Single Sign-On with SAML

Version 7.2

EN

24 October 2023

Copyright

Rüppurrer Straße 1, 76137 Karlsruhe (Germany), www.brandmaker.com

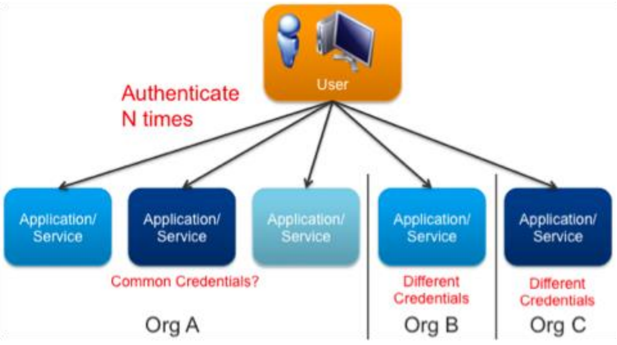
Your feedback is important to us!

We welcome all comments and would be grateful to be notified of any errors you may discover. Just send us an email to documentation@brandmaker.com.

Table of contents

1 Single Sign-On (SSO)

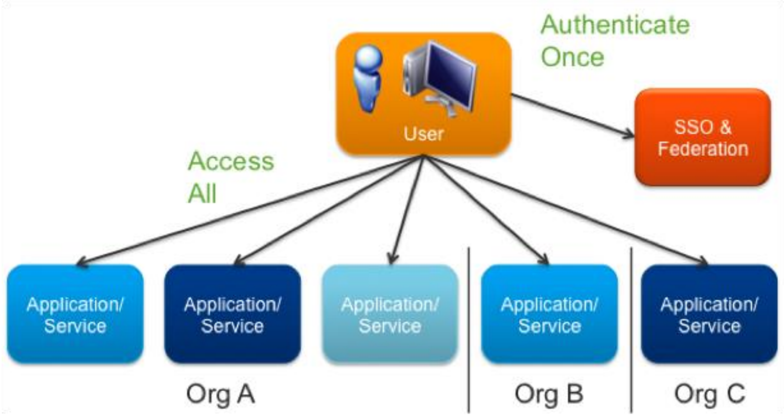
Modern companies and IT organizations have many applications, both internal and customer facing. With these many applications your users are faced with the challenge of not only managing multiple sets of credentials but are also forced to login to each and every individual application separately. This creates a bad experience for your users.



The solution is a combination of single sign-on and federation, where the credentials are unified for federation to target apps, authentication happens once, and the credentials are sent to the target apps for authorization.
This is what the original “true” meaning of SSO is.

Modern SSO Solutions: (True) SSO and Federation

SSO does not only provide your users with a single set of credentials which they can use across all SSO enabled applications, it also allows them to login just once for the whole set of applications. After they have logged in once they are no longer prompted to login, even if accessing a different application. Since the user is already authenticated by the time they reach your application, all your application has to do is apply its specific authorization rules based on the user's credentials (e.g., username, groups, roles, etc.) provided as part of the SSO process.



Federation takes SSO to the next level and enables users outside of your security domain, whether they are from a trusted partner or authenticated by a trusted 3rd party, to access your applications with their existing security credentials. With this, you can federate your SSO solution outside your organization and allow trusted 3rd parties to login once and use your applications.

Finally, the final major benefit of SSO and Federation is provisioning. You no longer must manually provision new users into your system, even if they are partners from outside the organization. The first time the user tries to access your application you use the data provided as part of the SSO process to automatically perform any required provisioning in your system and perform any necessary authorization, likely based on the user's groups or roles.

2 Info About SAML

The BrandMaker application uses *Security Assertion Markup Language (SAML)* to set up single sign-on (SSO). SAML standards define an XML-based framework for describing and exchanging security information (authentication, authorization, federation) to enable “true” SSO.

> *“Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee. SAML dates from 2001; the most recent major update of SAML was published in 2005, but protocol enhancements have steadily been added through additional, optional standards.*
>
> *The single most important requirement that SAML addresses is web browser single sign-on (SSO). Single sign-on is common at the intranet level (using cookies, for example) but extending it beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. [..]”*
>
> (Source: Wikipedia, https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language, 18 June 2015)

2.1 Advantages of SAML

These are some of the reasons why enterprises like SAML and therefore the BrandMaker application supports SAML:

Standards-Based

SAML is based on a standard that ensures interoperability across identity providers and gives enterprises the freedom to choose a vendor.

Usability

One-click access from portals or intranets, deep linking, password elimination and automatically renewing sessions make life easier for the user.

Security

Based on strong *digital signatures* for authentication and integrity, SAML is a secure single sign-on protocol that the largest and most security conscious enterprises in the world rely on.
User passwords may never cross the firewall, since user authentication in general occurs inside of the firewall and multiple web application passwords are no longer required.
SAML provides access to web apps for users outside of the firewall. If an outside user requests access to a web application, the SP can automatically redirect the user to an authentication portal located at the identity provider. After authentication, the user is granted access to the application, while their login and password remains locked safely behind the firewall (depending on your local infrastructure setup).

Phishing Prevention

If you don’t have a password for an app, you can’t be tricked into entering it on a fake login page.

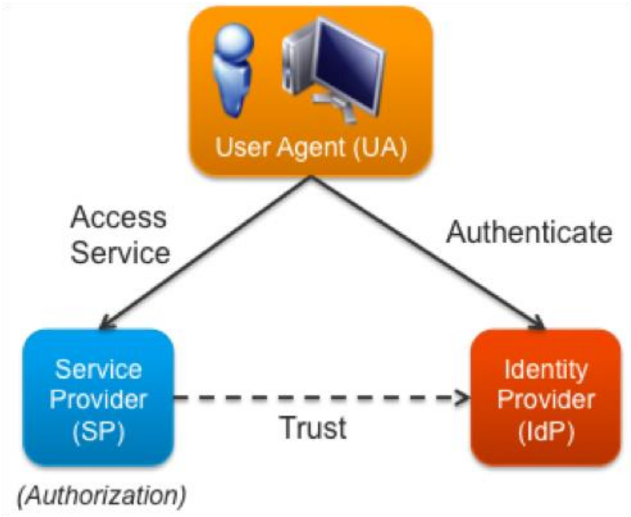
Web applications with no passwords are virtually impossible to steal, as the user must authenticate against an enterprise-class IdM first that can include strong authentication mechanisms.

IT Friendly

SAML simplifies life for IT because it centralizes authentication, provides greater visibility and makes directory integration easier.

2.2 Roles, Components and Scenarios

SAML, Security Assertion Markup Language is an OASIS standard for exchanging Authentication and Authorization user data between security domains. The idea being that users authenticate with their identity provider (IdP) in their domain (e.g., Active Directory) once, and SAML 2.0 authenticates their credentials across one or more service providers (SP) (e.g., applications, web sites or services) like the BrandMaker application, without having to log in again and again. SAML 2.0 handles the trust between the service providers (SP) and identity providers (IdP) using certificates and passes information about the users from the identity provider to the service providers as part of the SSO process.



In addition, SAML 2.0 can pass detailed information about the users as part of the SSO process, which can enable automatic provisioning of new users in your applications. Basically, if this is the first time a user accesses your application, and they have the proper authorization (e.g., roles) you can automatically provision a new account for them.

Components

The two main components of a SAML landscape are:

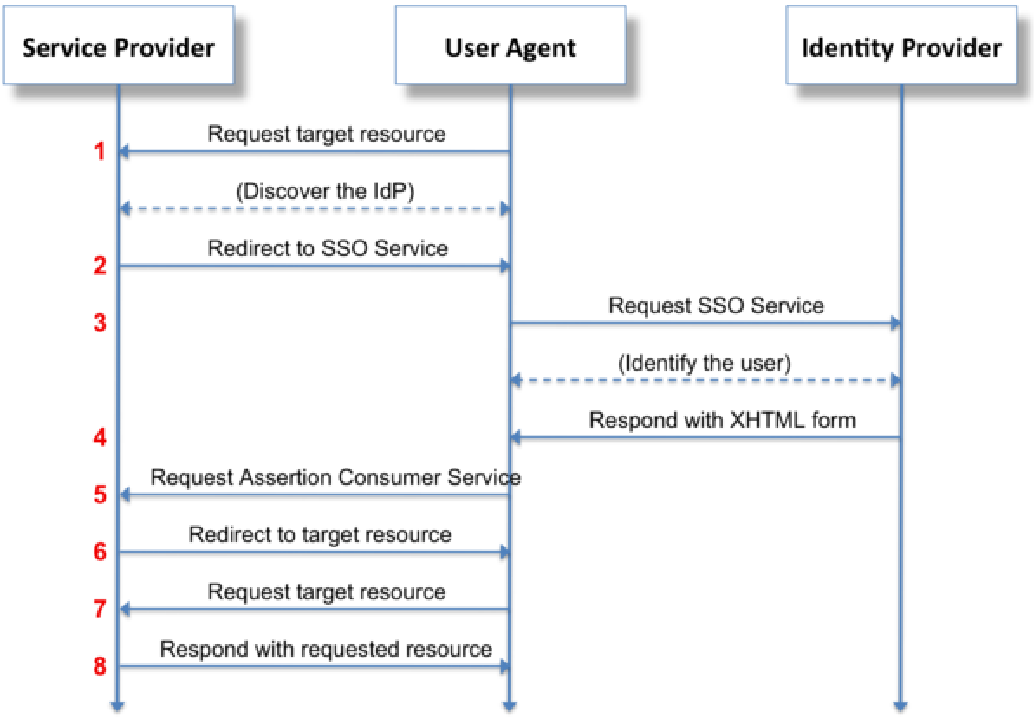
Service provider (SP) – like the BrandMaker application
The service provider is a system entity that provides a set of web applications with a common session management, identity management, and trust management.

Identity provider (IdP) – like Microsoft Active Directory Federation service
The identity provider is a system entity that manages identity information for principals and provides authentication services to other trusted service providers.

In other words, the service providers outsource the job of authenticating the user to the identity provider. The identity provider maintains the list of service providers where the user is logged in and is able to pass requests on logout to those service providers. The client that is trying to access the resource must be HTTP-compliant.

2.3 User SSO Login Flow With SAML

The primary SAML use case is called Web Browser Single Sign-On (SSO). A user wielding a user agent (usually a web browser) requests a web resource protected by a SAML service provider. The service provider (like the BrandMaker application), wishing to know the identity of the requesting user, issues an authentication request to a SAML identity provider through the user agent. The resulting protocol flow is depicted in the following diagram. (Source: Wikipedia)



The user may experience three different main scenarios:

Case 1: Already logged in at the SP

In case the user has already used the browser to authenticate himself/herself at the identity provider (IdP) and was taken into the BrandMaker application, a new session is not needed at all. Without any additional interaction with or redirection to the IdP the user reaches immediately the requested page.

Case 2a: Not logged in at the SP but already authenticated against the IdP

In case the user has already used his browser to authenticate himself at the identity provider (IdP) e.g. by using another web application, he or she just must click the *One-Click Login* button. This issues a new SAML assertion and the user gets automatically logged into the BrandMaker application without any additional interaction. He or she reaches immediately the requested page.

Case 2b: Not logged in at the SP but remembered and already authenticated against the IdP

In case the user has already used his browser to authenticate himself/herself at the identity provider (IdP) e.g. by using another web application, and the user has chosen the SSO solution for the last log-in into the BrandMaker application, then the system remembers him. The system issues a new SAML assertion and the user gets automatically logged into the BrandMaker application without any additional interaction. The user reaches immediately the requested page.

Case 3: Not authenticated against the IdP

Independently of the status at the SP, when the user arrives at the IdP for authentication, it depends on the system possibilities if the user is recognized as a known user so that the IdP can instantly authenticate him/her. In that case the user is taken to the BrandMaker application SP without any additional interaction and reaches immediately the requested page.

3 Prerequisites & Constraints

3.1 Prerequisites

- The BrandMaker application of the current version or above with SSL certificate (HTTPS).
- Identity provider supporting SAML 1.x or 2.0 in your landscape.

Note: SAML 1.x does not support all features and security mechanisms of SAML 2.0.
We recommend SAML 2.0 therefore.

3.2 Constraints

- The BrandMaker application cannot be used as identity provider.
- The BrandMaker application Web Services (API) does not support SAML.
- The BrandMaker application does not support WS-Trust Security Token Service.
- The BrandMaker application supports SP-initiated and IdP-initiated scenarios.
- The BrandMaker application introduces basic support for multiple IdPs starting with version 5.9.

3.2.1 Supported Identity Providers

As SAML is an open-standard data format, every SAML identity provider should work. BrandMaker systems use Microsoft ADFS 2.0, pingone.com, salesforce.com and Novell NetIQ.

3.3 Identity Provider Landscape

Use the following table with links to information about some identity provider solutions supporting SAML 2.0:

Solution	More information
CA Technologies	CA SiteMinder Federation Security Services Guide
Microsoft Active Directory Federation Services (AD FS)	Active Directory Federation Services - Overview Active Directory Federation Services - Troubleshooting Active Directory Federation Services - TechnNet Article Configuring ADFS 2.0 to Communicate with SAML 2.0 Configure ADFS 2.0 Integration with SharePoint 2013 on Windows Server 2008 R2
OneLogin	SAML - Secure Single Sign-On (SSO) Protocol
Ping Identity	PingFederate 7.3 Documentation PingFederate 6.1 Documentation
Salesforce.com	Enable Salesforce as an identity provider Salesforce as identity provider
SecureAuth	SecureAuth IdP
many more	…

4 Setup the BrandMaker Application as SAML Service Provider

To get single sign-on up and running using SAML, three steps have to be executed:

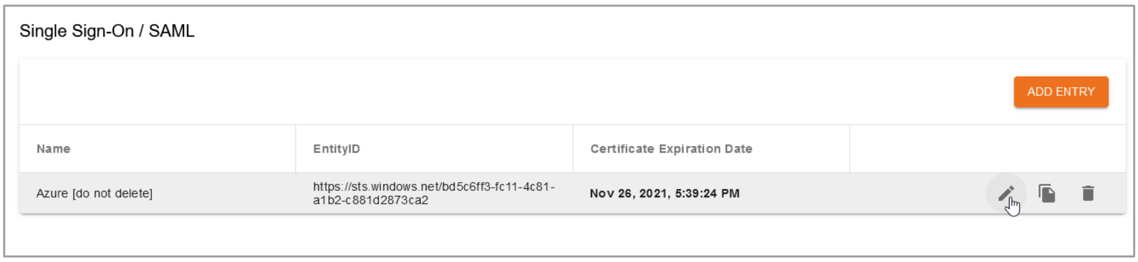
- Configure your identity provider as authentication service for the BrandMaker application, see chapter 3.3 Identity Provider Landscape, chapter 5 Example: Microsoft Active Directory Federation Service as SAML Identity Provider and chapter 6 Example: Salesforce as SAML identity provider.
- Configure identity attribute mappings between your IdP and the BrandMaker application, see chapter 4.2 Supported Attributes.
- Configure the BrandMaker application as service provider, see this chapter.

4.1 Configure the BrandMaker Application

To configure the BrandMaker application as service provider, log in with administrator rights.

4.1.1 Configuration of the Identity Providers

1. Click > *Administration* > *System Configuration* > *Single Sign-On / SAML*.

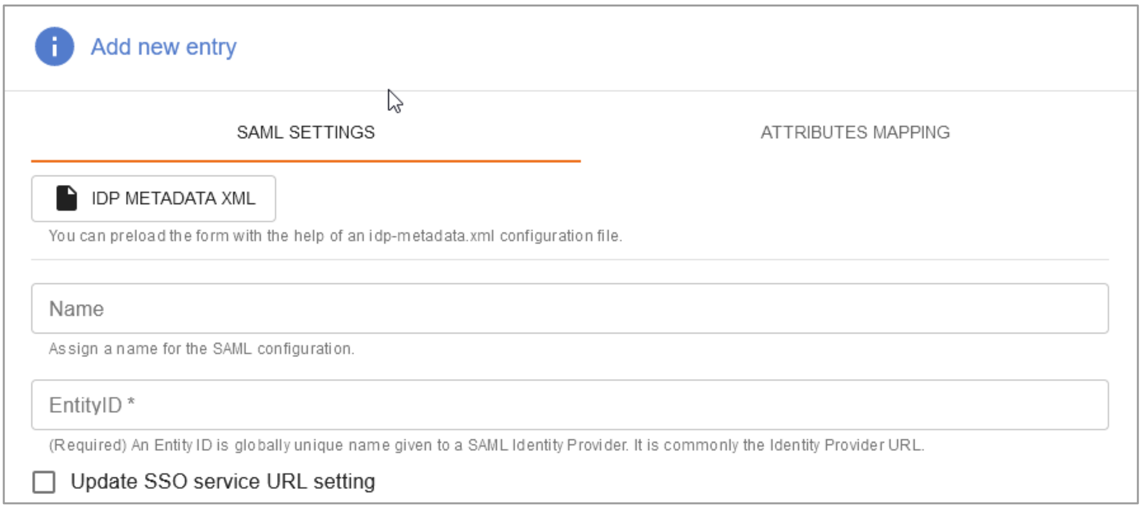


Single Sign-On / SAML

Name	EntityID	Certificate Expiration Date
Azure [do not delete]	https://sts.windows.net/bd5c6ff3-fc11-4c81-a1b2-c881d2873ca2	Nov 26, 2021, 5:39:24 PM

In the case that there is an existing configuration you see a grid as shown above.

2. Click > *Create* to create a new configuration for an additional identity provider.



Add new entry

You can preload the form with the help of an idp-metadata.xml configuration file.

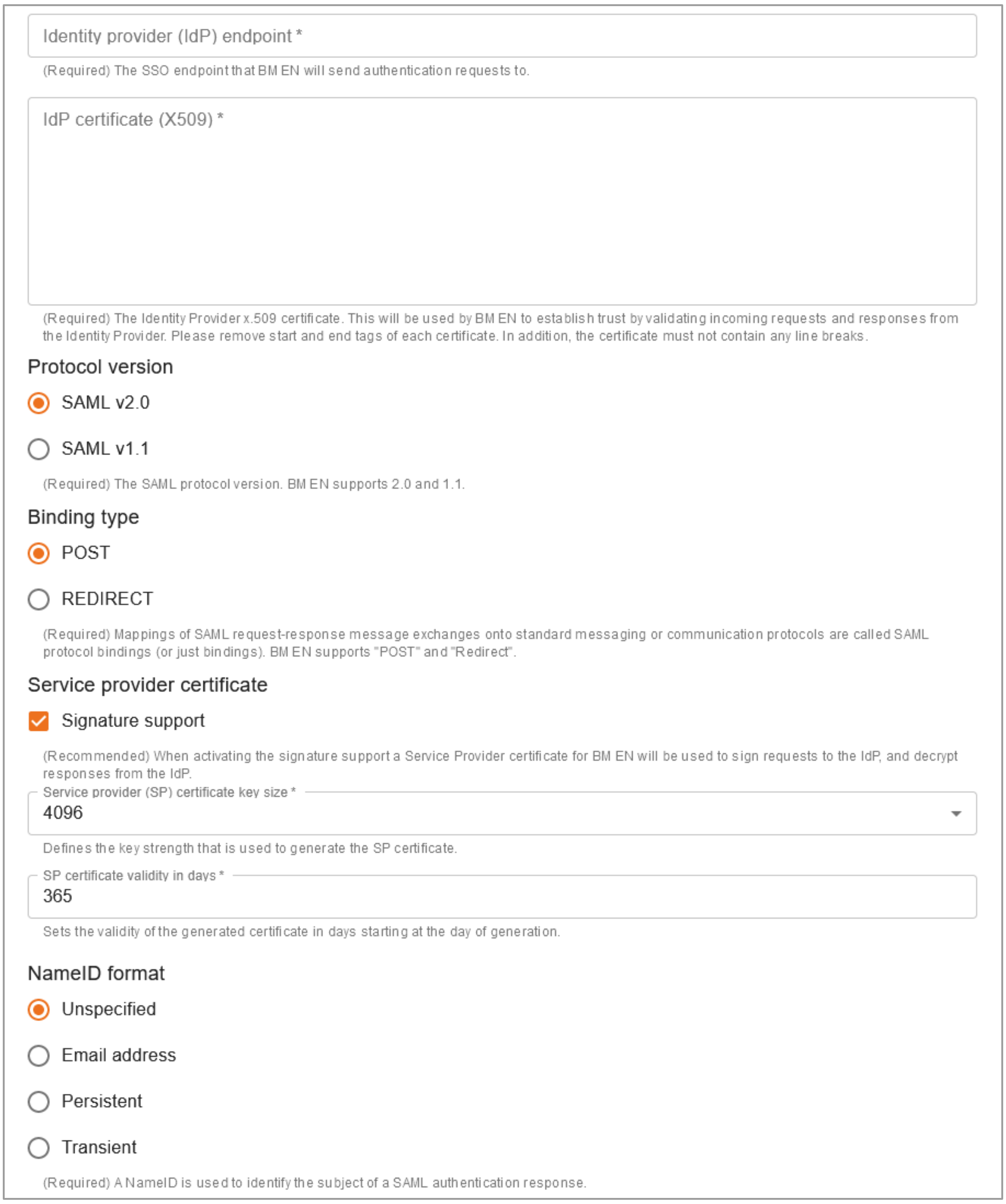
Name

Assign a name for the SAML configuration.

EntityID *

(Required) An Entity ID is globally unique name given to a SAML Identity Provider. It is commonly the Identity Provider URL.

□ Update SSO service URL setting



Identity provider (IdP) endpoint *

(Required) The SSO endpoint that BM EN will send authentication requests to.

IdP certificate (X509) *

(Required) The Identity Provider x.509 certificate. This will be used by BM EN to establish trust by validating incoming requests and responses from the Identity Provider. Please remove start and end tags of each certificate. In addition, the certificate must not contain any line breaks.

Protocol version

● SAML v2.0

○ SAML v1.1

(Required) The SAML protocol version. BM EN supports 2.0 and 1.1.

Binding type

● POST

○ REDIRECT

(Required) Mappings of SAML request-response message exchanges onto standard messaging or communication protocols are called SAML protocol bindings (or just bindings). BM EN supports "POST" and "Redirect".

Service provider certificate

☑ Signature support

(Recommended) When activating the signature support a Service Provider certificate for BM EN will be used to sign requests to the IdP, and decrypt responses from the IdP.

Service provider (SP) certificate key size *
4096

Defines the key strength that is used to generate the SP certificate.

SP certificate validity in days *
365

Sets the validity of the generated certificate in days starting at the day of generation.

NameID format

● Unspecified

○ Email address

○ Persistent

○ Transient

(Required) A NameID is used to identify the subject of a SAML authentication response.

3. Select the metadata file you exported on the IdP side to automate the partner setup or fill in the given fields resp. Select the appropriate options.

   Please note that the automated population of the form field requires a meta data XML file and not a PEM or CRT file.

> **Note:** The needed settings depend on the setup of your identity provider.

4. The configuration can get an optional name to identify it easily in the overview of the single sign-on configurations. For example the name could be “Test connection” if you want to differentiate between test and live configurations.

5. With checking the box *Update SSO service URL setting* the respective setting *Administration: SSO service URL* which is part of the settings table does not need to be changed manually (see chapter 4.1.4.2 Enable One-Click Login Button on Login Page). Please note that the setting is overwritten every time the box is checked and the form is saved.

6. After you selected and configured the required settings, press the *Save* button.

Now the BrandMaker application is configured as a service provider for SSO using SAML.

> **Note:** In case of changes of the IdP configuration you may need to update your BrandMaker application SAML configuration as well.

4.1.1.1 Data for Identity Provider Configuration

Two links appear on the configuration page:

- *Download metadata of Service Provider*
  Download link for the entire configuration data in xml format incl. the SP certificate. The metadata are automatically updated on saved changes.
- *Download certificate of Service Provider*
  Download link for the SP certificate in PEM format.
  Required just for some IdP vendors.

The next step is to set up your service provider with the necessary fundamental objects followed by configuring the identity provider system to cooperate with (and trust) the BrandMaker application and to configure the user attribute mappings.

4.1.2 Configuration of Necessary Rights, Roles, and Groups

The access control to assets, Web-to-Publish documents and other related parts of the BrandMaker application is done via different mechanisms. Therefore, the user needs to have defined (module) roles and be part of specific groups. Among others they are shown in Figure 1: BrandMaker application access controls.

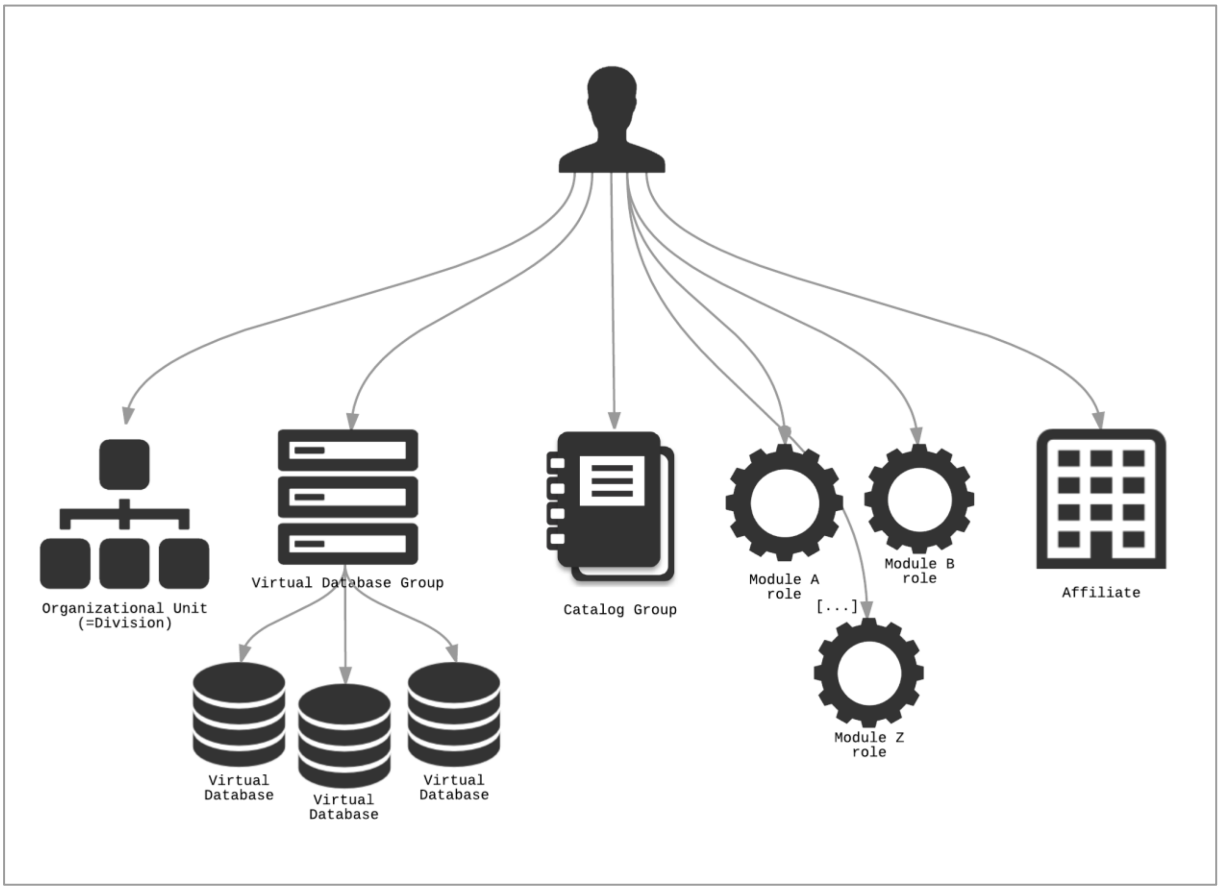


Figure 1: BrandMaker application access controls

Most of these relations are indirectly established via Single Sign-On (SSO) Groups and controlled by the *SAML_SSO_GROUP* parameter but some can be set directly with specific parameters. For the complete list of supported parameters please refer to chapter 4.2 Supported Attributes.

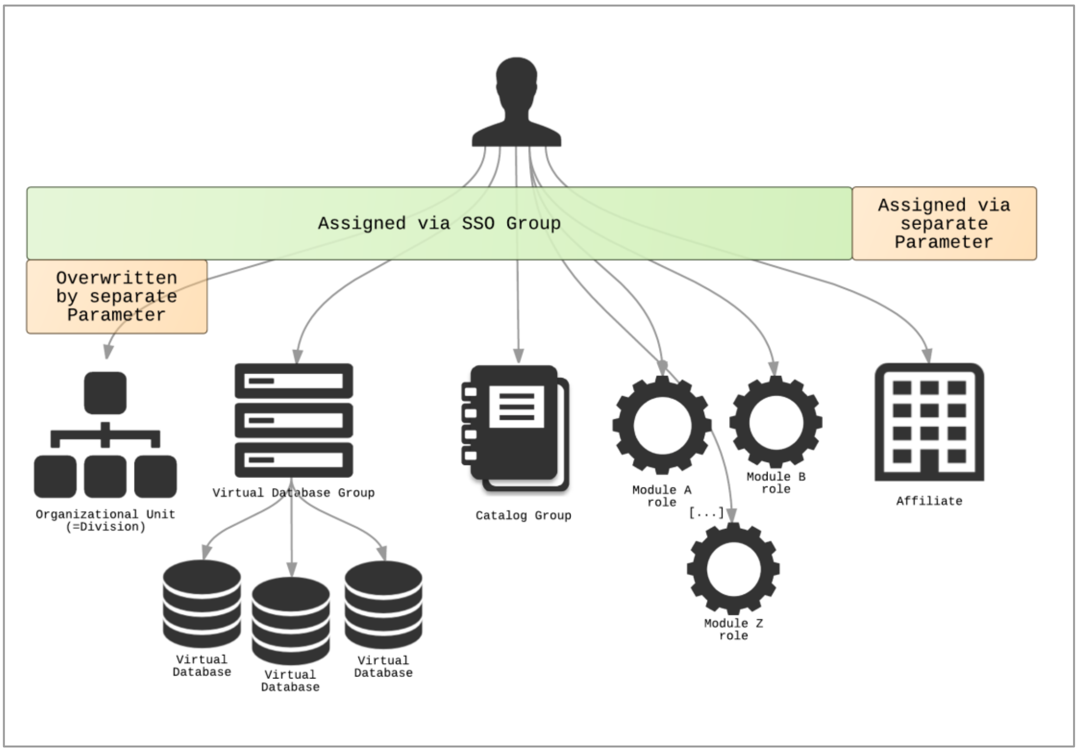


Figure 2: Single Sign-On parameters controlling the BrandMaker application access controls

Note: For detailed instructions about how to maintain SSO groups please refer to chapter 2.4 of the general *Administration Manual*.

Users who have no valid group name information are either rejected or logged in using a configurable default SSO group. That behavior can be adjusted by the setting *Administration: SSO group match*.

To be correct here users are actually not “assigned” to SSO groups inside the BrandMaker application. These groups act more like some kind of template for the other linked objects, like roles, virtual database groups, organizational units or catalog groups. Whenever you change a SSO group, it does not directly affect any existing user.

Next to this there are two crucial parameters that control the persistence of users in the BrandMaker application - *SAML_CREATE_USER* and *SAML_UPDATE_USER*.

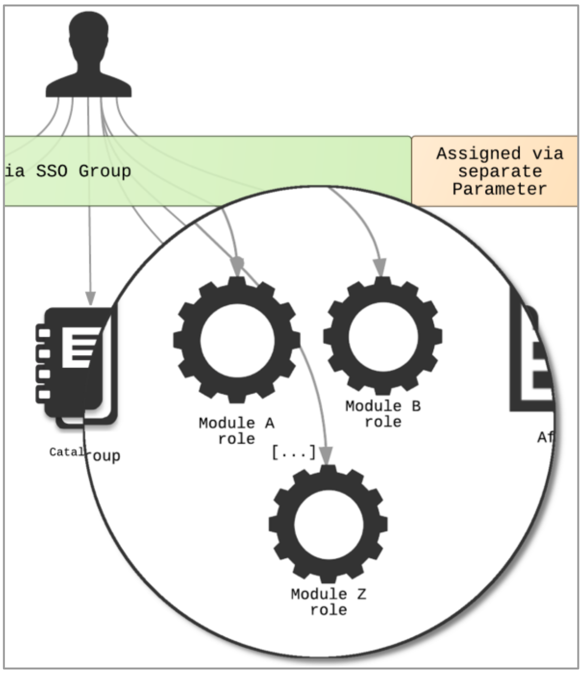
If the parameter *SAML_CREATE_USER* is set to true, it is checked if the user account already exists, means if a login name matches the value of *SAML_USERNAME*. If the user account does not exist yet, it is checked if all mandatory information is given and in that case the user account is created automatically. If the user account exists, all given parameters are updated.

SAML_UPDATE_USER on the other hand just updates an existing user account and the process fails in the case of a missing *SAML_CREATE_USER* for non-existent user accounts; so *SAML_CREATE_USER* includes *SAML_UPDATE_USER.* This can be useful if you want to avoid the generation of new user accounts via SAML.

Note: For detailed instructions about how to maintain SSO groups please refer to chapter 2.4 of the general *Administration Manual*.

4.1.2.1 Roles

Module roles are indirectly assigned to the user via SSO groups. You cannot set them directly via SAML.



Note: For detailed instructions about how to maintain module roles please refer to chapter 3.4 of the general *Administration Manual*.

Please note that for the BrandMaker application, one user can only have one role assignment per module. If multiple groups are defined for one user, they are processed sequentially, beginning with the first, then the second etc. in their sequence of the *SAML_SSO_GROUP* parameter. For each group the defined roles are assigned to the user. If another role was assigned for the same module previously, the assignment is overwritten by the most recent assignment in the parameter sequence. A complete example of how this process looks like can be found in Figure 3: Complete processing example for multiple SSO groups.

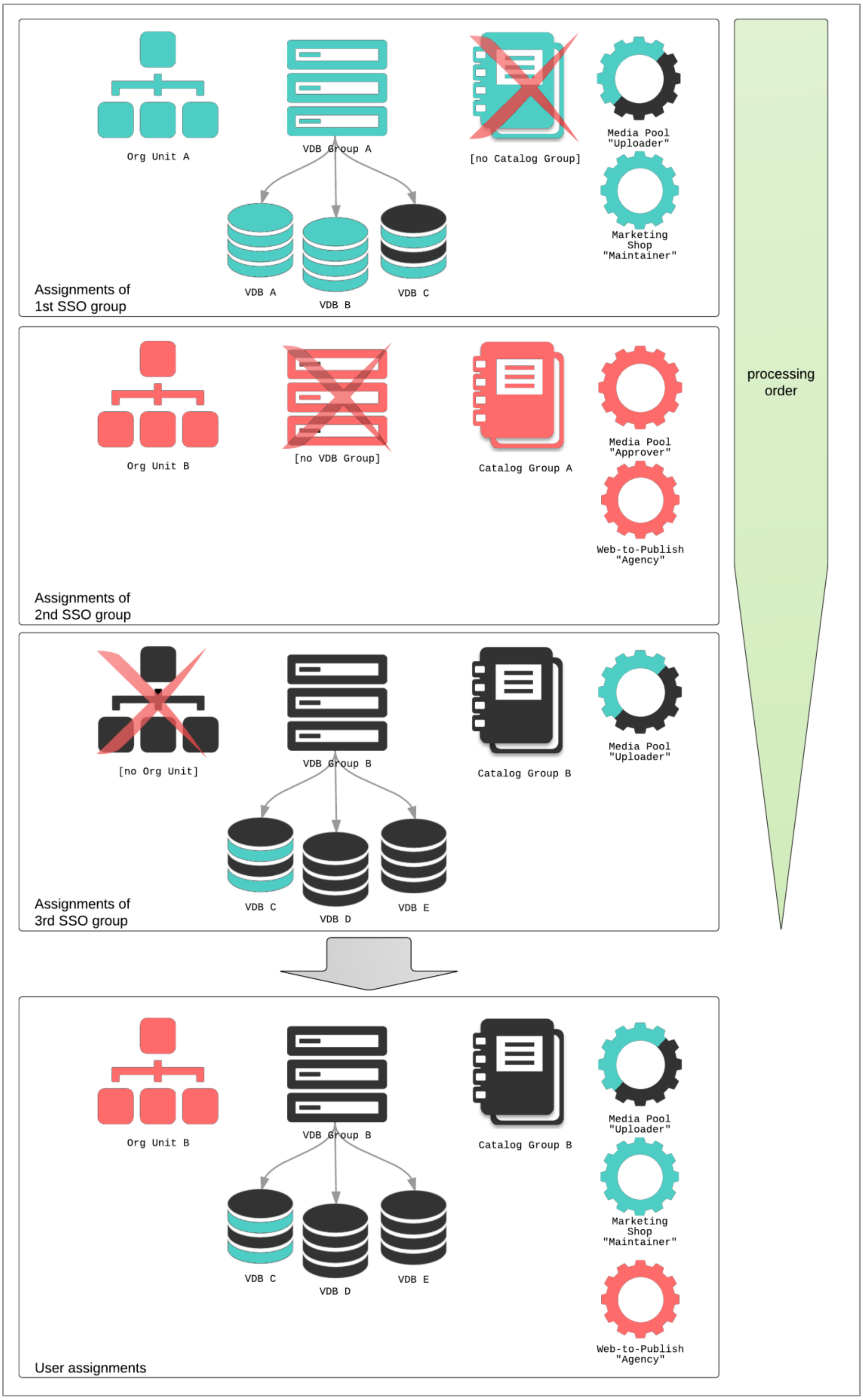
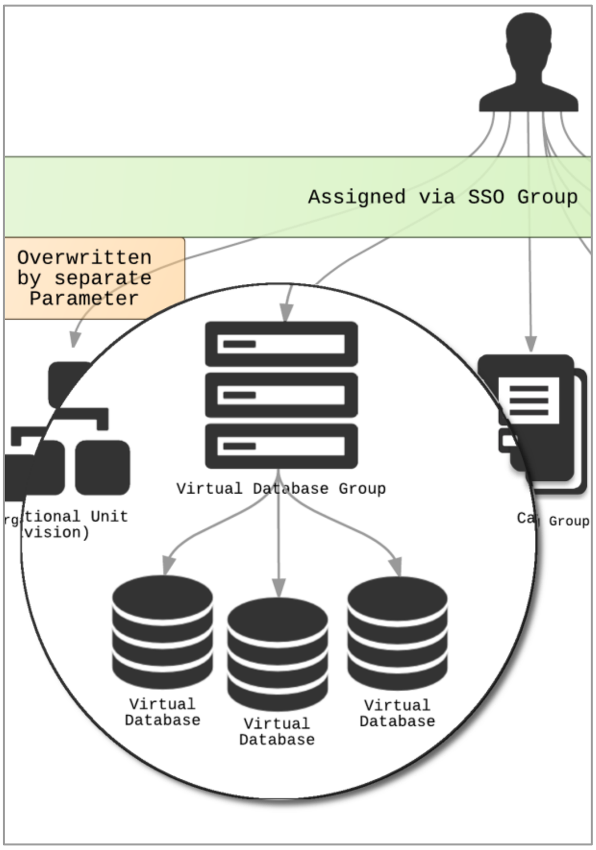


Figure 3: Complete processing example for multiple SSO groups

4.1.2.2 *Virtual Databases*

Virtual Databases are assigned with the help of Virtual Database groups.



Note: For detailed instructions about how to maintain module roles please refer to chapter 3.1 and 3.2 of the general *Administration Manual*.

Please note that for the BrandMaker application, one user can only have one VDB group. VDB groups are assigned indirectly via *SAML_SSO_GROUP* parameter and the processing is equal to the one for the module roles. For each group the defined VDB group is assigned to the user. If another VDB group was assigned previously, the assignment is overwritten by the most recent assignment in the parameter sequence. Please check Figure 3: Complete processing example for multiple SSO groups again.

With the setting *Administration: VDB group auto-generation* you find one specialty. When this setting is activated the system automatically generates new VDB groups based on given VDBs (via *SAML_SSO_GROUP* → VDB groups) as shown in in the following figure.

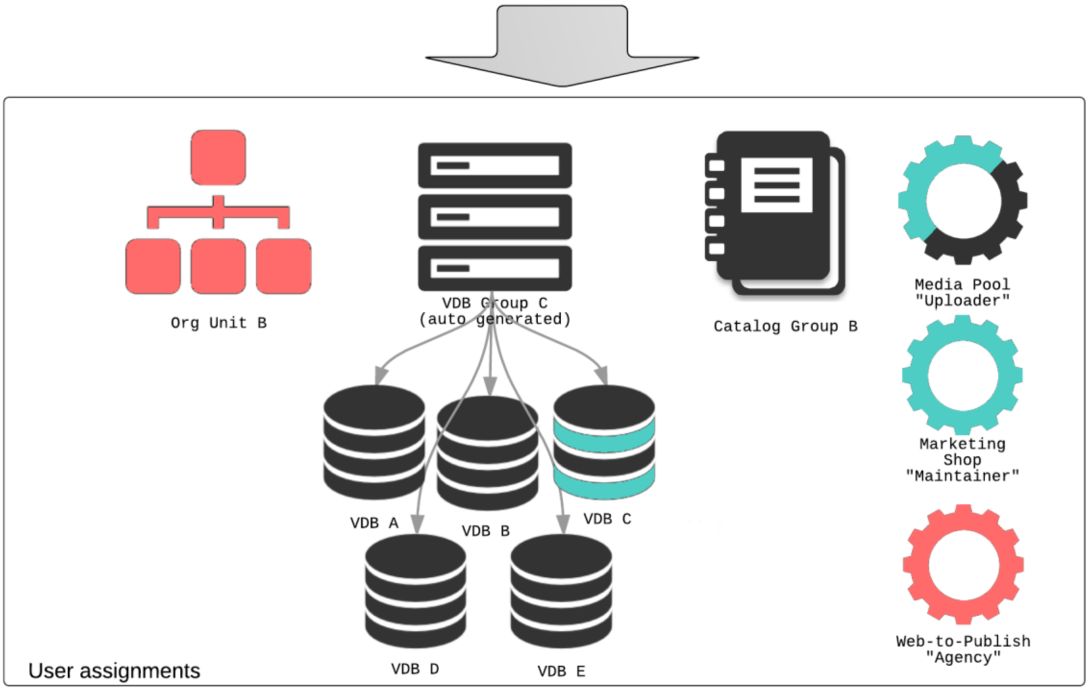
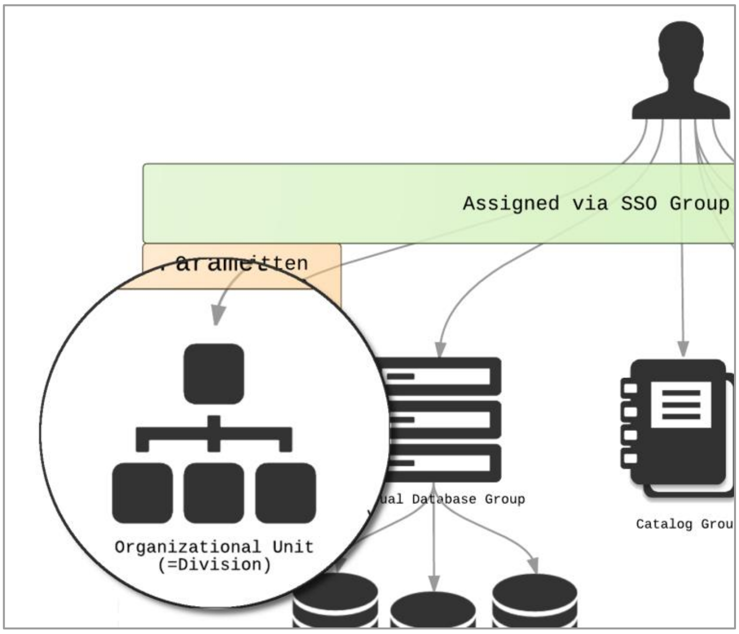


Figure 4: Auto-generated VDB group

But before the generation the system checks whether a VDB group exists holding exactly the wanted set of all the VDBs. In this case it is assigned to the user.

4.1.2.3 Organizational Unit

> **Note:** *Division* is the old identifier for *organizational unit* and for backwards compatibility still used in some places.

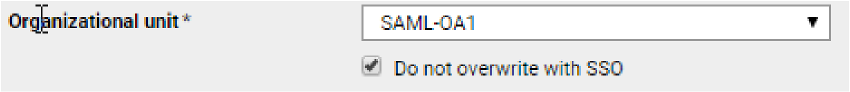


Every user has to have exactly one organizational unit. It can either be assigned with the help of the given SSO groups or directly in the *SAML_OVERRIDE_ORGUNIT* parameter whereby the separate

parameter outweighs the mapping in the SSO group.
As for the VDB group, the assignment is overwritten by the most recent assignment in the parameter sequence. Please check Figure 3: Complete processing example for multiple SSO groups for reference again.

If an organizational unit name is given that does not exist yet, then the organizational unit is created automatically. The attribute *SSO-Key* of the organizational unit is relevant for the identification.

You can protect the organizational unit assignment for existing users from being overwritten by following logins. This needs to be done in the user administration as shown in the next figure. Please be aware that this protection is limited to organizational units.



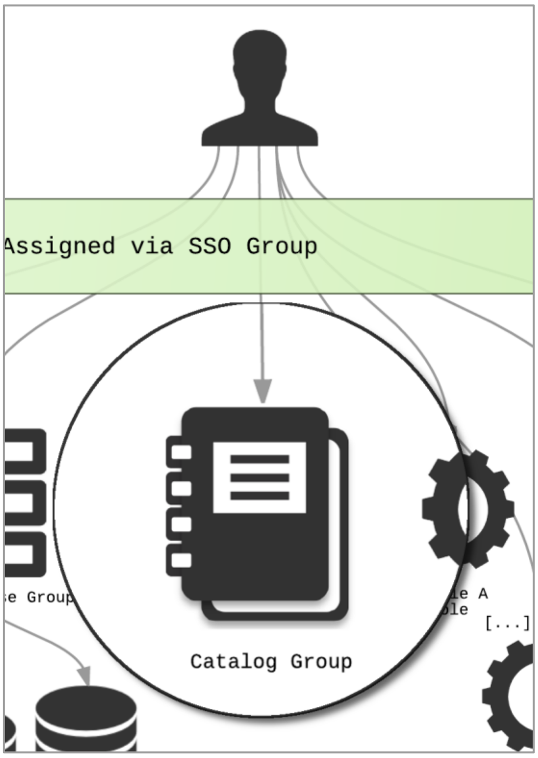
Organizational unit * SAML-OA1 ▼

☑ Do not overwrite with SSO

Note: For detailed instructions about how to maintain organizational units please refer to chapter 3.3 of the general *Administration Manual*.

4.1.2.4 Catalog Groups

Catalog groups are used only by the BrandMaker Marketing Shop module to restrict access to specific articles and catalogs.



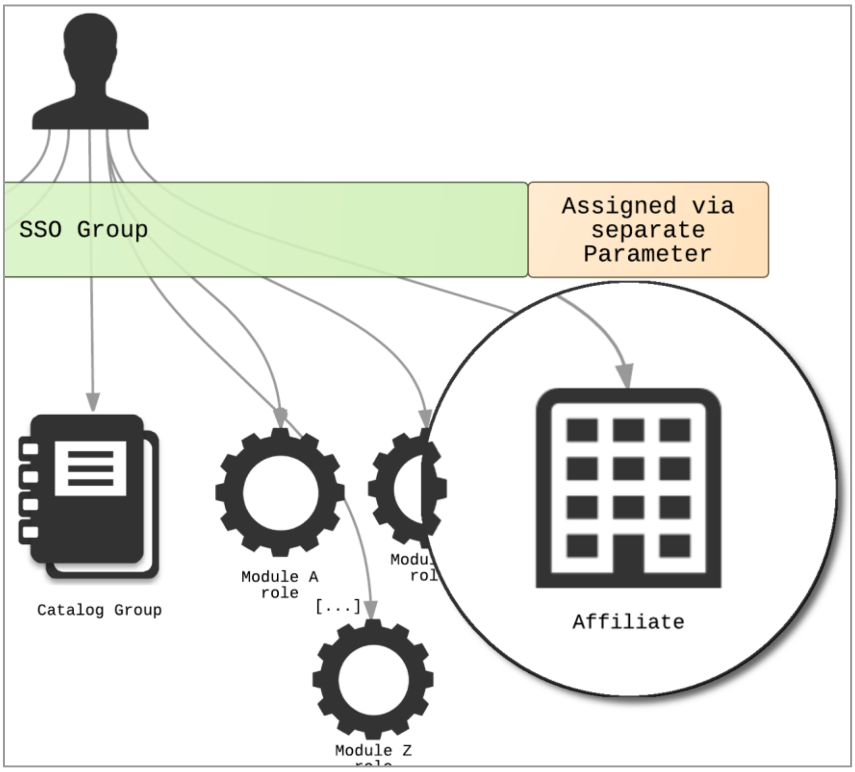
Note: For detailed instructions about how to maintain Catalog Groups please refer to chapter 9.1 of the general *Marketing Shop Administration Manual*.

4.1.2.5 *Affiliates*

Note: *BLZ* is the old identifier for (selected) affiliate and for backwards compatibility still used in some places.

You can only assign affiliates directly via *SAML_AFFILIATEID* parameter. It can be a single value or multiple values separated by commas.

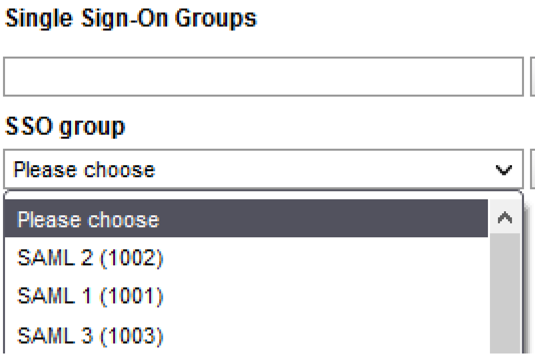
If the user already has a (selected) affiliate set, which is not in that given list, the assignment is going to be dropped. If the list contains only one affiliate id, this id is chosen for both attributes, *selected* and *alternative*.



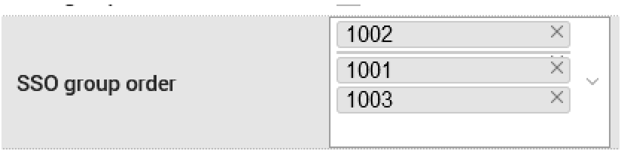
During the processing each value from the list is evaluated against the regular expression defined in *Administration: Affiliate ID validation* and dropped in the case of a mismatch.

4.1.3 Sorting of SSO groups

An administrator can define the prioritization of SSO groups when logging in via SSO. For this purpose, the ID of the group is now displayed behind each SSO group name under > *Administration* > *User & Groups* > *Single-Sign-On Groups*. The administrator can enter these IDs as a comma-separated list in the new system setting SSO group order.



The setting *Administration: SSO group order* can be found in *> Administration > System Configuration > System Settings.*



SSO group order: 1002, 1001, 1003

Enter a comma-separated list of SSO group IDs. Once an ID is entered, SSO groups are prioritized according to the IDs when logging in via SSO. The SSO group ID that is on the first position is taken as first, the SSO group ID on the last position is applied as the last one to the user.

If the system setting is empty, the functionality is disabled.

4.1.4 System Configuration and Tweaks for User Guidance

4.1.4.1 Automatic Redirection of all Users to the IdP

In the case you want to support single sign-on as the only way to access the system you can redirect every user automatically from the login page the identity provider.
You can activate this with the setting *Administration: SSO service.* Additionally, you have the possibility to restrict this redirection to specific IP addresses via *Administration: SSO service IP addresses.*

> **Note:** There's no way to manually log into the system now – even not for the BrandMaker support team. In the case you need help, you have to (temporarily) disable this behavior again.

4.1.4.2 Enable One-Click Login Button on Login Page

Two additional settings need to be done, to display the *One-Click Login* button on the login page to allow SP initiated SAML assertions to one IdP:

1. Click > Administration > System Configuration > System Settings.
2. Edit the following settings:

- *Administration: SSO button SSO*: Set it to *activated*.
  Turn the login form on the login page on or off. The login form consists of the fields User name and Password, as well as the button Login.
- *Administration: SSO service URL*: Enter the URL of the authentication service.
  Set URL to:
  https://yourcompany.brandmaker.com/secure/saml.do?issuer=[configuration name / entityId]

Note: The setting *Administration: SSO service URL* can be set automatically with saving the SAML configuration (see chapter 4.1.1 Configuration of the Identity Providers, step 5).

The *One-Click Login* button is enabled for the chosen IdP.

4.1.4.3 Special Treatment of Particular User Information

With the following settings you can influence the particular behavior in different ways. Please check the respective setting descriptions in the BrandMaker application.

- *Administration: SSO email update mode*

  Select the update mode for the email address if SSO is used to update the user data:
  Do not update - The email address is not updated.
  Fill empty - The email address is updated if no address is entered.
  Overwrite - The email address is always updated.
- *Administration: SSO email verification*

  Turn email verification on or off. If verification is turned on, the user has to confirm the submitted email address.
- *Administration: SSO email address syntax check*

  Turn the syntax check for email addresses on or off for login via SSO.

4.1.4.4 Module-Specific Role Assignment (Override Functionality)

With the possibility to override single module roles which were set by *SAML_SSO_GROUP* (and corresponding by the Single-Sign-on Groups in the system) BrandMaker offers a second way of assigning module roles via SAML.

One way is the assignment of the attribute *SAML_SSO_GROUP* which hands over one role for the entire system, which then can be configured via > *Administration* > *Users & Groups* > *Single Sign-On Groups*. For every Single Sign-On Group the set of module roles can be configured.

The second way is the module specific assignment of roles. This makes it possible to assign a separate role combinatorics for each user and to perform these completely outside the BrandMaker system. So, the roles that are configured in a Single Sign-On Group which is set via *SAML_SSO_GROUP* can be overridden by the following attributes:

Media Pool:	SAML_OVERRIDE_MEDIAPOOL_ROLE
Web-to-Publish:	SAML_OVERRIDE_W2P_ROLE

Administration:	SAML_OVERRIDE_ADMIN_ROLE
Smart Access:	SAML_OVERRIDE_SMARTACCESS_ROLE
Marketing Shop:	SAML_OVERRIDE_SHOP_ROLE
Marketing PIM:	SAML_OVERRIDE_PIM_ROLE
Job Manager:	SAML_OVERRIDE_JOBMANAGER_ROLE
Brand Management Portal:	SAML_OVERRIDE_PORTAL_ROLE
Event Manager:	SAML_OVERRIDE_EVENTMGR_ROLE
Review Manager:	SAML_OVERRIDE_REVIEWMGR_ROLE
DMC:	SAML_OVERRIDE_DMC_ROLE
SEW:	SAML_OVERRIDE_SEW_ROLE
Reporting Center.	SAML_OVERRIDE_REPORTINGCTR_ROLE
Language Center:	SAML_OVERRIDE_LC_ROLE

Marketing Planner requires group-role-pairs to control the access to the module's functionalities. It is possible to assign more than of these pairs. Therefore, the attribute *SAML_ADD_MAPS_ROLE* allows adding group-role-pairs to the ones which were set by *SAML_SSO_GROUP* without overriding existing ones. Whereas, the attribute *SAML_OVERRIDE_MAPS_ROLE* overrides existing group-role-pairs with the ones set by this attribute.

The two Marketing Planner attributes should be in the following format:

```
[Group01] – [Role01]; [Group02] – [Role02]; [Group03] – [Role03]…
```

Moreover, the following attributes allow overriding access control variables which are also set by *SAML_SSO_GROUP*:

- SAML_OVERRIDE_VDBGROUP
- SAML_OVERRIDE_ORGUNIT
- SAML_OVERRIDE_CATALOGGROUP
- SAML_OVERRIDE_LOGIN_AS_USER

In case module role which is set via the attribute *SAML_SSO_GROUP* and the corresponding Single Sign-On Group should be removed the overriding attribute needs to have *[%NULL%]* as value.

4.1.4.5 Generic User Attributes

You can set generic user attributes. The names of the attributes can be chosen freely and they can be set via SSO via SAML and are so a part of the user object in the application.

Other modules, such as Marketing Shop, can then consume these attributes for their workflows. It is completely in the hands of the system administrator which attributes are created.

Marketing Shop can use an attribute for the cost center of a customer during an order process. To map the SAML attribute and the cost center in Marketing Shop it is necessary to set the setting *Marketing Shop: Unique name of cost center at the generic user attributes* (or with its technical name: *COST_CENTER_ATTRIBUTE_NAME*) according to the value that is sent via SAML.

These generic attributes require to new SAML attributes:

SAML_ADD_GENERIC_ATTRIBUTES can be used to add attributes to already existing ones.

```
{"Cost_center":"0013021","Billability":"False"}
```

Whereas *SAML_GENERIC_ATTRIBUTES* can be used to completely override the existing generic attributes of a user.

```
{"Cost_center":"0013021","Billability":"False"}
```

Note: The name of a generic attribute can be chosen freely and is case sensitive.

4.2 Supported Attributes

Below all attributes are enlisted that are supported by the BrandMaker application.

Note: To identify BrandMaker application users, the BrandMaker SAML endpoint requires custom attributes to be included in the SAML assertion of the IdP.
The mandatory attributes are marked with (*)!

BrandMaker application users derive their rights and roles from the configured SSO groups, therefore it is important to carefully setup and name the groups and organizational units.

It is important that on both sides, the BrandMaker application and the IdP, the attributes have the exact name. Otherwise the values cannot be mapped successfully.

Note: In case the attribute names on the IdP cannot be changed or IT administrators would create an attribute with redundant data, it is possible that the attribute names are mapped with the ones of the BrandMaker application (see chapter 4.3 Mapping of Custom Attribute Names). BrandMaker consultants can help to identify a good and working structure and can help to configure the BrandMaker application SSO groups and roles.

Note: The attribute mapping configuration at IdP side cannot be done by a BrandMaker consultant on his own. A good understanding how to configure the user authentication system as an IdP using SAML is needed as well – as the configuration steps are vendor specific. Therefore, we recommend an IT administrator is setting up the configuration and the user attribute mapping.

Please keep in mind that all attribute names are case sensitive. This also holds true for the most attribute values especially Boolean values.

Attribute name (case sensitive)	**Type**	**Value** (case sensitive)	**Max. chars**	**Description**
*SAML_USERNAME**	Literal	IdP mapping	vchar255	Login name of the user.
SAML_FIRST_NAME	Literal	IdP mapping	vchar255	First name of the user.
SAML_LAST_NAME	Literal	IdP mapping	vchar255	Last name of the user.
*SAML_CREATE_USER**	Boolean	true, false	vchar255	true: User created if mandatory values provided. false: User not created. See chapter 4.1.2 for details.
*SAML_UPDATE_USER**	Boolean	true, false	-	true: User updated if existing. false: User not updated if *SAML_CREATE_USER* not set or false. See chapter 4.1.2 for details.
*SAML_SSO_GROUP**	Literal	IdP mapping	vchar255	Defines Single Sign-On Groups that are used to assign the roles, virtual databases, organizational unit and other related objects to the user. This assignment can be changed as often as necessary—for existing or new users. Multiple SSO-groups can be provided at once. **Note:** Be aware that the order of the given SSO groups matters.
SAML_SUPPLIER	Literal	IdP mapping	vchar255	Name of the supplier which needs to be filled with values that are existing as supplier companies in Shop.
SAML_FUNCTION	Literal	IdP mapping	vchar255	Defines user's function which is part of the user profile.
SAML_AFFILIATEID	Literal	IdP mapping	vchar255	Affiliate ID. Multiple affiliate IDs separated by "," are supported. **Note:** In the case of multiple affiliate IDs, none of them is set as the active affiliate. The user has to choose it from *My data* configuration page afterwards.

Attribute name (case sensitive)	Type	Value (case sensitive)	Max. chars	Description
SAML_TYPE	Literal	IdP mapping	vchar255	Type field refers to custom objects of the custom structure "USER_TYPE"
*SAML_EMAIL**	Literal	IdP mapping	vchar255	The email address of the user.
SAML_USER_LANGUAGE	Literal	IdP mapping	vchar255	Code of the language in which the application GUI must be displayed. Example: DE
SAML_GENDER	Literal	IdP mapping	vchar255	Gender of the user (m/f or Male/Female)
SAML_STREET	Literal	IdP mapping	vchar255	Street of user's address. **Note:** The address information is set for all three address types (postal, delivery, invoice) at once.
SAML_STREET_ NUMBER	Literal	IdP mapping	vchar255	Street number of user's address. Use an underscore char ("_") if blanks are necessary. Other characters might get removed or trimmed by the system.
SAML_ZIP	Literal	IdP mapping	vchar255	ZIP code of user's address. Alphanumeric values are possible.
SAML_CITY	Literal	IdP mapping	vchar255	City of user's address.
SAML_ADDRESS_STATE	Literal	IdP mapping	vchar255	State of user's address
SAML_COUNTRY	Literal	IdP mapping	vchar255	Country of user's address.
SAML_OPT_ADDRESS1	Literal	IdP mapping	vchar255	Optional address information
SAML_OPT_ADDRESS2	Literal	IdP mapping	vchar255	Optional address information
SAML_COMPANY	Literal	IdP mapping	vchar255	Name of user's company.
SAML_WORK_PHONE	Literal	IdP mapping	vchar255	Business phone number of the user.
SAML_HOME_PHONE	Literal	IdP mapping	vchar255	Private phone number of the user.
SAML_USER_LABELS	Literal	IdP mapping	vchar255 per label	Label for grouping of users (label1, label2, label3, …)
SAML_MOBILE_PHONE	Literal	IdP mapping	vchar255	Mobile phone number of the user.

Attribute name (case sensitive)	Type	Value (case sensitive)	Max. chars	Description
SAML_ALTERNATE_EMAIL	Literal	IdP mapping	vchar255	Alternative/second email address of the user.
SAML_TITLE	Literal	IdP mapping	vchar255	Title of the user (Prof., Dr., etc.)
SAML_FAX	Literal	IdP mapping	vchar255	Fax number of the user.
SAML_STARTURL	Literal	IdP mapping	vchar255	Can be used for special URL parameters, e.g. a different start page. startURL=/shop/dologin.do **Note:** This start point has the highest priority and overwrites any deep links that users are about to visit.
SAML_PREFERRED_UNIT_OF_LENGTH	Literal	IdP mapping	vchar30	Possible values: mm, cm, inch
SAML_SELECTED_AFFILIATEID	Literal	IdP mapping	vchar255	Selected AffiliateID in UserSettings.do
SAML_USER_TIME_ZONE	Literal	IdP mapping	vchar100	Preferred time zone of the user, for example “Asia/Novosibirsk”
SAML_USER_REGION_ID	Literal	IdP mapping	vchar2	Preferred region id of the user, for example “US”, “DE”
SAML_OVERRIDE_ORGUNIT	Literal	IdP mapping	vchar255	Defines Organizational Unit (Division) to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_VDBGROUP	Literal	IdP mapping	vchar255	Defines VDB Group to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_CATALOGGROUP	Literal	IdP mapping	vchar255	Defines Catalog Group to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_LOGIN_AS_USER	Boolean	true, false	-	true: Admins can log in as this user false: Admins cannot log in as this user **Note:** This overwrites any mapping from the provided SSO groups.

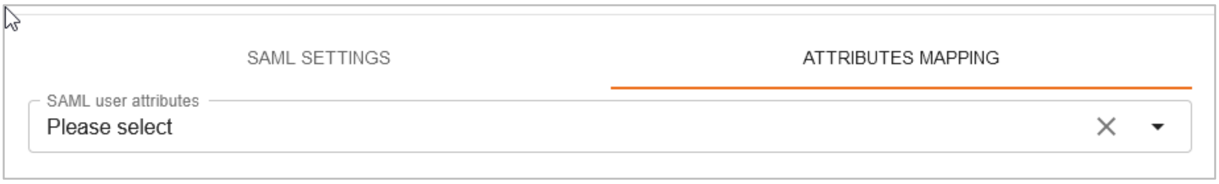
Attribute name (case sensitive)	**Type**	**Value** (case sensitive)	**Max. chars**	**Description**
SAML_OVERRIDE_MEDIAPOOL_ROLE	Literal	IdP mapping	vchar255	Defines Media Pool role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_W2P_ROLE	Literal	IdP mapping	vchar255	Defines Web-to-Publish role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_ADMIN_ROLE	Literal	IdP mapping	vchar255	Defines Administration role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_SMARTACCESS_ROLE	Literal	IdP mapping	vchar255	Defines Smart Access role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_SHOP_ROLE	Literal	IdP mapping	vchar255	Defines Marketing Shop role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_PIM_ROLE	Literal	IdP mapping	vchar255	Defines Marketing PIM role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_JOBMANAGER_ROLE	Literal	IdP mapping	vchar255	Defines Job Manager role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_PORTAL_ROLE	Literal	IdP mapping	vchar255	Defines Brand Management Portal role to which the user is assigned. Note: This overwrites any mapping from the provided SSO groups.

Attribute name (case sensitive)	**Type**	**Value** (case sensitive)	**Max. chars**	**Description**
SAML_ADD_MAPS_ROLE	Literal	IdP mapping	vchar255	Adds a Marketing Planner group-role-pair to the role set to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_MAPS_ROLE	Literal	IdP mapping	vchar255	Overrides Marketing Planner group-role-pairs to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_EVENTMGR_ROLE	Literal	IdP mapping	vchar255	Defines Event Manager role to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_REVIEWMGR_ROLE	Literal	IdP mapping	vchar255	Defines Review Manager role to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_DMC_ROLE	Literal	IdP mapping	vchar255	Defines DMC role to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_SEW_ROLE	Literal	IdP mapping	vchar255	Defines SEW role to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_REPORTINGCTR_ROLE	Literal	IdP mapping	vchar255	Defines Reporting Center role to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.
SAML_OVERRIDE_LC_ROLE	Literal	IdP mapping	vchar255	Defines Language Center role to which the user is assigned. **Note:** This overwrites any mapping from the provided SSO groups.

4.3 Mapping of Custom Attribute Names

In case it is not possible to change the attribute names on the side of the IdP, it is possible to map the names of the BrandMaker application with the ones of the IdP. Therefore there is a separate tab in the configuration of a Single Sign-On configuration.

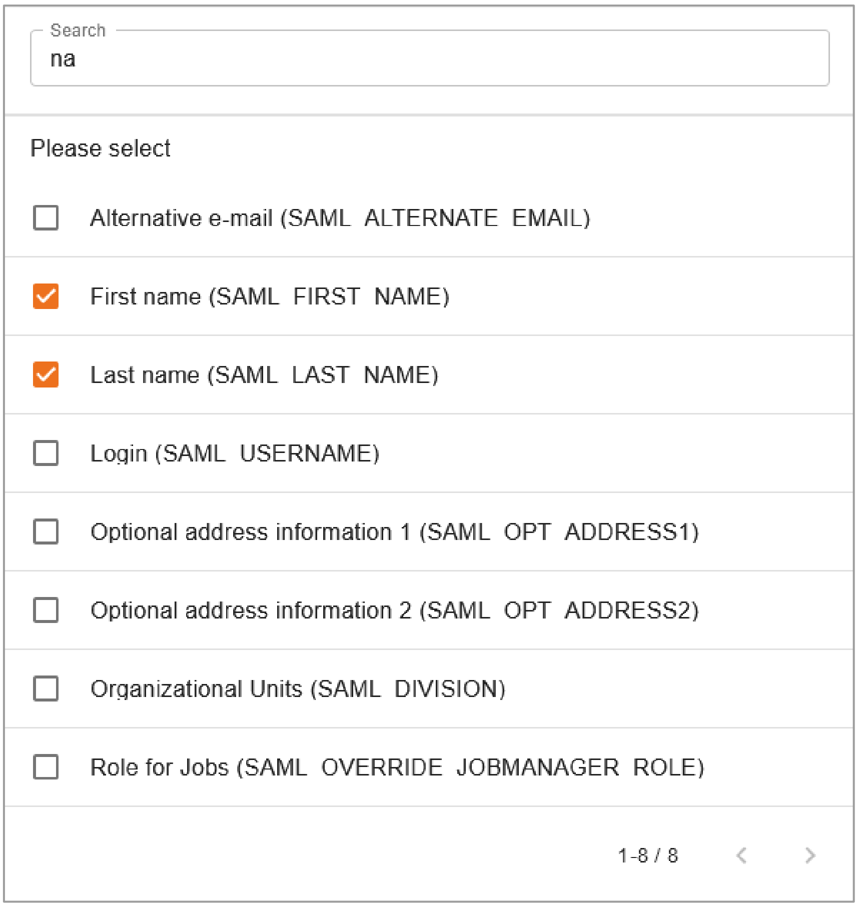
1. Click > *Administration* > *System Configuration* > *Single Sign-On / SAML*, chose the configuration you would like to change.



2. Switch the tab to *Attributes Mapping* on top of the configuration screen.

3. If there are no mappings defined, click in the checkbox and the search filter for the available BrandMaker application attributes is opened.

4. By typing in the search field attributes can be found easily:

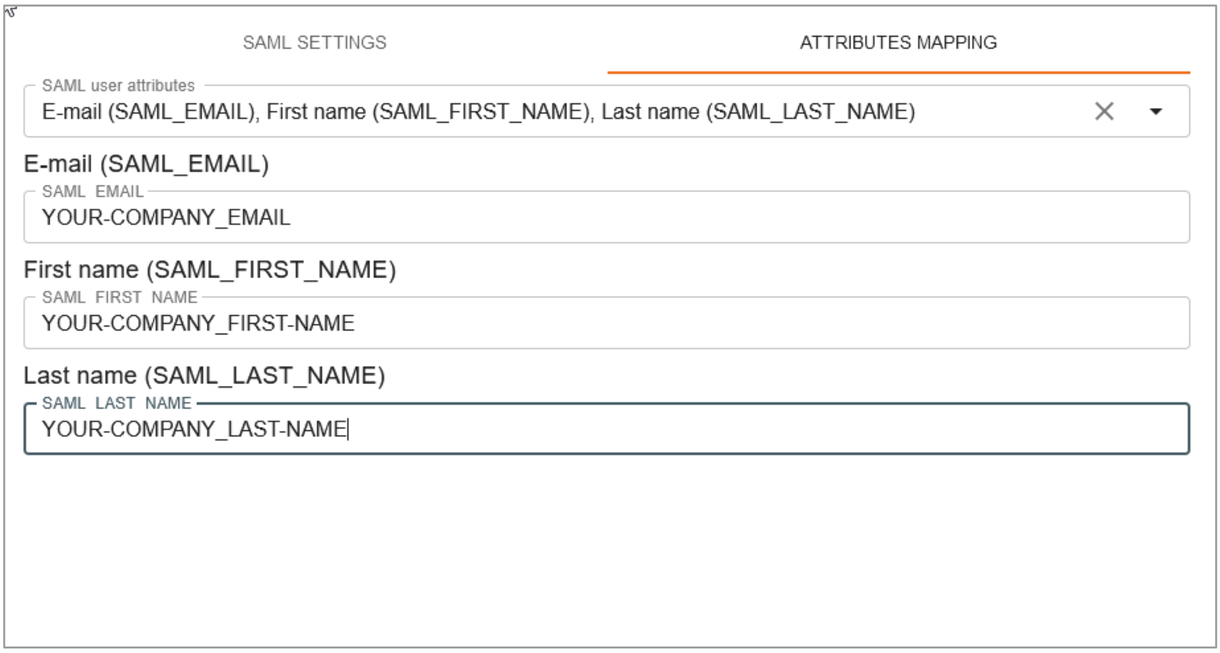


Search: na

Please select

- ☐ Alternative e-mail (SAML ALTERNATE EMAIL)
- ☑ First name (SAML FIRST NAME)
- ☑ Last name (SAML LAST NAME)
- ☐ Login (SAML USERNAME)
- ☐ Optional address information 1 (SAML OPT ADDRESS1)
- ☐ Optional address information 2 (SAML OPT ADDRESS2)
- ☐ Organizational Units (SAML DIVISION)
- ☐ Role for Jobs (SAML OVERRIDE JOBMANAGER ROLE)

1-8 / 8



SAML user attributes: E-mail (SAML_EMAIL), First name (SAML_FIRST_NAME), Last name (SAML_LAST_NAME)

E-mail (SAML_EMAIL)
SAML EMAIL: YOUR-COMPANY_EMAIL

First name (SAML_FIRST_NAME)
SAML FIRST NAME: YOUR-COMPANY_FIRST-NAME

Last name (SAML_LAST_NAME)
SAML LAST NAME: YOUR-COMPANY_LAST-NAME

5. After selecting one or many attributes they are shown on the mapping page. For each attribute the name on the side of the IdP can be entered. In the following screen this is shown by exemplary names like *YOUR-COMPANY_FIRST-NAME.*

4.4 Technical Setup Remarks

In case of technical issues while set up SAML, please check the length of the *SAML_SSO_GROUP* attribute. It has a limit of vchar255. Exceeding this limit by the SAML identity provider leads to an error.

Next to this all boolean values must be lower case to work correctly. Please ensure your IdP respects this.

4.4.1 Security

There are (at least) two different things to consider when talking about SAML security:

- Securing the transport (incl. SAML requests) via HTTPS (SSL/TLS) which is mandatory in the BrandMaker hosting environment.
- Using digital signatures to sign the SAML assertions to ensure trust between the IdP and SP
    - This can be easily achieved via certificate exchange and appropriate configuration on both sides.

4.5 Current Implementation Limits

Besides others the SAML implementation does not support “Home Realm Discovery” (HRD) and Single Logout at the moment.

5 Example: Microsoft Active Directory Federation Service as SAML Identity Provider

This chapter describes briefly how to configure MS ADFS as identity provider for the BrandMaker SSO.

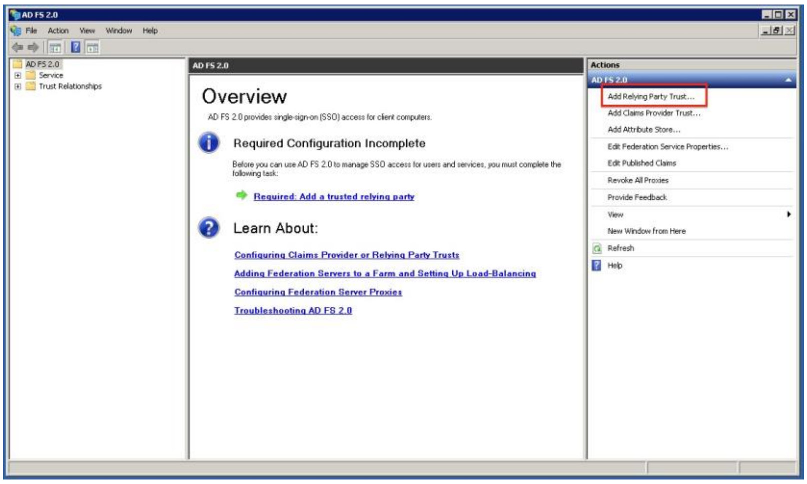
Attention: BrandMaker does not support the IdP setup in detail.

The prerequisites are:

- Microsoft Active Directory Federation Service 2.0
- The BrandMaker application must be accessible via HTTPS.
  This is necessary because ADFS accepts only HTTPS-URLs for SAML endpoints.

5.1 Configure ADFS: Setup Relay Party

1. Open the AD FS 2.0 Management Console and select *Add Relying Party Trust* to start the Add Relying Party Trust Wizard.



Overview

AD FS 2.0 provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS 2.0 to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

Learn About:

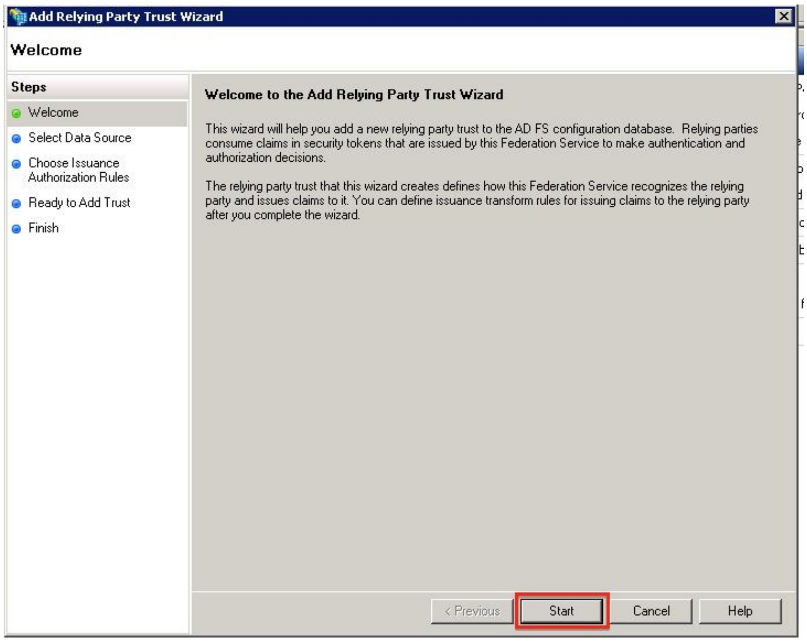
Configuring Claims Provider or Relying Party Trusts

Adding Federation Servers to a Farm and Setting Up Load-Balancing

Configuring Federation Server Proxies

Troubleshooting AD FS 2.0

2. Click *Start*.



Add Relying Party Trust Wizard

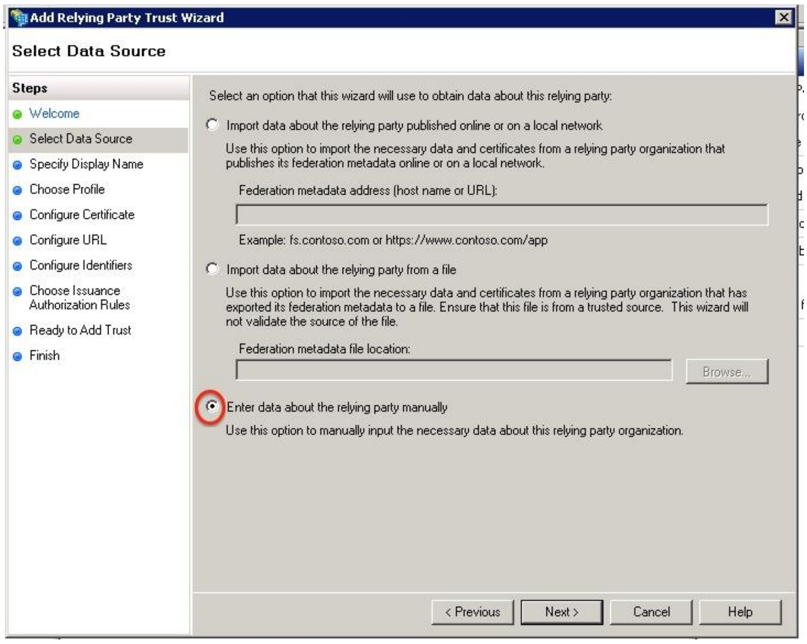
Welcome

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

3. Select *Enter date about the relying party manually* and click *Next*.



Add Relying Party Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

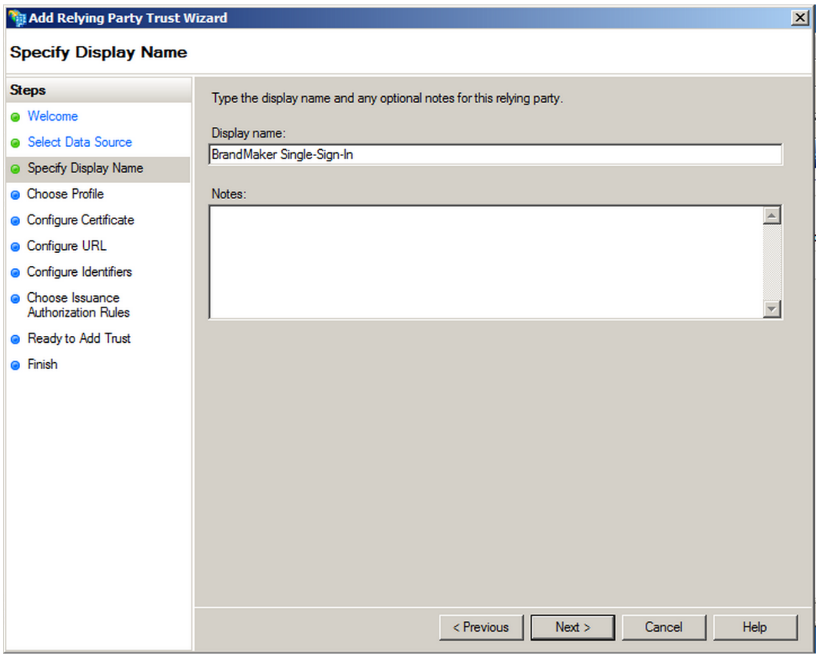
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

4. Specify a display name of your choice and click *Next*.



Add Relying Party Trust Wizard

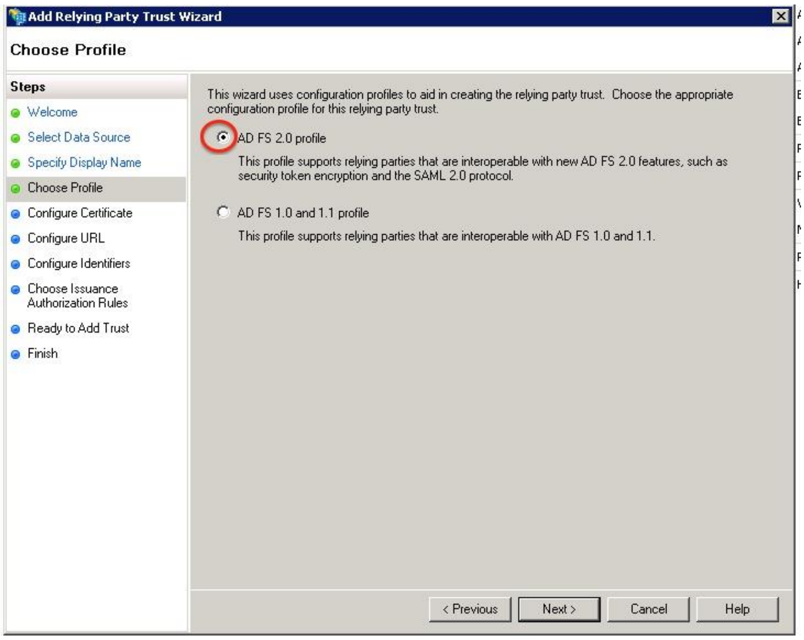
Specify Display Name

Type the display name and any optional notes for this relying party.

Display name: BrandMaker Single-Sign-In

Notes:

5. Select *AD FS 2.0 profile* and click *Next*.



Add Relying Party Trust Wizard

Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

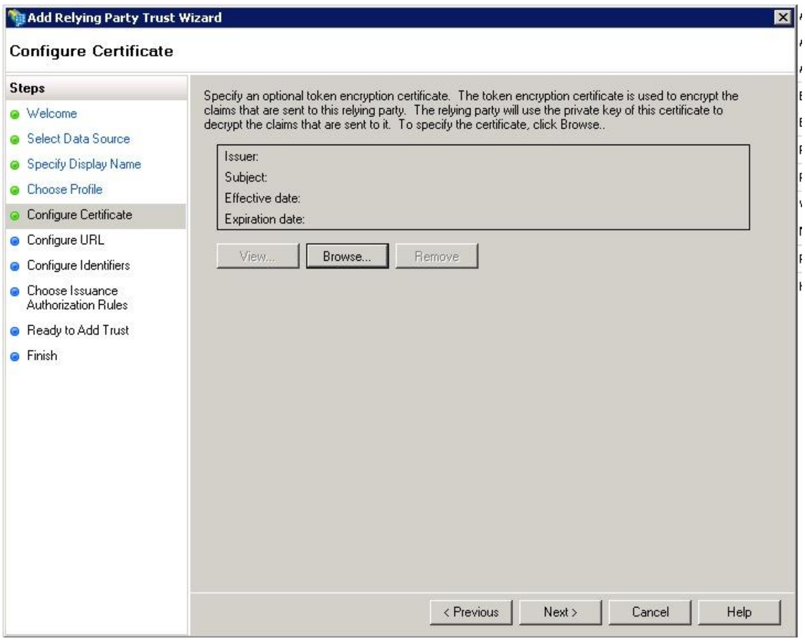
● AD FS 2.0 profile

This profile supports relying parties that are interoperable with new AD FS 2.0 features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

6. In this step you can import the certificate of the BrandMaker application; use the provided certificate from the *Download certificate of Service Provider* (see chapter 4.1.2 Configuration of Necessary Rights, Roles, and Groups):



Add Relying Party Trust Wizard

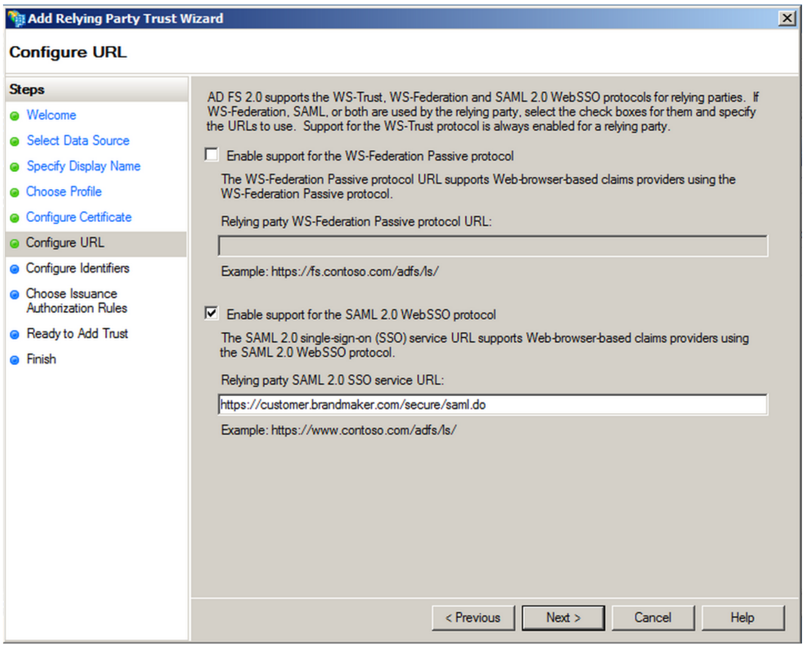
Configure Certificate

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

7. Select *Enable support for the SAML 2.0 WebSSO protocol* and configure the URL to the SAML endpoint as *Relying party SAML 2.0 SSO service URL*.
   This URL has the format https://<baseUrl>/secure/saml.do
   So if your system is running at
   https://yourcompany.brandmaker.com/ the URL is
   https://yourcompany.brandmaker.com/secure/saml.do.

8. Click *Next*.



Add Relying Party Trust Wizard

Configure URL

AD FS 2.0 supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

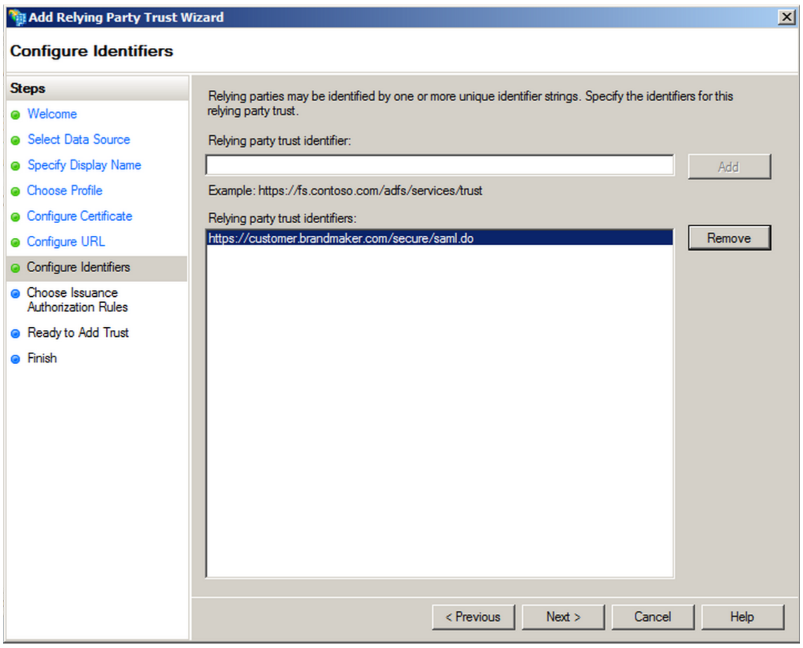
☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:
https://customer.brandmaker.com/secure/saml.do

Example: https://www.contoso.com/adfs/ls/

9. Enter the same URL as *Relying party trust identifier* and click *Add* to add it to the list. Click *Next*.



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

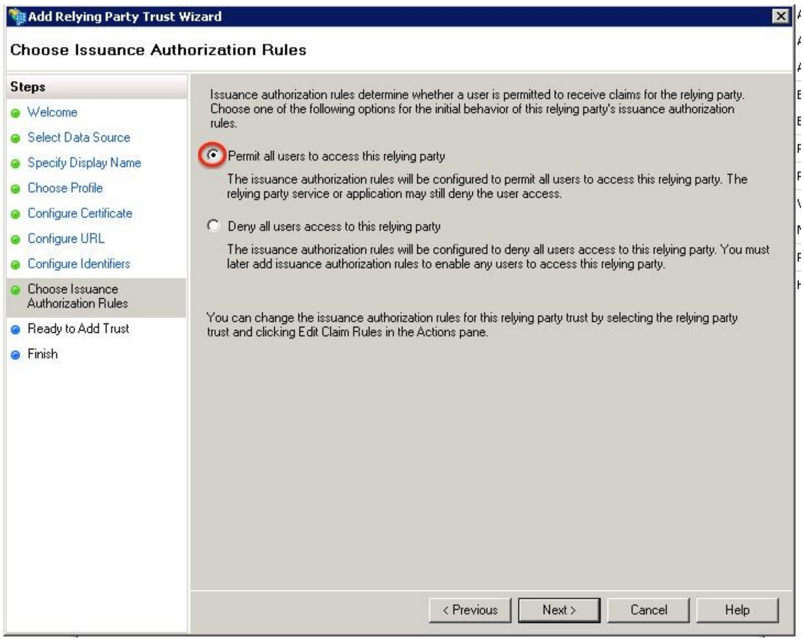
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

https://customer.brandmaker.com/secure/saml.do

10. Select *Permit all users to access the relying party* and click *Next*.
This configuration defines that ADFS returns any authenticated user to the BrandMaker application.



Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

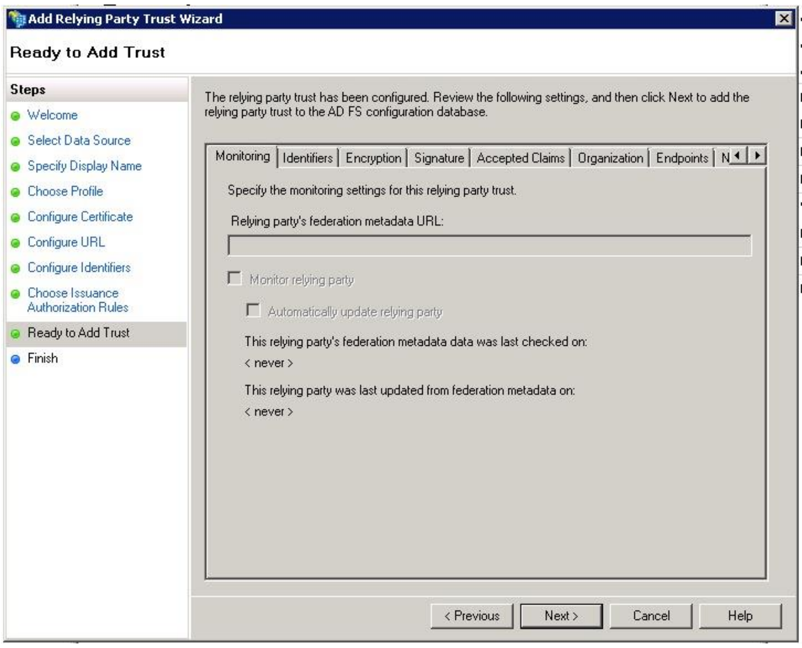
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

11. Just click *Next* on the next page.



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

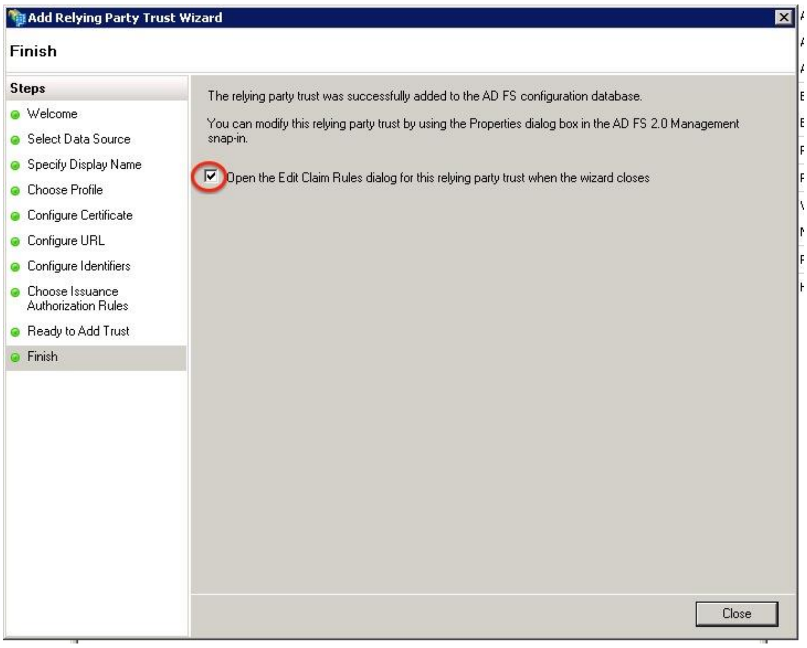
☐ Monitor relying party

☐ Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

12. Tick Open the *Edit Claim Rules* dialog and click *Close*.



The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in.

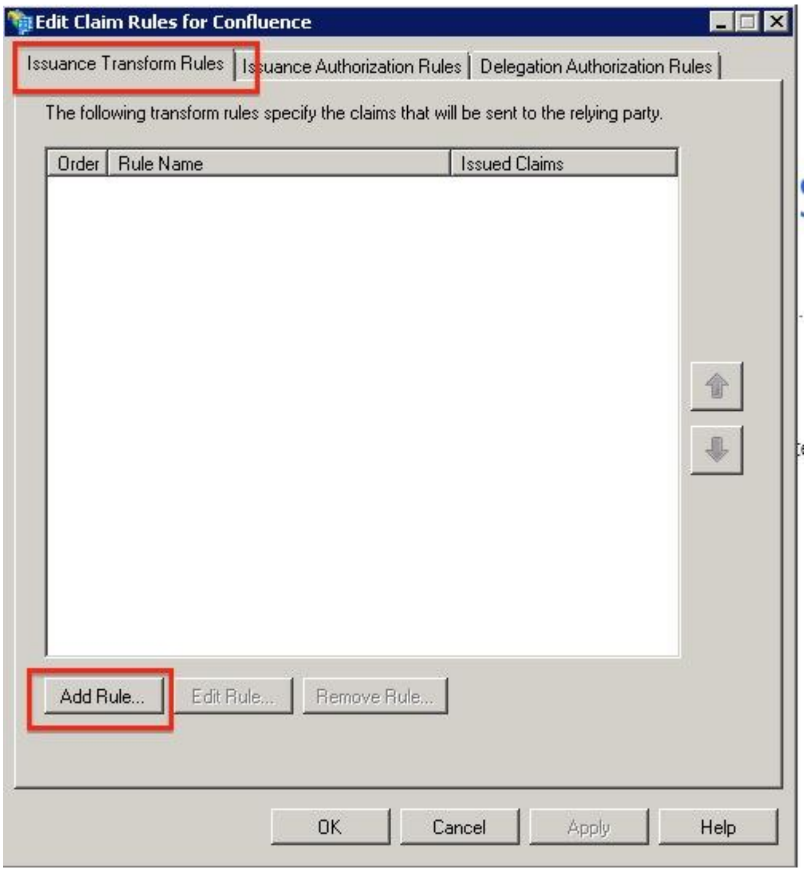
☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

The window *Edit Claim Rules* opens. Proceed in chapter 5.2 Configure ADFS: Setup Claim Rules.

5.2 Configure ADFS: Setup Claim Rules

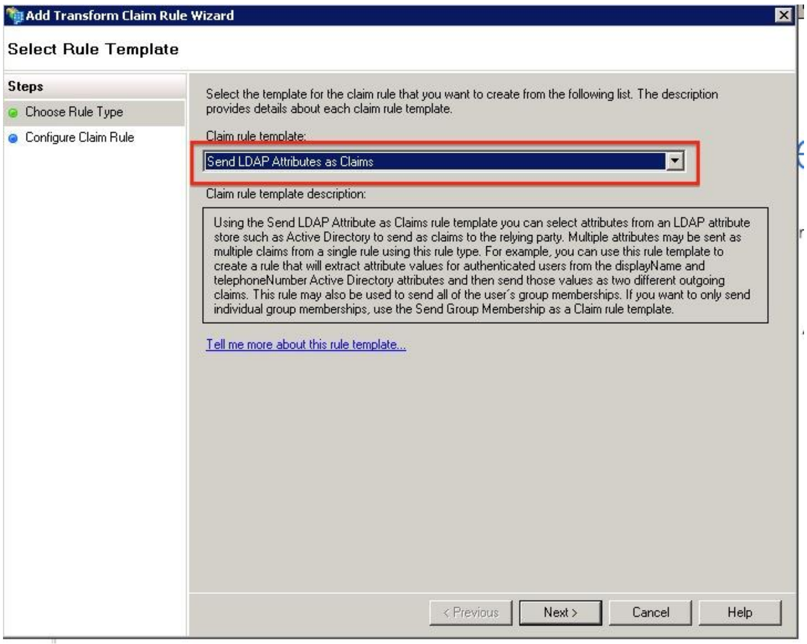
The *Edit Claim Rules Window* is opened.

1. In the first tab, click *Add Rule*.



The following transform rules specify the claims that will be sent to the relying party.

2. Select *Send LDAP Attributes as Claims* and click *Next*.



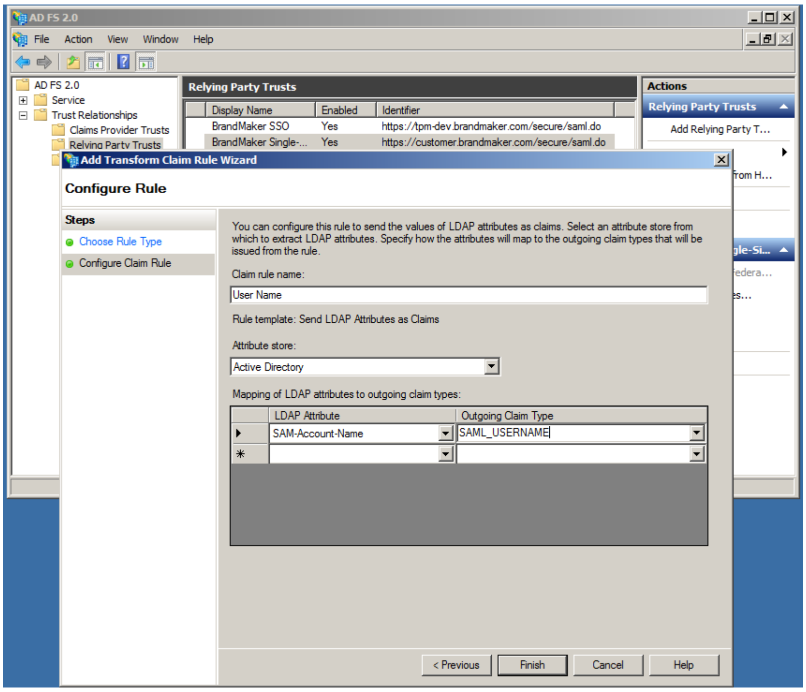
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user´s group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

3. Enter a name of your choice for the rule. Select *Active Directory* as Attribute store. Here you map the attributes from your Active Directory to BrandMaker application attributes (see chapter 4.2 Supported Attributes). Click *Finish*.



Relying Party Trusts

Display Name	Enabled	Identifier
BrandMaker SSO	Yes	https://tpm-dev.brandmaker.com/secure/saml.do
BrandMaker Single-...	Yes	https://customer.brandmaker.com/secure/saml.do

Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: User Name

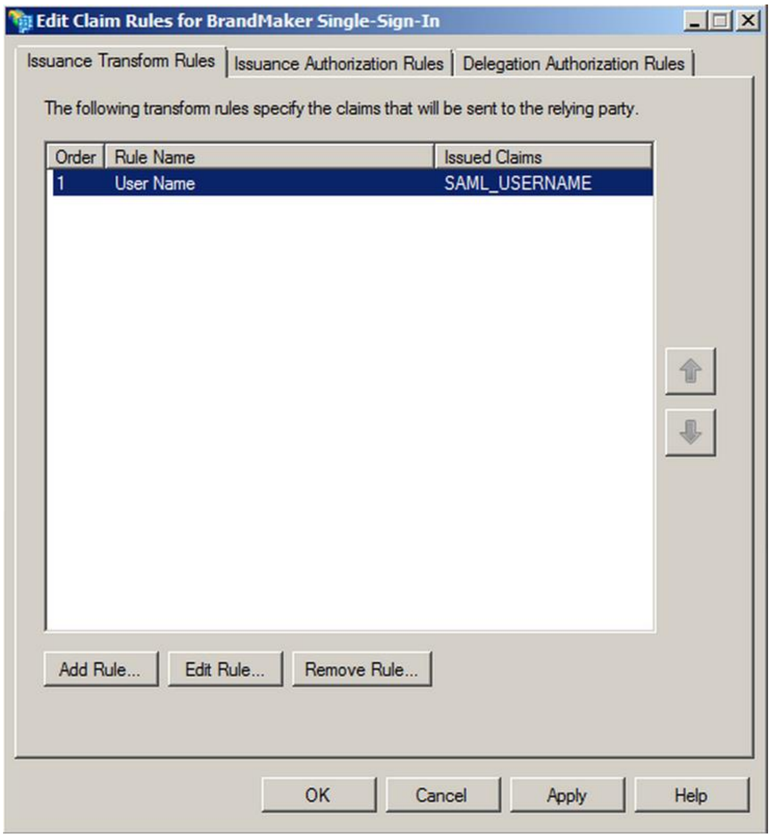
Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	SAML_USERNAME

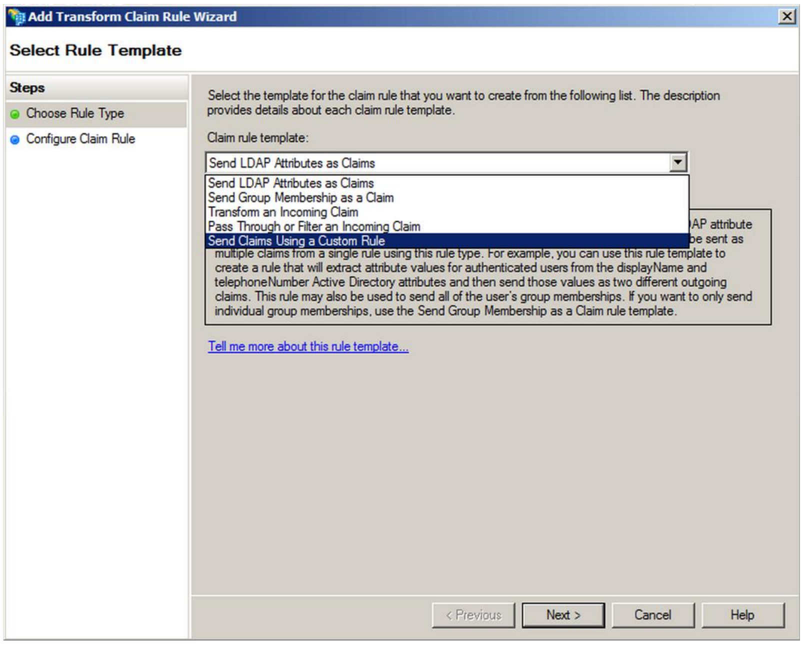
4. Click *OK* to save the settings.


Edit Claim Rules for BrandMaker Single-Sign-In
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	User Name	SAML_USERNAME

In ADFS you can as well define custom rules, which help you to configure BM specific attributes which cannot be mapped from AD, e.g. *SAML_CREATE_USER* or *SAML_UPDATE_USER*.



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

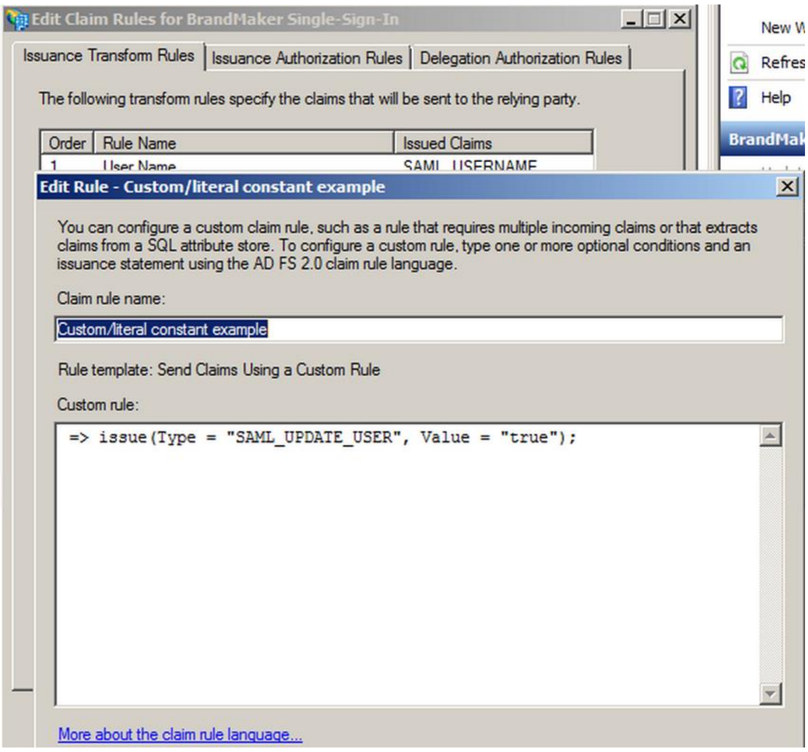
Claim rule template:

Send LDAP Attributes as Claims

- Send LDAP Attributes as Claims
- Send Group Membership as a Claim
- Transform an Incoming Claim
- Pass Through or Filter an Incoming Claim
- Send Claims Using a Custom Rule

AP attribute
be sent as
multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Tell me more about this rule template...



Edit Claim Rules for BrandMaker Single-Sign-In
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
New W
Refres
Help
BrandMak

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	User Name	SAML_USERNAME

Edit Rule - Custom/literal constant example

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name:

Custom/literal constant example

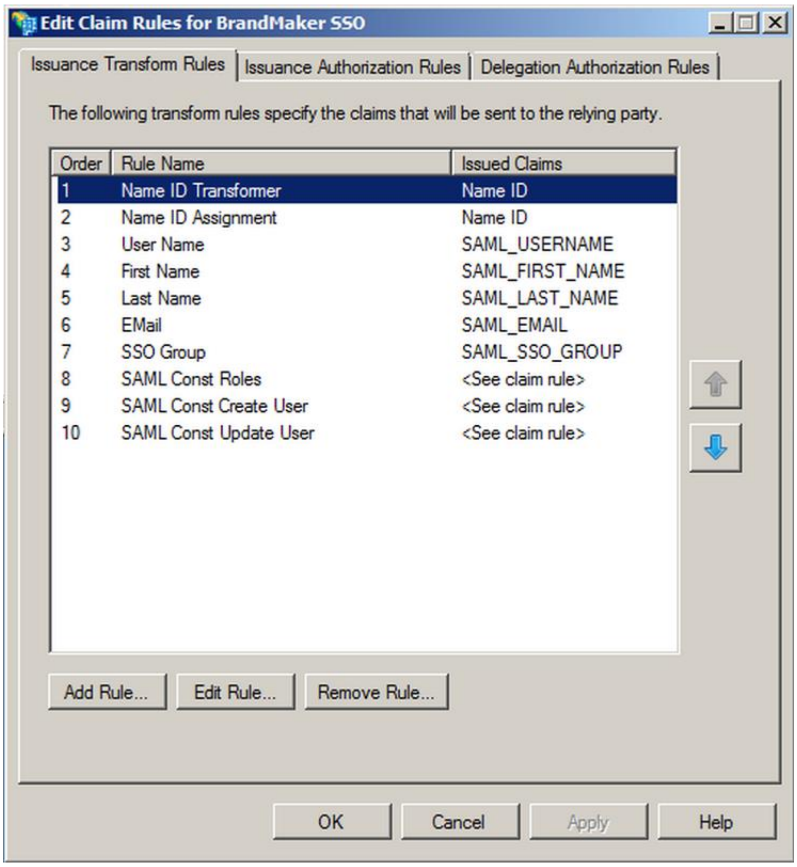
Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> issue(Type = "SAML_UPDATE_USER", Value = "true");
```

More about the claim rule language...

At least for all required attributes (see chapter 4.2 Supported Attributes) a claim rule needs to exist. At the end the claim rules may look like this:



Edit Claim Rules for BrandMaker SSO
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

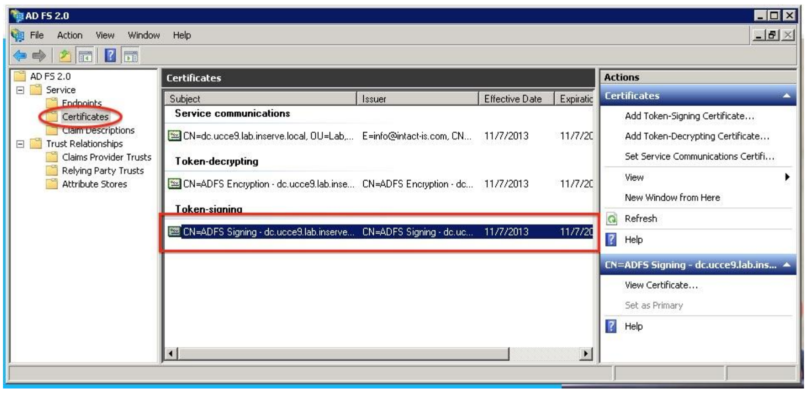
Order	Rule Name	Issued Claims
1	Name ID Transformer	Name ID
2	Name ID Assignment	Name ID
3	User Name	SAML_USERNAME
4	First Name	SAML_FIRST_NAME
5	Last Name	SAML_LAST_NAME
6	EMail	SAML_EMAIL
7	SSO Group	SAML_SSO_GROUP
8	SAML Const Roles	<See claim rule>
9	SAML Const Create User	<See claim rule>
10	SAML Const Update User	<See claim rule>

5.3 Configure ADFS: Export token signing certificate

The SAML response coming from ADFS is signed to ensure that the authentication is coming from the correct identity provider. To validate this signature, the certificate must be exported from ADFS and configured in the plugin configuration.

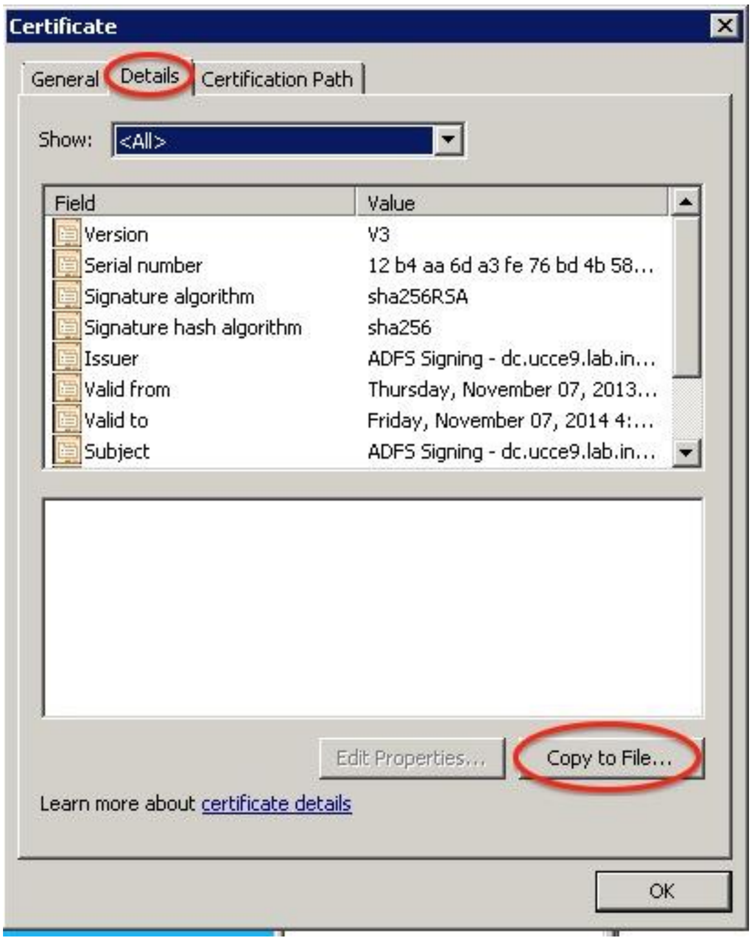
This might already be done during the IdP setup in the BrandMaker application as described in chapter 4.1.1 Configuration of the Identity Providers.

1. In the ADFS management console, click the *Certificates* folder and double-click on the Token Signing certificate.



Subject	Issuer	Effective Date	Expiratic
Service communications			
CN=dc.ucce9.lab.inserve.local, OU=Lab,...	E=info@intact-is.com, CN...	11/7/2013	11/7/20
Token-decrypting			
CN=ADFS Encryption - dc.ucce9.lab.inse...	CN=ADFS Encryption - dc...	11/7/2013	11/7/20
Token-signing			
CN=ADFS Signing - dc.ucce9.lab.inserve...	CN=ADFS Signing - dc.uc...	11/7/2013	11/7/20

2. Click the *Details* tab and the Button *Copy to File…*

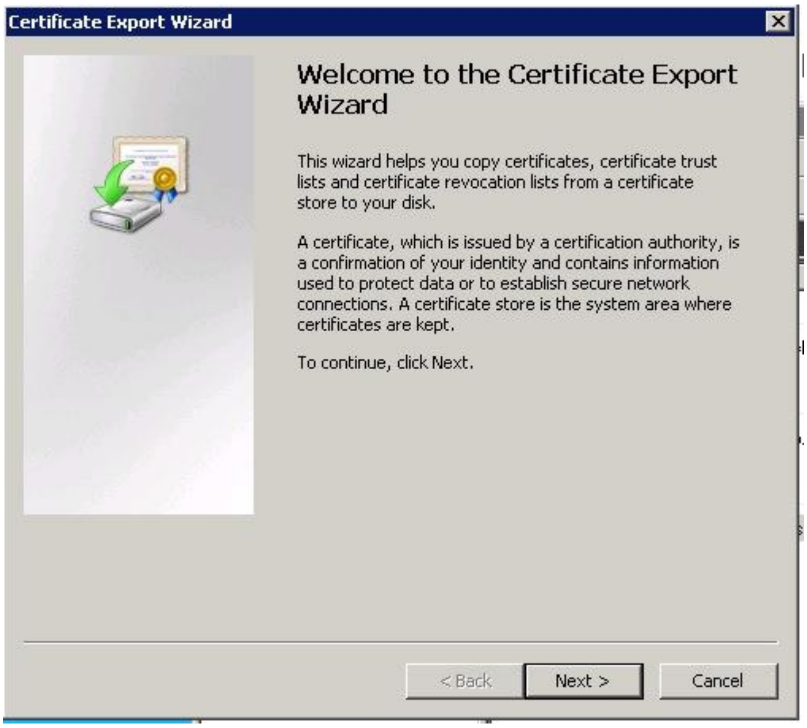


Show: <All>

Field	Value
Version	V3
Serial number	12 b4 aa 6d a3 fe 76 bd 4b 58...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - dc.ucce9.lab.in...
Valid from	Thursday, November 07, 2013...
Valid to	Friday, November 07, 2014 4:...
Subject	ADFS Signing - dc.ucce9.lab.in...

Learn more about certificate details

3. Export the certificate as *Base-64 encoded X.509 (.CER)*.



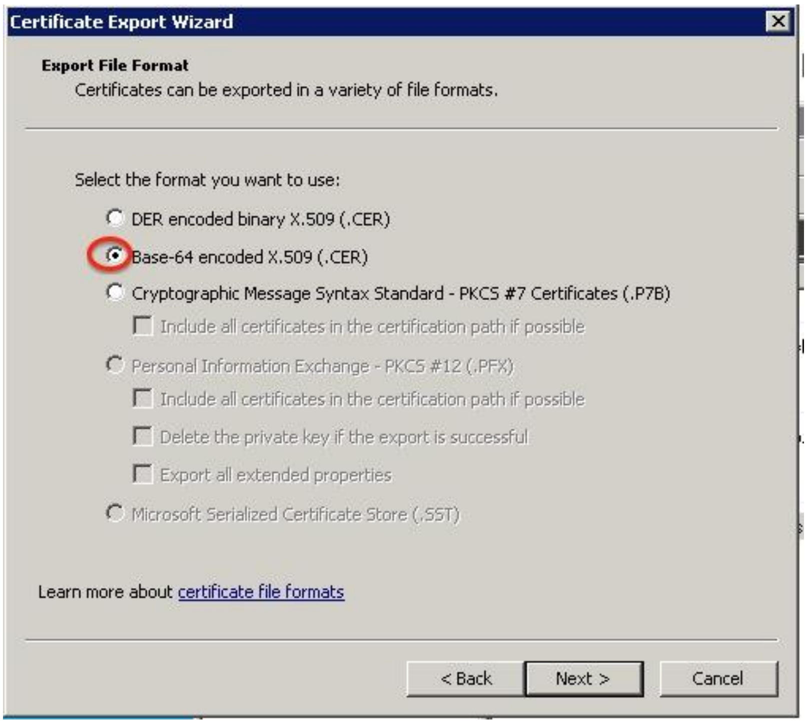
Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

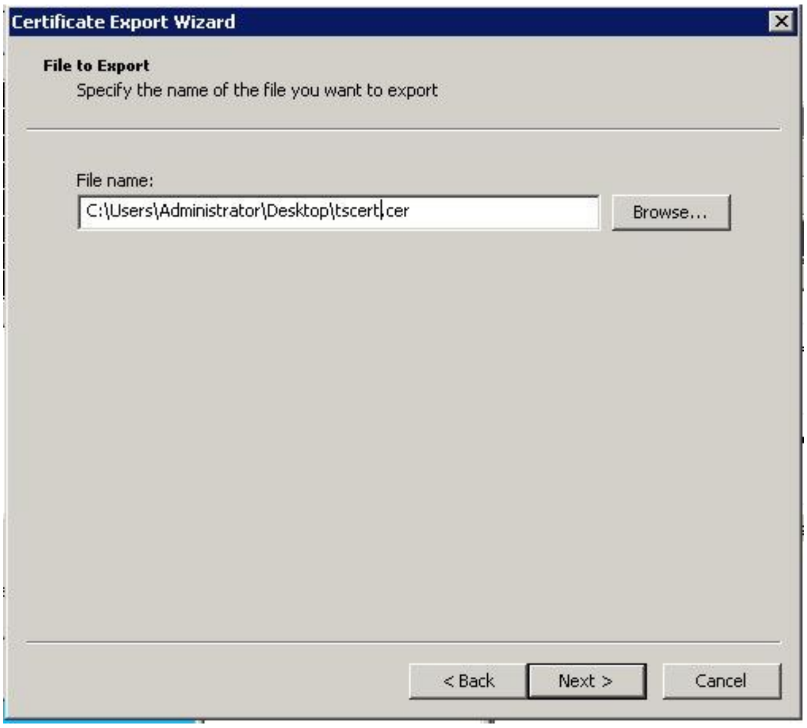
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats



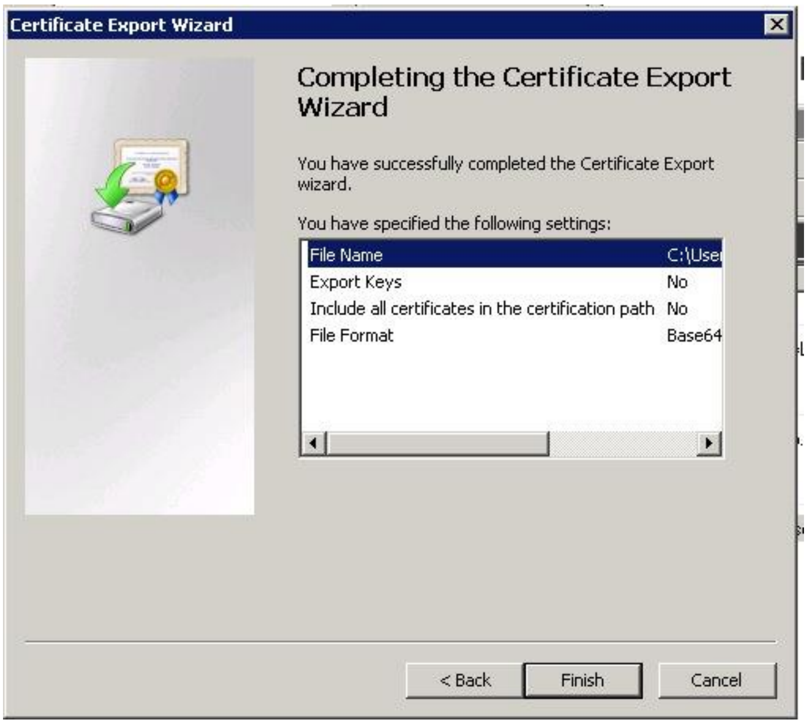
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

C:\Users\Administrator\Desktop\tscert.cer



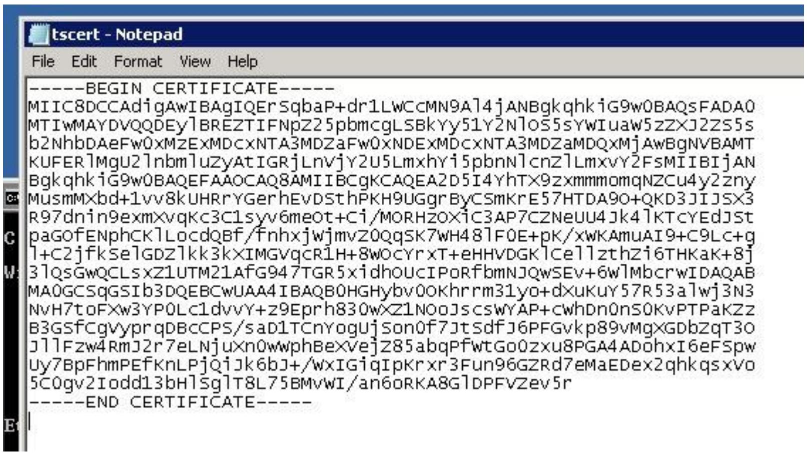
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

4. Open the exported file in a text editor and copy the content into the clipboard for the next step.



```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQErSqbaP+dr1LWCcMN9Al4jANBgkqhkiG9w0BAQsFADA0
MTIwMAYDVQQDEylBREZTIFNpZ25pbmcgLSBkYy51Y2NlOS5sYWIuaW5zZXJ2ZS5s
b2NhbDAeFw0xMzExMDcxNTA3MDZaFw0xNDExMDcxNTA3MDZaMDQxMjAwBgNVBAMT
KUFERlMgU2lnbmluZyAtIGRjLnVjY2U5LmxhYi5pbnNlcnZlLmxvY2FsMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2D5I4YhTX9zxmmmomqNZCu4y2zny
MusmMXbd+1vv8kUHRrYGerhEvDSthPKH9UGgrByCSmKrE57HTDA9O+QKD3JIJSX3
R97dnin9exmXvqKc3C1syv6meOt+Ci/MORHzOXiC3AP7CZNeUU4Jk4lKTcYEdJSt
paGOfENphCKlLocdQBf/fnhxjWjmvZ0QqSK7WH48lF0E+pK/xWKAmuAI9+C9Lc+g
l+C2jfkSelGDZlkk3kXIMGVqcR1H+8WOcYrxT+eHHVDGKlCellzthZi6THKaK+8j
3lQsGwQCLsxZ1UTM21AfG947TGR5xidhOUcIPoRfbmNJQwSEv+6WlMbcrwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4IBAQB0HGHybv0OKhrrm31yo+dXuKuY57R53alwj3N3
NvH7toFXw3YP0Lc1dvvY+z9Eprh830wXZ1NOoJscsWYAP+cWhDn0nS0KvPTPaKZz
B3GSfCgVyprqDBcCPS/saD1TCnYogUjSon0f7JtSdfJ6PFGvkp89vMgXGDbZqT3O
JllFzw4RmJ2r7eLNjuXn0WwphBeXVejZ85abqPfWtGo0zxu8PGA4ADohxI6eFSpw
Uy7BpFhmPEfKnLPjQiJk6bJ+/WxIGiqIpKrxr3Fun96GZRd7eMaEDex2qhkqsxVo
5C0gv2Iodd13bHlSglT8L75BMvWI/an6oRKA8GlDPFVZev5r
-----END CERTIFICATE-----
```

5. Paste this BASE64-encoded Token Signing Certificate into the BrandMaker application SAML configuration (> *Administration* > *System Configuration* > *Single Sign-On / SAML* > *IdP certificate (X509)* field).

6. Save the form

The BrandMaker application now trusts your configured identity provider.

6 Example: Salesforce as SAML identity provider

Attention: BrandMaker does not support the IdP setup in detail.

See salesforce.com online help:

- Enable Salesforce as an identity provider
- Salesforce as identity provider

7 Additional Info and Links

For further information about SAML the following articles may be interesting:

Wikipedia:
https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

SAP Security and Identity Management:
http://wiki.scn.sap.com/wiki/display/Security/Security+and+Identity+Management+at+SAP

Integrating Third-Party SAML Solution Providers with AWS:
http://docs.aws.amazon.com/IAM/latest/UserGuide/identity-providers-saml-solution-providers.html

VMware vFabric Blog about SSO:
http://blogs.vmware.com/vfabric/2013/03/putting-the-single-back-in-single-sign-on-sso.html

SimpleSAMLphp Documentation:
https://simplesamlphp.org/docs/1.5/

ServiceNow SSO Product Documentation:
http://wiki.servicenow.com/index.php?title=External_Authentication_(Single_Sign-On_-_SSO)