WALLIX Bastion SAML

This page is temporary, until we have a dedicated template on Trustelem and integration into the 'setup intructions' page dedicated to Bastion and AM.

Step 1: on Trustelem, create an application

As we don't have a dedicated template yet, you have to choose the **generic SAML2 model**. Once the application is created, you can save it without any modification and then download the metadata file.

Step 2: on the Bastion, create an External authentication

On the Bastion admin interface:

1. Create a new **SAML** external authentication (Configuration > External authentications)
2. Upload the Trustelem metadata file on the field **IdP metadata**
3. Complete the claims customization
   - Username: email or sAMAccountName, depending on whether Trustelem users come from the AD or not.
   - Display name: displayname
   - Email: email
   - Language: empty
   - Group: groups
4. Click on apply
5. Copy the **SP entity ID** and the **SP assertion concumer service**

Step 3: on the Bastion, create an Authentication domain

On the Bastion admin interface:

1. Create a new **Other IdPs** authentication domain (Configuration > Authentication domains)
2. Define a Domain server name
3. Define an Authentication domain name
    - This value will be used to authenticate on the proxy if this Authentication domain is not the default one
    - This value will be used in the Access Manager setup, if you want to use this product
4. Choose the Authentication protocole created in the 2nd step
5. Define the Label for authentication button on the login page
6. Define a default email domain
7. Choose a default language
8. Save the configuration
9. Copy the **IdP initiated URL**

Step 4: on Trustelem, edit the previous application

Edit the application created at the 1st step.

- EntityID: SP entity ID copied during the 2nd step
- Assertion Consumer Service: SP assertion concumer service copied during the 2nd step
- NameID Format: default value
- NameID Attribute: default value
- Attributes List: email,displayname
- Custom login URL: IdP initiated URL copied during the 3rd step
- Custom script:
  This script can be adapted if something else should be sent to the Bastion

  ```
  for (let g in groups){
    msg.addAttr("groups",g);
  }
  ```

Step 5: define the access & rights

Now the setup is ready, but users can't authenticate on the Bastion and don't have rights.

1. On Trustelem, create permissions for users who should have access to the Bastion
2. On the Bastion Authentication domain (step 3), create the mapping between the Bastion user groups and the groups existing on Trustelem

Access Manager with SAML Bastion

If you want to use Access Manager with SAML Bastion, the Access Manager should be > 5.0
In addition, some parameters on the SAML Access Manager should be identical as what was setup for the Bastion:

- AM Domain Name = Bastion Authentication domain name
- AM Login = Bastion Username

Finally, you have to create the same script for you SAML Access Manager app, as the one existing on the Bastion.

```
for (let g in groups){
  msg.addAttr("groups",g);
}
```

Revision #2
Created 18 December 2024 08:00:18 by WALLIX Admin
Updated 18 December 2024 08:50:44 by WALLIX Admin