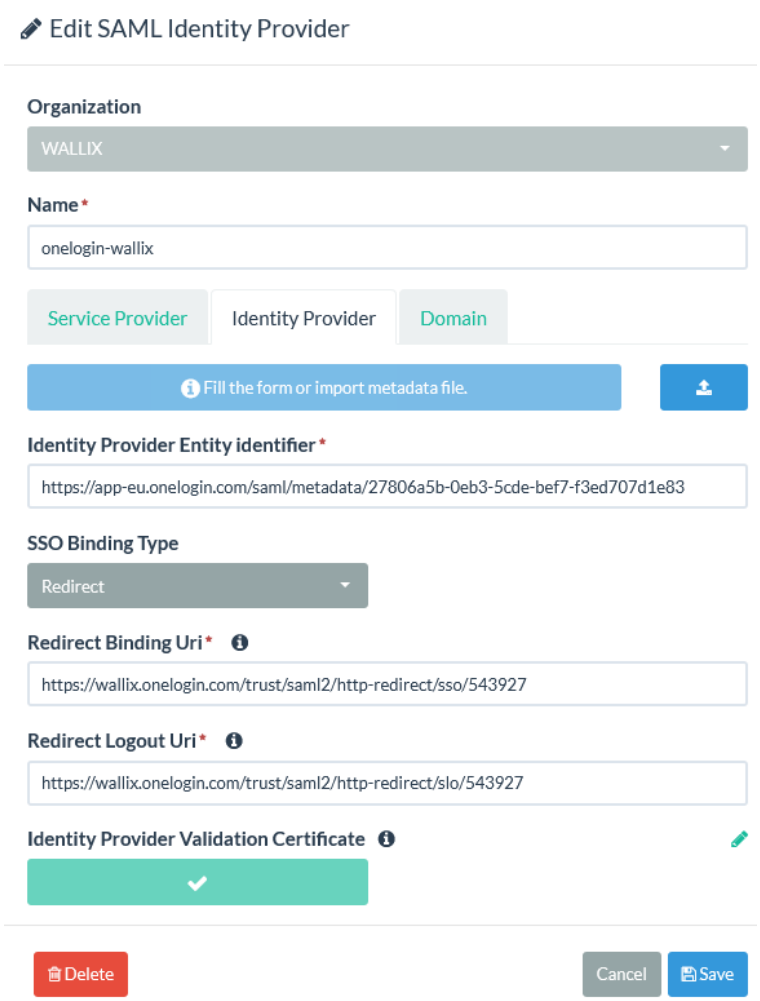

Figure #9: SAML Identity Provider – Identity Provider

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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”.

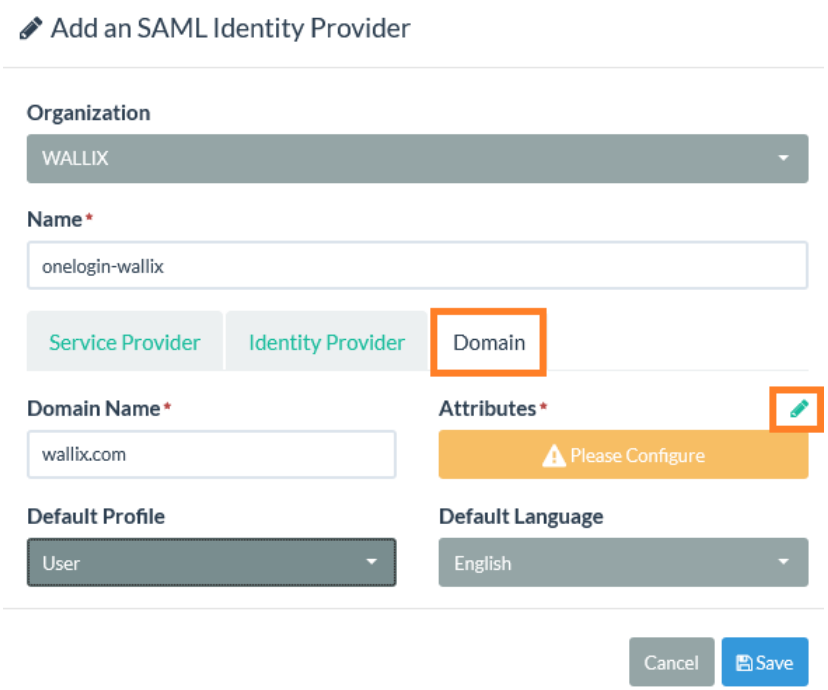

Figure #10: SAML Identity Provider - Domain

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

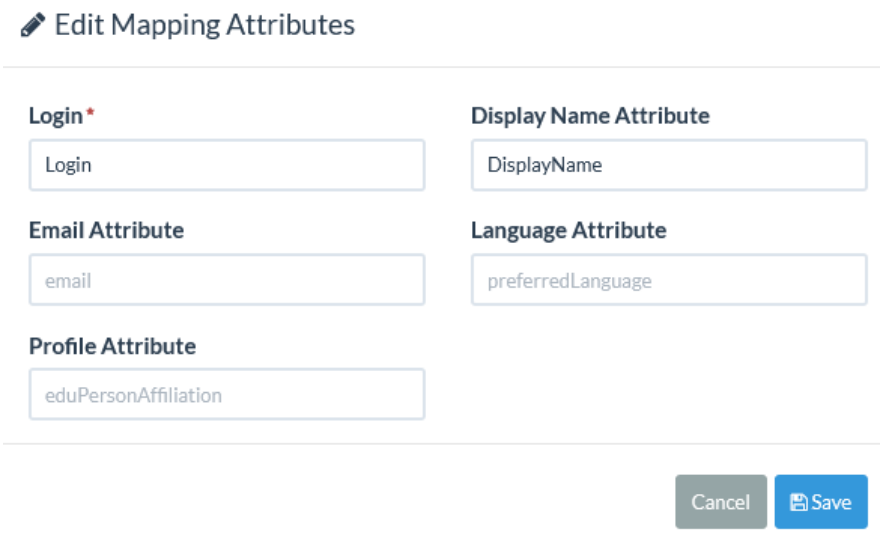

Figure #11: SAML Identity Provider - Domain

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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

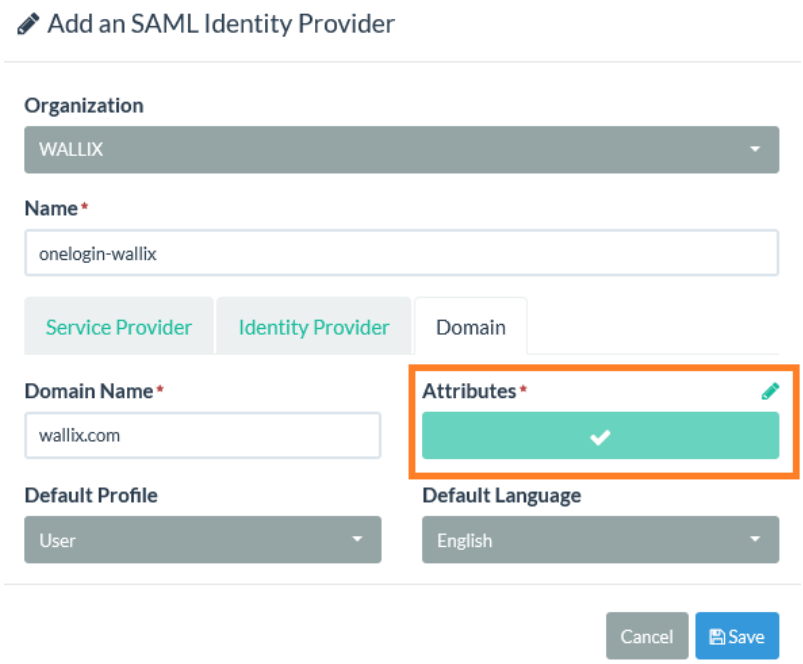

Figure #12: SAML Identity Provider - Domain

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.

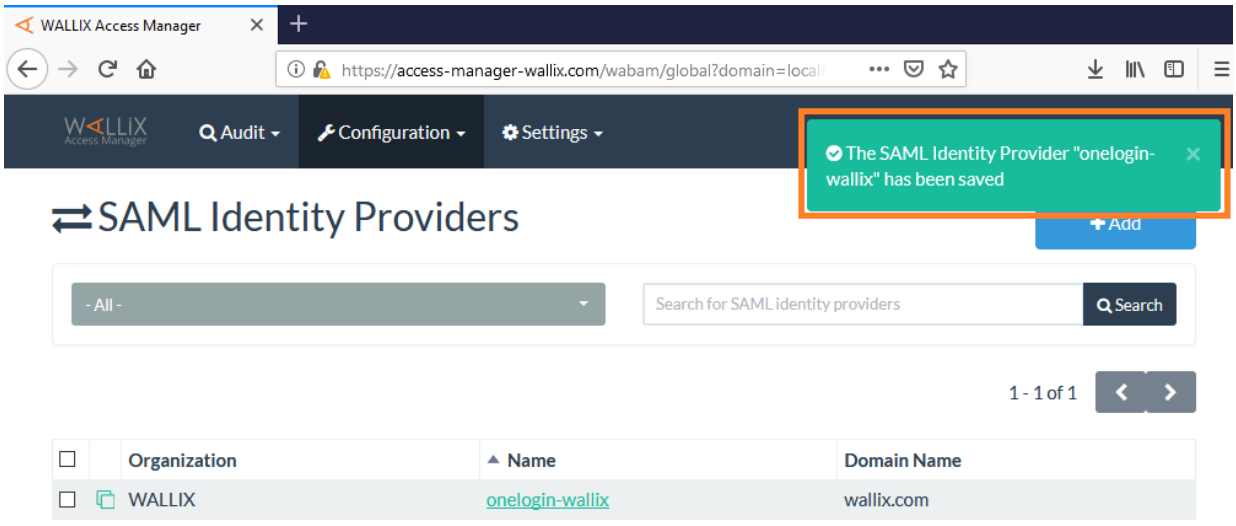

Figure #13: SAML Identity Provider - Domain

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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.

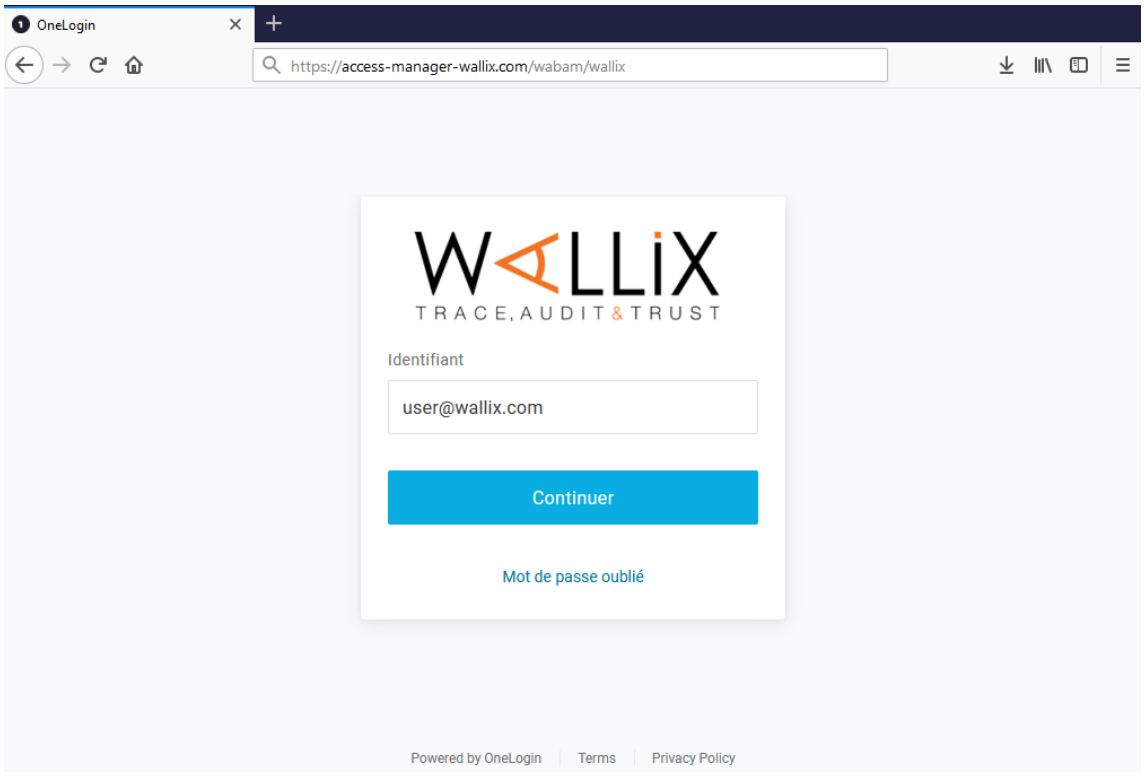

Figure #14: OneLogin Authentication

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.

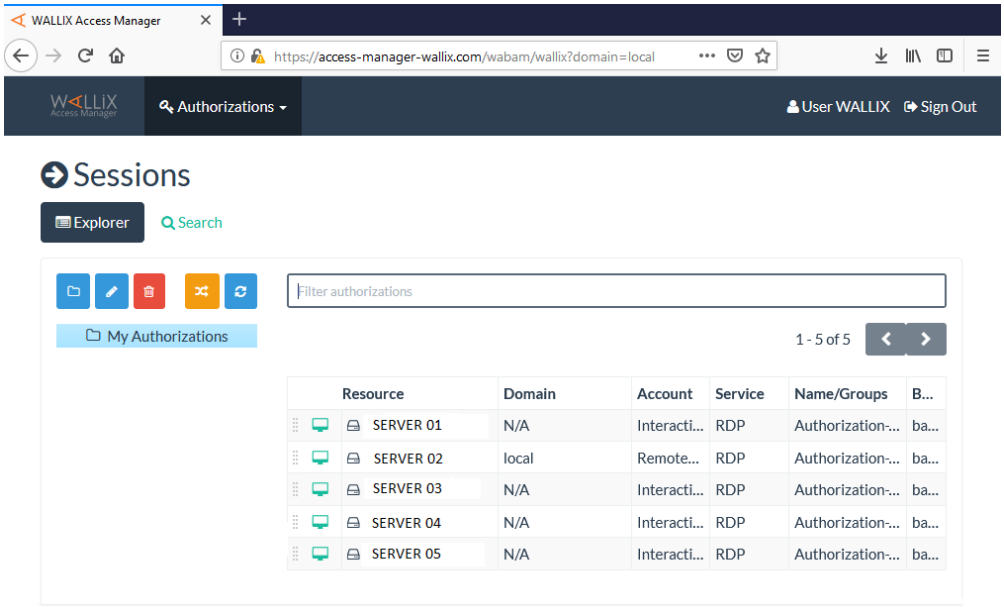

Figure #15: User list of authorizations

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68

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".

250Bis, rue du Faubourg Saint Honoré - 75008 Paris – France
Tél. +33 1 53 42 12 90 - Fax +33 1 43 87 68