SAML Admin Guide

Version 1.1

Contents

1 SAML Service Workflow

1.1 Step 1: Terena Level

The Terena SAML admin configures the full list of allowed IDPs (identity providers) via a single URL that contains multiple IDPs.

1.2 Step 2: NREN Level

After the Terena SAML admin downloads the IDPs, each NREN SAML admin must configure their own Registration Authority to specify which of the IDPS their Participants (below them) may use.

1.3 Step 3: Participant Level

Once the NREN SAML admin configures the Registration Authority, each Participant can then create an IDP Attribute Mapping between the DigiCert Validated Organization and the organization identifier sent in the SAML assertion.

1.4 New Login URL

Along with the new SAML process changes, we have changed the login URL to:

https://www.digicert.com/sso

2 SAML Role and Account Access

The SAML admin role is available at the Terena, NREN, and Participant levels. However, what the SAML admin can do at each level is different.

2.1 SAML Admin Role

The primary function of the SAML Admin role is to allow an administrator to manage their SAML settings for their account. A SAML administrator's tasks may include configuring allowed IDPs, configuring their Registration Authority, creating an attribute mapping, etc. To access the SAML settings (IDP Manager, IDP Mapping, Attribute Mapping, and SAML Organization Mapping) you must be assigned the SAML Admin role or have the SAML Admin role as one of your roles (i.e. *SAML Admin* or *Administrator + SAML Admin*).

2.1.1 Terena Level SAML Admin Role

This SAML Admin can access the IPD Manager, which they use to configure the allowed IDPs for the entire Terena system.

This admin can also access Attribute Mapping, which they uses to configure the default attribute mappings for the entire Terena system.

2.1.2 NREN Level SAML Admin Role

This SAML Admin can access **IDP Mapping**, which they can use to configure their Registration Authority for their NREN. They can enable any IDPs from the Terena level list of allowed IDPs.

This SAML Admin can also access **Attribute Mapping**, which they can use to override any of the default attribute mappings set up by the Terena SAML admin.

2.1.3 Participant Level SAML Admin Role

This SAML Admin can access SAML Organization Mapping, which they can use to map a Validated Organization from the DigiCert system to an organization that is specified in the SAML assertion (*schacHomeOrganization*).

2.2 Managing SAML Admins

2.2.1 How to Add a SAML Admin to Your Account/Add the SAML Admin Role

1. In your account, in the sidebar menu, click **Account > Manage Users**.
2. On the **Manage Users** page, click **+ New User**.
3. On the **New Users** page, provide the following details for the new user:

First Name:	Type the user's first name.
Last Name:	Type the user's last name.
Email:	Type an email address at which the user can be contacted.
Phone:	Type a phone number at which the user can be reached. A phone number is required if the user will be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests) and/or a **CS Verified User** (able to approve Code Signing certificate requests).
Job Title:	Type the user's job title. A job title is required if the user will be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests) and/or a **CS Verified User** (able to approve Code Signing certificate requests).

Username: Type the username for the user.

Although you can create a unique username for each user, we recommend using their email address (i.e. *john.doe@example.com*).

Division: In the drop-down list, select the Division or Subdivision to which you want to assign the user.

Role: Select a role(s) for the new user: **SAML Admin** or **Administrator** + **SAML Admin**.

SAML Admin Note:

To access the **SAML** settings in your account, you must be a SAML Admin. When assigning the **SAML Admin** role, you can just select that role (i.e. *SAML Admin*), or you can select that role along with another (i.e. *Administrator* + *SAML Admin*).

4. When you are finished, click **Save User**.

   The user should be added to the account (**Account > Manage Users**). The newly added user will be sent an email that contains a link, which lets them create a password to log into the account.

2.2.2 How to Edit User Accounts to Change User Roles/Add the SAML Admin Role

1. In your account, in the sidebar menu, click **Account > Manage Users**.
2. On the **Manage Users** page, in the **Division** drop-down list, select the Division or Subdivision to which the user belongs.
3. To the right of the user account whose details you need to modify, click **View**.
4. On the "*User's*" page, click **Edit User**.
5. On the **Edit User** page, change any of the following details:

   First Name: Edit the user's first name.

   Last Name: Edit the user's last name.

   Email: Edit the email address at which the user can be contacted.

Phone: Add, edit, or remove the phone number at which the user can be reached.

You must provide the user's phone number if you want them to be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests) and/or a **CS Verified User** (able to approve Code Signing certificate requests).

Job Title: Add, edit, or delete the user's job title.

You must provide the user's job title if the user will be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests) and/or a **CS Verified User** (able to approve Code Signing certificate requests).

Username: Edit the username for the user.

Although you can create a unique username for each user, we recommend using their email address.

Role: Select a different role for/add another role to the user: **SAML Admin** or **Administrator** + **SAML Admin**.

SAML Admin Note:

To access the **SAML** settings in your account, you must be a SAML Admin. When assigning the **SAML Admin** role, you can just select that role (i.e. *SAML Admin*), or you can select that role along with another (i.e. *Administrator* + *SAML Admin*).

6. When you are finished, click **Save User**.

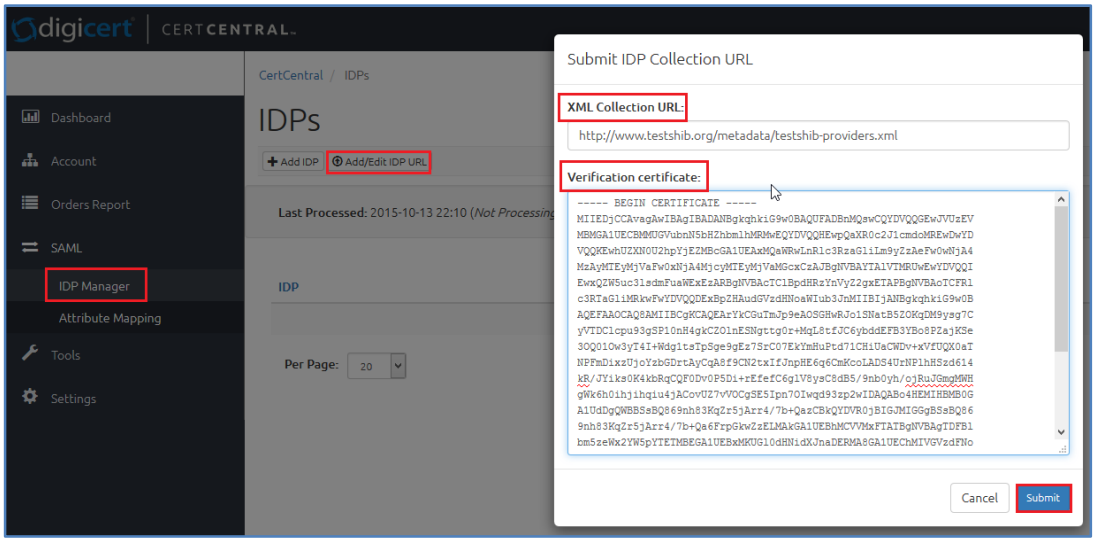
3 Managing SAML Settings

3.1 IDP Manager

This is used to configure the IDP URL that contains all the allowed IDPs for the whole Terena system. The XML file containing the IDPs at this URL will be downloaded once a day; any new IDPs will be added automatically while any old IDPs will be removed. The process is done in the background; it may take a few minutes to pull down the new XML file and process it.

3.1.1 How to Configure the IDP Manager (Terena SAML Admin)

1. In your account, in the sidebar menu, click SAML > IDP Manager.
2. On the IDPs page, click Add/Edit IDP URL.



3. In the Submit IDP Collection URL window, enter the following information:

XML Collection URL:	Enter IDP URL that contains all the IDPs metadata.
Verification certificate	Enter the certificate that was used to sign the IDP xml file.

4. When you are finished, click Submit.

3.2 Attribute Mapping

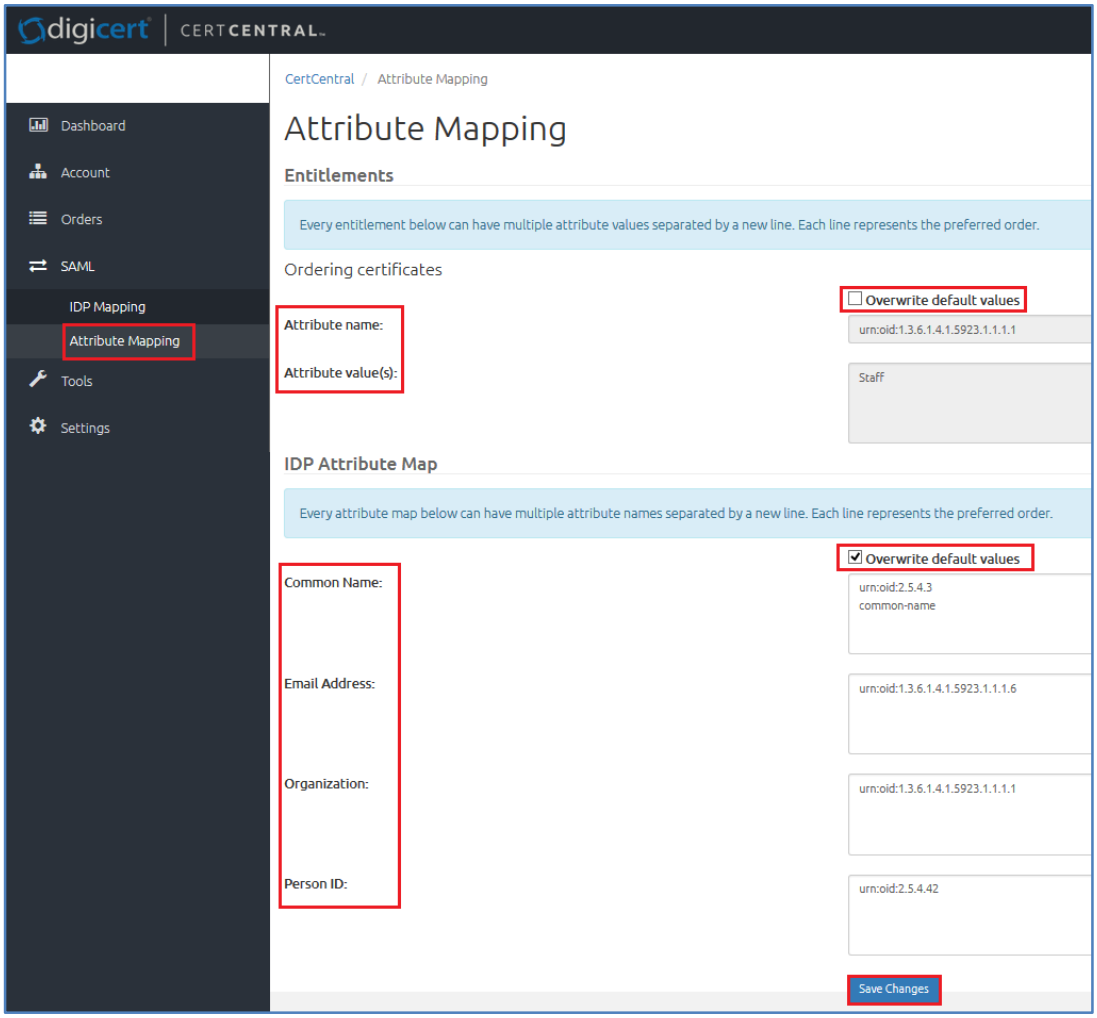
At the Terena level, this can be used to set up the default attribute mappings for the entire Terena System. At the NREN level, this can be used to change/overwrite the default attribute mappings if needed.

3.2.1 How to Set Up Attribute Mapping (Terena or NREN SAML Admin)

1. In your account, in the sidebar menu, click SAML > Attribute Mapping.
2. On the Attribute Mapping page, under Entitlements enter the following information for Ordering certificates:

Attribute name:	Enter the attribute name.

Attribute value(s):	Enter the attribute value(s) you want to associate with the attribute name. Values can be comma or new line delimited.
Overwrite default values	Check this box to overwrite the default attribute values.



3. Under **IDP Attribute Map**, enter the following information for the attributes that you want to map:

Common Name:	Enter the value for the common name or name to be displayed.

Email Address:	Enter the value for the email address.
Organization:	Enter the value for the organization (i.e. *schacHomeOrganization*).
Person ID:	Enter the value for the person's personal ID.
Overwrite default values	Check this box to overwrite the default attribute values.

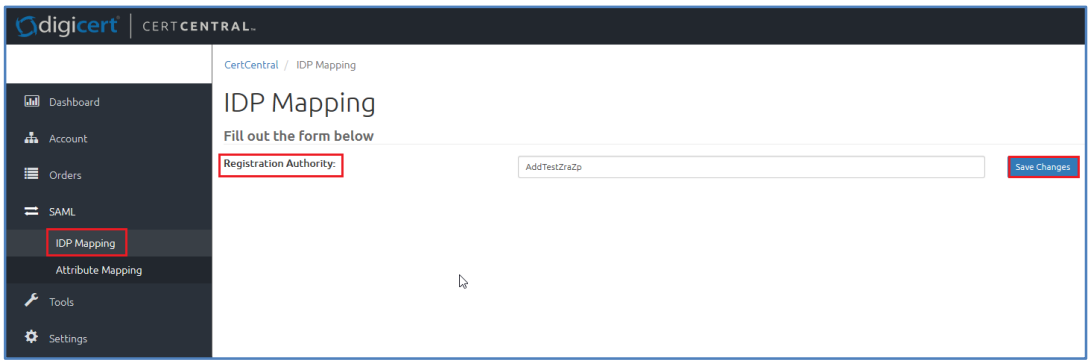
4. When you are finished, click **Save Changes**.

3.3 IDP Mapping

This is used to configure the Registration Authority for the NREN. The Registration Authority is where the NREN SAML admin enables which IDPs (from the list of Terena allowed IDPs) they want to use for them and their Participants.

3.3.1 How to Configure IDP Mapping (NREN SAML Admin)

1. In your account, in the sidebar menu, click **SAML > IDP Mapping**.
2. On the **IDP Mapping** page, in the **Registration Authority** box, enter the straight string match from the value entered in the UI form and the *registrationAuthority* in the IDP metadata.



3. When you are finished, click **Save Changes**.

3.4 Organization Mapping

This is used to map a *Validated* Organization in the DigiCert system to an organization specified in the SAML assertion (i.e. *schacHomeOrganization*). When the Participant SAML Admin adds a mapping, the can select their IDP, their DigiCert Organization, and enter in their *schacHomeOrganization* value.

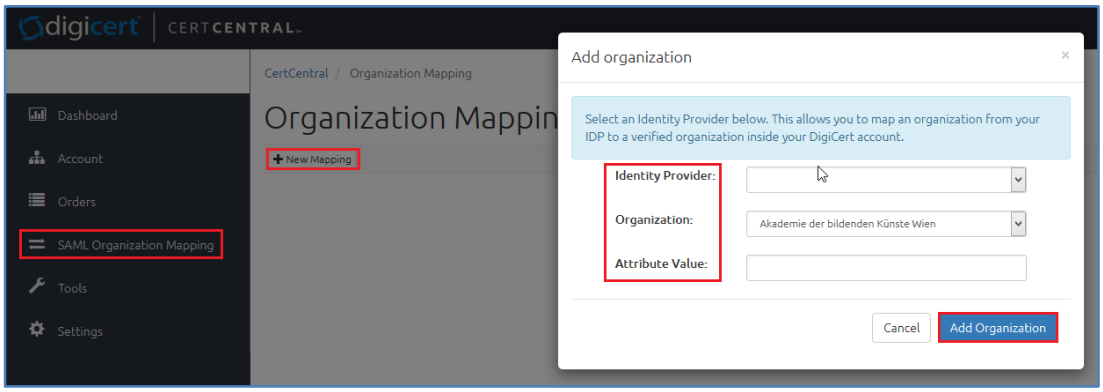
3.4.1 How to Add an Organization Mapping (Participant SAML Admin)

1. In your account, in the sidebar menu, click **SAML Organization Mapping**.
2. On the **Organization Mapping** page, click **New Mapping**.
3. In the **Add Organization** window, enter the following information to map an organization from your IDP to a *Validated* organization in your DigiCert account:

   Identity Provider: In the drop-down list, select an IDP.

   Organization: In the drop-down list, select a DigiCert validated organization.

   Attribute Value: Enter the organization value (i.e. *schacHomeOrganization*).



4. When you are finished, click **Add Organization**.