SAML Admin Guide (GÉANT)

Version 1.5

Table of Contents

1 SAML Service Workflow

1.1 Step 1: GÉANT Level

The GÉANT 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 GÉANT SAML admin downloads the IDPs, each NREN SAML administrator 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 Step 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 GÉANT, 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 (e.g., *SAML Admin* or *Administrator + SAML Admin*).

2.1.1 GÉANT Level SAML Admin Role

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

This admin can also access **Attribute Mapping**, which they uses to configure the default attribute mappings for the entire GÉANT 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 GÉANT 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 GÉANT 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 Create a SAML Admin Account/Add the SAML Admin Role

1. In your account, in the sidebar menu, click **Account > Users**.
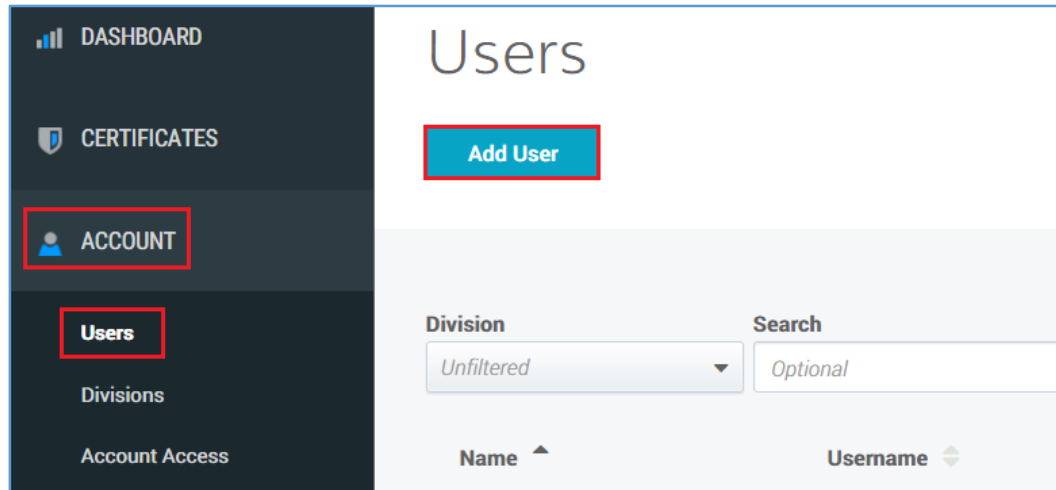
2. On the **Users** page, click **Add User**.

3. On the **Add User** page, in the **User Details** section, provide the following details for the 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. The user will be sent an email with instructions for creating a password to log into their account.
Phone:	Type a phone number at which the user can be reached. A phone number is only required if the user will be an **EV Verified User**, an **EV CS Verified User**, and/or a **CS Verified User**.
Job Title:	Type the user's job title. A job title is only required if the user will be an **EV Verified User**, an **EV CS Verified User**, and/or a **CS Verified User**.

4. In the **User Access** section, provide the following access information for user.

|	
Username:	The username will auto-populate.
	Although you can create a unique username for each user, we recommend using their email address (e.g., *john @example.com*).
Division:	In the drop-down list, select the Division or Subdivision to which you want to assign the user.
Role(s)	Select a role(s) for the new user:
	SAML Admin or **Administrator** + **SAML Admin**.
	Note: To access the **SAML** settings in your account, the user must be assigned the **SAML Admin** role.

5. When you are finished, click **Add User**.

    The newly added user will be sent an email that contains a link, which lets them create a password to log into their account.

2.2.2 How to Edit an Existing Account to Add the SAML Admin Role/Change the Account to a SAML Admin Account

If you are an administrator and need the SAML Admin role added to your account or need your account changed to a SAML Admin account, you must get another administrator to edit your account and make those changes. You cannot change or add roles to your own account.

1. In your account, in the sidebar menu, click **Account > Users**.
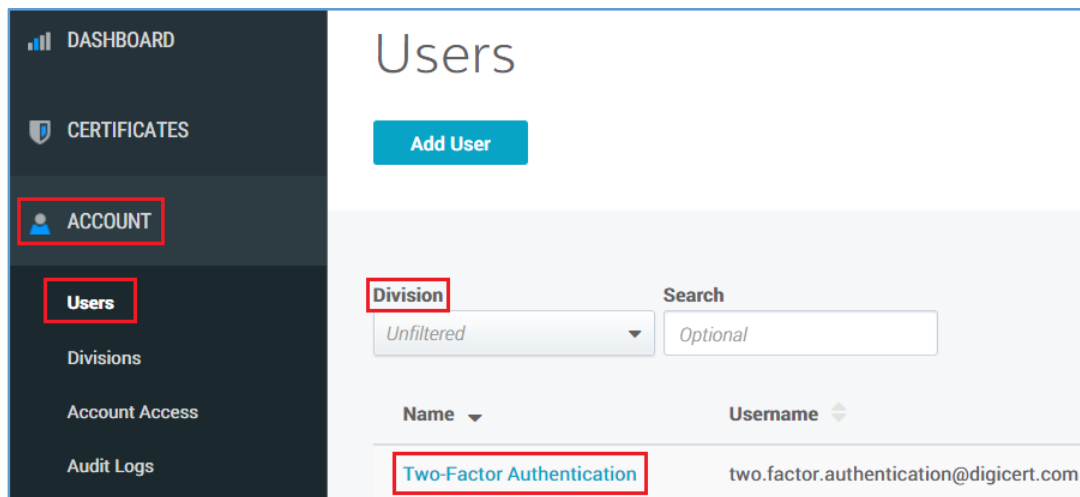
2. On the **Users** page, locate the user account whose role you want to modify, click the **"User's Name"** link.

3. On the **"User's Name"** page, in the **User Access** section, under **Role(s)**, do one of the following:

Add the **SAML Admin** role to the account (e.g., *Administrator + SAML Admin*):	Check **SAML Admin**.
Change the account to a SAML Admin account (e.g., *change from Administrator to SAML Admin*):	Uncheck the current role and then check **SAML Admin**.

User Access

Username

2.factor.authentications@digicert.com

Division

Charles Test Nren Division

Role(s)

☑ Administrator

☑ SAML Admin

Update User   Cancel

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

3 Managing SAML Settings

3.1 IPD Manager

This function is used to configure the IDP URL that contains all the allowed IDPs for the whole GÉANT 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 (GÉANT SAML Admin)

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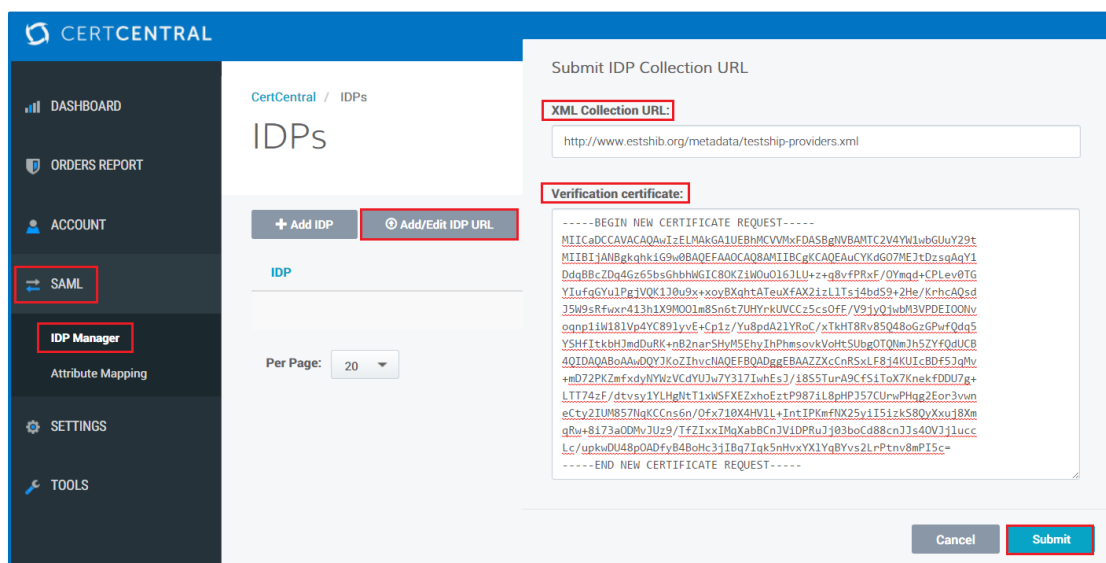
2. On the **IDPs** page, click **Add/Edit IPD URL**.

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

   XML Collection URL: Enter the 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 GÉANT level, this can be used to set up the default attribute mappings for the entire GÉANT 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 (GÉANT or NREN SAML Admin)

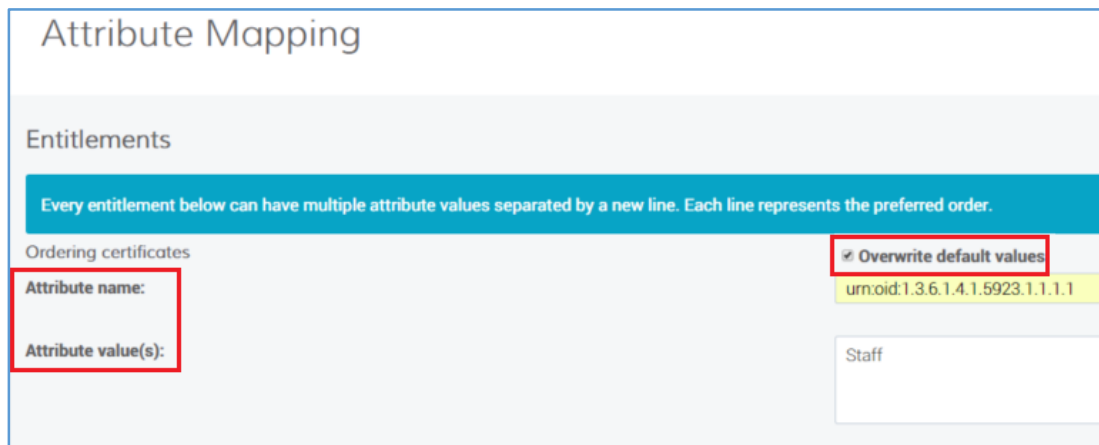1. In your account, in the sidebar menu, click **SAML > Attribute Mapping**.
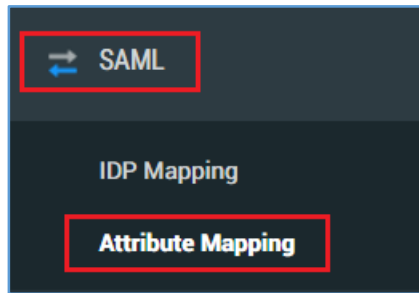
2. On the **Attribute Mapping** page, under **Entitlements**, enter the following information for **Ordering certificates**:

   Note: You can enter multiple values. Make sure that each value is on its own line, where each line represents the preferred order.

   Attribute name: Enter the attribute name(s).

   Attribute value(s):   Enter the attribute value(s) you want to associate with the attribute name.

   Overwrite default values   Check this box to overwrite the default values.

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

Note: You can enter multiple values. Make sure that each value is on its own line, where each line represents the preferred order.

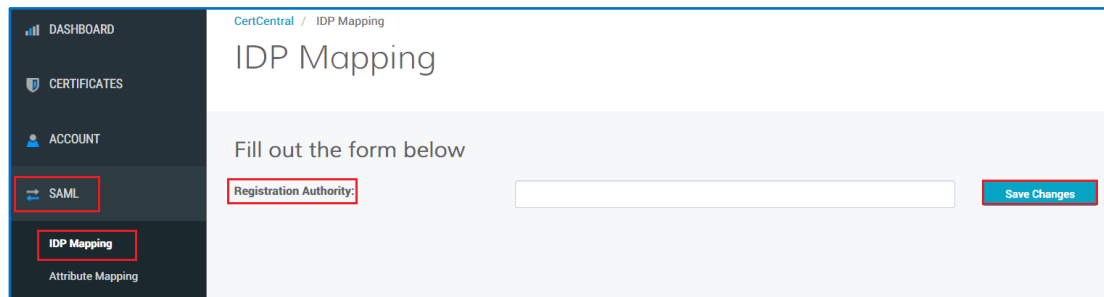|	
Common Name:	Enter the value for the common name or name to be displayed
Email Address:	Enter the value for the email address.
Organization:	Enter the value for the organization (e.g., *schacHomeOrganization*).
Person ID:	Enter the value for the person's personal ID.
Username:	Enter the value for the person's username.
Overwrite default values	Check this box to overwrite the default 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 GÉANT 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 > IPD Mapping**.
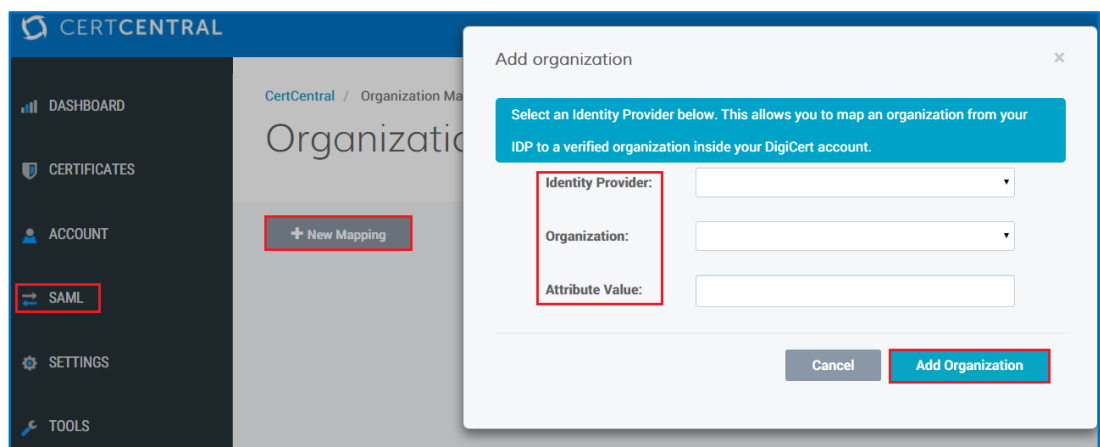

2. On the **IDP Mapping** page, in the **Registration Authority** box, enter the straight string match from the value entered in the UI form and the *registrationAuthority* in IPD metadata.

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 (e.g., *schacHomeOrganization*). When the Participant SAML Admin adds a mapping, they 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**.

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 attribute value (e.g., *schacHomeOrganization*).

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

About DigiCert

DigiCert is a premier provider of security solutions and certificate management tools. We have earned our reputation as the **security industry leader** by building innovative solutions for SSL Certificate management and emerging markets.

DIGICERT
2600 WEST EXECUTIVE PKWY STE. 500
LEHI, UTAH 84043
PHONE: 801.701.9690
EMAIL: SALES@DIGICERT.COM