SAML Authentication

SAML Authentication

uthentication Options				
ladius	Enable SAML	OFF		
AP	User Attribute:			
ML Service	Oreun Atteilustes			
JO Mobile	Group Attribute:	Or apply a default groups to every customer logged via SAML If the Identity Provider doesn't include group list in the login response you can apply a default ones. Use the dropdown bellow to specify the groups that will be applied to the users logged via SAML.		
	IDP Metadata:			
SAML Service provider configuration.				
	Sign logout request:	OFF		
	Sign redirect request:	OFF		
	Unencrypted Assertions from IdP Will be rejected:	OFF		
	Private key:			
	Certificate:			
	The Identity Provider you want t	to connect needs the ProVision SP Metadata file. You can download it in PHP or XML for		
		Test SAML configuration Save		

SAML is a Single Sign On (SSO) authentication method that uses an external identity provider to authenticate a user at their first login, saving a token to the user's browser that is then used for subsequent logins, so that the user does not need to re-submit credentials.

SAML Authentication options are accessed by clicking the "Authentication" sub-tab at the top of the Admin Settings page, then selecting "SAML Service" under the "Authentication Options" module.

- SAML Setup

 - Set up the IdP
 Users and Permissions:
 Configure SAML in ProVision
- SAML Login

- Initial Login:
- Subsequent Logins:

SAML Setup

Before configuring SAML in ProVision, you must have an account set up with an Identity Provider (IdP) and ProVision users / groups set up in the IdP:

Set up the IdP

To use SAML authentication, you will need SAML set up for your instance with an Identity Provider (IdP), such as *Microsoft ADFS*, *OneLogin*, *Elastic SSO*, or others. You can view a list of available SAML IdPs at Wikipedia's SAML based products page.

Note

Some identity providers (such as Workspace One) have additional public/private key authentication requirements in excess of what is required in ProVision.

If you receive a SAML configuration error of "Unable to load private key" or similar, please check your IdP requirements and documentation.

Users and Permissions:

User credentials will need to be created and associated with ProVision permission group names via the IdP. All user creation, management and permissions handling occurs via the IdP, externally from ProVision.

Configure SAML in ProVision

ProVision setup for SAML is located in Admin Admin Settings Authentication Options.

Under SAML Configuration:

Enable SAML authentication by clicking the checkbox next to "Enable".

The following fields are required and will need to be obtained from the IdP:

- User Attribute(Required):
- Group Attribute(Required):
- IdP Metadata(Required):

Under SAML Service Provider Configuration:

- Sign logout request:
- Sign redirect request:
- Unencrypted Assertions from IdP Will be rejected:
- Private Key:
- Certificate (Required):

Links are provided below the configuration settings for the ProVision SP Metadata file in php and xml format, which will be needed to provide to the IdP.

You can test the configuration by clicking the "Test SAML Configuration" button, a new page will open giving health check information for your provided attributes.

Using the External ID Field

For some SAML providers it is not possible to have a user friendly group name. For example, while ProVision tries to match ProVision group names against Microsoft Azure group names, MS Azure exports group names like "abc-GFHEKJSHD-123". In these cases, you can set the "External ID" field for a group (in the below example "New Global Group") to be equal to "abc-GFHEKJSHD-123". Then, when logging in via SAML, ProVision will correctly recognize that the SAML User should be part of the "New Global Group" group.

New Global Group		Group da	Group data and permissions		Custom navigation options		
Group information	Resource permissions C: Create R: Read U: Update D:				: Delet		
Group Name	Resource lookup						
New Global Group	Start typing to find	a resource			\sim	Add reso	ource
External Id	TLR					3	×
This group is enabled	IPAM	Peer	Resource	User	SWIP	Admin	
Comments							
Example							
Group Users 0							
Group Users 0 Filter users Manage users							
Group Users O Filter users Manage users No users to display							-

To add an external ID, go to Admin User Groups. Select a group to edit, enter the external ID, and click "Save". For more details on working with permissions groups see Working with Groups.

SAML Login

Once the correct configuration has been established and users set up for SAML in the IdP, users will be able to use SAML logins.

Documentation Note: Depending on the IdP used, some screens may appear different from what is shown here.

Initial Login:

The initial login process occurs for the first time a user logs in, and anytime afterwards if the browser token is not present (e.g., cookies are cleared from the browser, the browser closed, or a new browser is used).

From the ProVision login page, select SAML from the authentication options dropdown - you do not need to enter Username or Password.

	6connect ProVision⊷		
	User Name Password		
		Local V Login Local Radius	
Version 8		LDAP SAML	A .

You will be redirected to the IdP site as set up in the Admin Configuration - here, we are using Microsoft ADFS (Active Directory Federation Services).

Log into the IdP site using your SAML credentials, and click "Sign In".

6connect
Sign in with your organizational account bomeone@example.com Password
Sign in

If the sign in is successful, you will be logged into the ProVision home page.

Subsequent Logins:

After the initial login via the IdP (as long as the auth token is present) users will be able to login to ProVision simply by selecting the "SAML" options from the ProVision login page without entering credentials.

	6connect ProVision-∞		
	User Name Password		
		Local V Local Radius	Login
Version 8		LDAP SAML	4

The auth token may be destroyed or not available if browser cookies have been cleared, a different browser used, or the browser fully closed, depending on security settings. In these cases, the user will need to sign in again via the IdP.

Setting default login authentication options

In the login screen, you would select the authentication method from the dropdown. If you like, you can set the default login option in the following way:

Go to the /data/globals.php and open in vi (or other editor). Add in the following text as the last line of the file (before the closing ?>)

define('DEFAULT_LOGIN_TYPE', 'saml');

Acceptable values are "local", "radius", "ldap" and "saml". If this line is not present in globals.php, the default option is "local".