

SAML Admin Guide (GÉANT)

Version 1.6

Table of Contents

- 1 SAML Service Workflow 3
 - 1.1 Step 1: GÉANT Level 3
 - 1.2 Step 2: NREN Level 3
 - 1.3 Step 3: Participant Level 3
 - 1.4 Step 4: New Login URL 3
- 2 SAML Role and Account Access 4
 - 2.1 SAML Admin Role 4
 - 2.1.1 GÉANT Level SAML Admin Role 4
 - 2.1.2 NREN Level SAML Admin Role 4
 - 2.1.3 Participant Level SAML Admin Role 4
 - 2.2 Managing SAML Admins 4
 - 2.2.1 How to Create a SAML Admin Account/Add the SAML Admin Role 4
 - 2.2.2 How to Create Your New SAML Admin (Invitee) Account 6
 - 2.2.3 How to Create Your New SAML Admin User (Invitee) Account 7
 - 2.2.4 How to Approve/Activate an Invitee's SAML Admin Account 8
 - 2.2.5 How to Edit an Existing Account to Add the SAML Admin Role/Change the Account to a SAML Admin Account 8
- 3 Managing SAML Settings 10
 - 3.1 IDP Manager 10
 - 3.1.1 How to Configure the IDP Manager (GÉANT SAML Admin) 10
 - 3.2 Attribute Mapping 10
 - 3.2.1 How to Set Up Attribute Mapping (GÉANT or NREN SAML Admin) 10
 - 3.3 IDP Mapping 12
 - 3.3.1 How to Configure IDP Mapping (NREN SAML Admin) 12
 - 3.4 Organization Mapping 13
 - 3.4.1 How to Add an Organization Mapping (Participant SAML Admin) 13
- About DigiCert 15

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 **IDP Manager**, which they use to configure the allowed IDPs for the entire GÉANT system.

This admin can also access **Attribute Mapping**, which they use 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

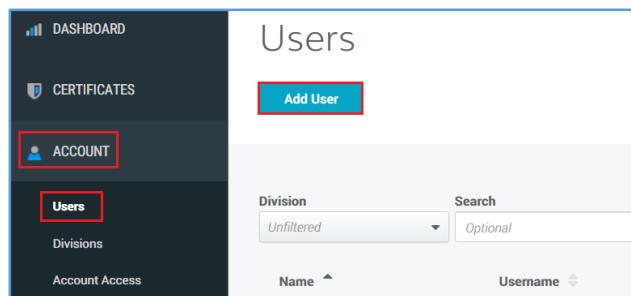
This SAML Admin can access **SAML Organization Mapping**, which they can use to map a validated organization from the DigiCert system to an organization that is specified in the SAML assertion (*schacHomeOrganization*).

2.2 Managing SAML Admins

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

Use this instruction to create new user accounts yourself. After creating the account, the user is sent an email with a link to set a password and to log into their account.

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**.

The screenshot shows a web form titled "Add User". Under the "User Details" section, there are five input fields: "First Name" (containing "Luke"), "Last Name" (containing "Warmly"), "Email" (containing "warmly@digicert.com"), "Phone" (containing "555-555-5555"), and "Job Title" (containing "Tepster"). Below the "Phone" and "Job Title" fields, there are small notes: "A phone number is required if this user will be requesting EV certificates." and "A job title is required if this user will be requesting EV certificates." respectively.

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

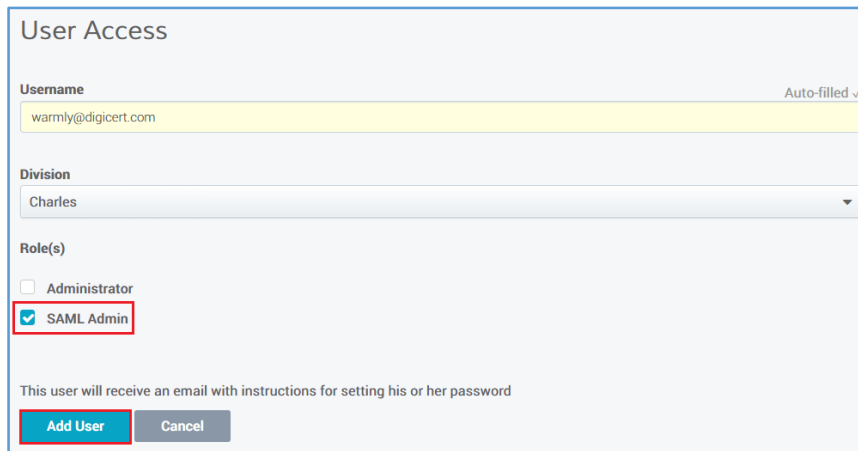
Username: The username will auto-populate.
Although you can create a unique username for each user, we recommend using their email address (e.g., *john@example.com*).

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.



The screenshot shows a 'User Access' form with the following fields and options:

- Username:** A text input field containing 'warmly@digicert.com' with an 'Auto-filled ✓' indicator.
- Division:** A dropdown menu with 'Charles' selected.
- Role(s):** A list of roles with checkboxes: 'Administrator' (unchecked) and 'SAML Admin' (checked). The 'SAML Admin' checkbox is highlighted with a red box.
- Message:** 'This user will receive an email with instructions for setting his or her password'.
- Buttons:** 'Add User' (highlighted with a red box) and 'Cancel'.

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 Create Your New SAML Admin (Invitee) Account

Use this instruction to send an email inviting a new user to set up their SAML Admin account themselves. Once the account is set up, you will need to go to the **User Invitations** page (**Account > User Invitations**) and approve/activate the new user account request.

1. In your account, in the sidebar menu, click **Account > User Invitations**.
2. On the **User Invitations** page, click **Invite New User**.
3. In the **Invite New Users** window, do the following:

Email Addresses

In the box, type the email addresses (comma separated) of the new users who you want to invite to join your account.

Send custom message

1. Check the box.
2. In the field that appears, type the message that you want to include in the new account invitee email.

4. When you are finished, click **Send Invitations**.

You should receive the ***“Invitations successfully sent”*** message.

2.2.3 How to Create Your New SAML Admin User (Invitee) Account

1. In your email account inbox, locate the ***Please create your user login for DigiCert CertCentral*** email, and click the link provided for creating your account user profile.
2. On the **Create CertCentral User** page, under **Personal Information**, provide the following information:

- **Email Address**
- **First Name**
- **Last Name**
- **Phone Number**
- **Job Title**

3. Under **Account information**, do the following:

Username

Create a username per your company’s policy (for example they may want you to use your email address as your username).

Password/Confirm Password

Create and confirm the password you want to use to log into your account.

Security Question/Security Answer

Select a security question and then answer it.

4. When you are finished, click **Enroll**.

- You should receive a ***Your request has been received*** email, which let you know that your account request has been sent to the account administrator for approval

- You cannot log into your account until your account request has been approved by your administrator, and you are notified via email (**User account for "User Name" has been approved**) that your request has been approved.

2.2.4 How to Approve/Activate an Invitee's SAML Admin Account

- In your account, in the sidebar menu, click **Account > User Invitations**.
- On the **User Invitations page**, use the filters and column headers to locate the new user account you want to approve/activate.
- To the right of the user account to want to activate, click the **Details** link.
- On the **User Invitation to "Username"** page, click **Approve**.
- In the **Approve User Invitation** window, provide the following information:

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.

Approval Message to Invitee Enter a message to be included in the approval email.

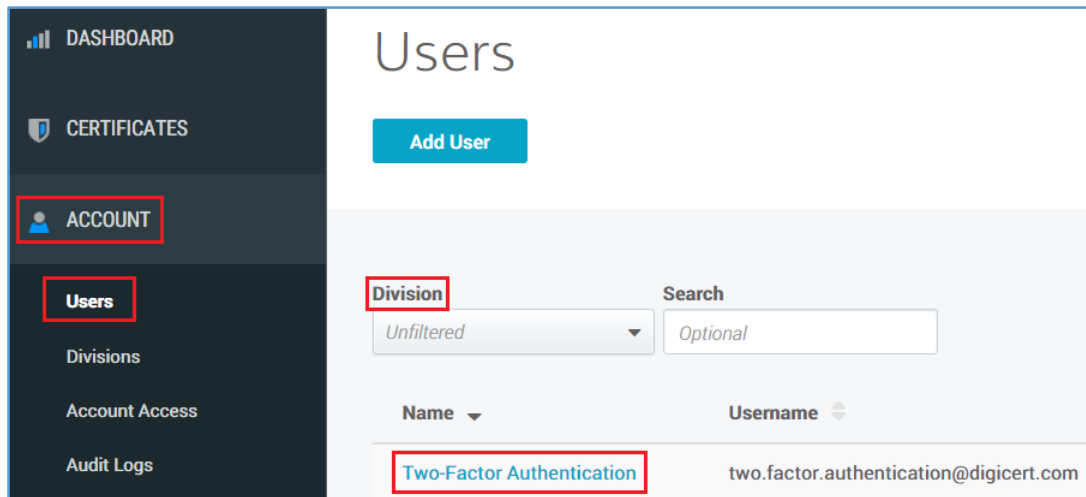
- When you are finished, click **Approve**.

The new user is added to your account (**Account > Users**). The new user is sent an email (**User account for "User Name" has been approved**) with a link which takes them to the account login page.

2.2.5 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.

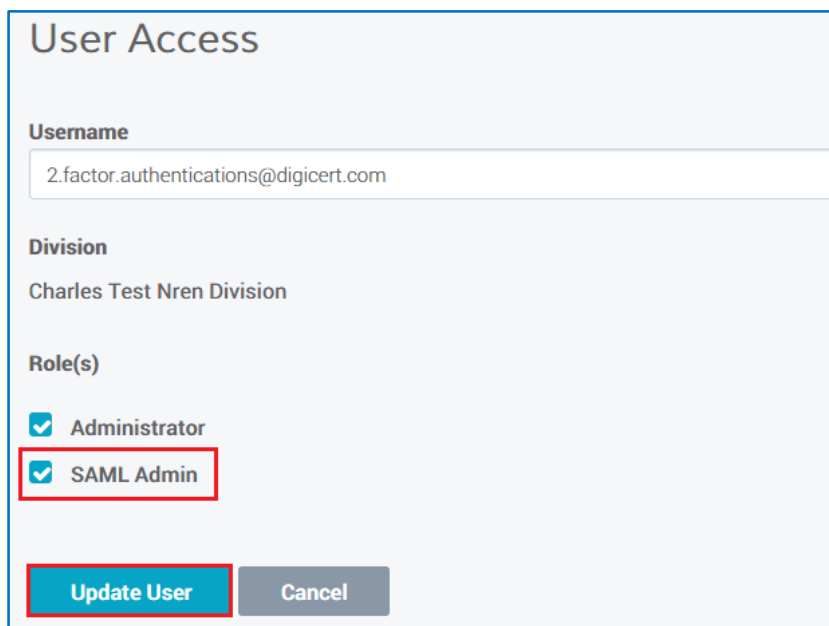
- In your account, in the sidebar menu, click **Account > Users**.



2. On the **Users** page, locate the user account whose role you want to modify and 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**.



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

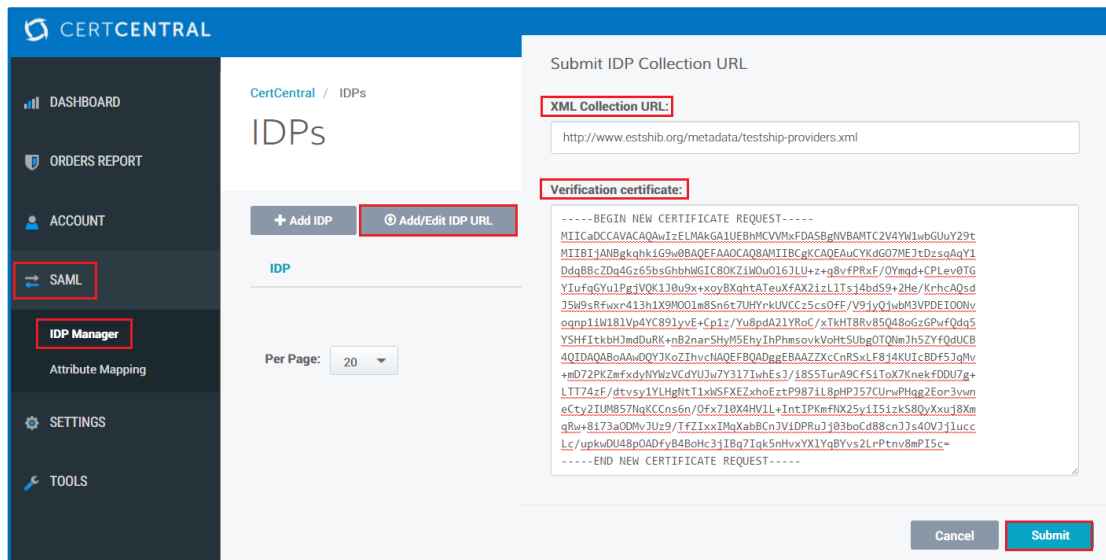
3 Managing SAML Settings

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.

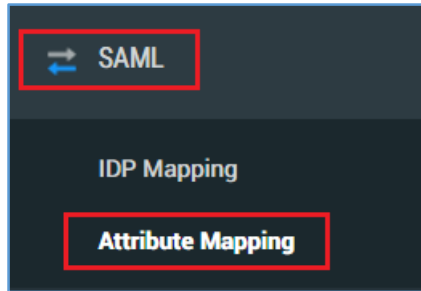
4. When you are finished, click **Submit**.

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.

 A screenshot of the 'Attribute Mapping' web interface. The 'Entitlements' section is highlighted in light blue. Below it, a teal banner contains the text: 'Every entitlement below can have multiple attribute values separated by a new line. Each line represents the preferred order.' Underneath, the 'Ordering certificates' section is visible. It includes a checkbox labeled 'Overwrite default values' which is checked and highlighted with a red box. Below this checkbox, the attribute name 'urn:oid:1.3.6.1.4.1.5923.1.1.1.1' is displayed in a yellow box. The 'Attribute name:' and 'Attribute value(s):' labels are also highlighted with red boxes. A text input field containing the word 'Staff' is visible at the bottom right of the section.

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.

The screenshot shows the 'IDP Attribute Map' configuration page. At the top, a blue banner states: 'Every attribute map below can have multiple attribute names separated by a new line. Each line represents the preferred order.' Below this, there is a table of attributes. On the left side, a red box highlights the labels for 'Common Name:', 'Email Address:', 'Organization:', 'Person ID:', and 'Username:'. On the right side, there is a checked checkbox labeled 'Overwrite default values' (also highlighted with a red box). Below the checkbox, there are four rows of URNs: 'urn:oid:2.5.4.3', 'urn:oid:1.3.6.1.4.1.5923.1.1.1.6', 'urn:oid:1.3.6.1.4.1.5923.1.1.1.1', and 'urn:oid:2.5.4.42'. At the bottom right, there is a blue 'Save Changes' button highlighted with a red box.

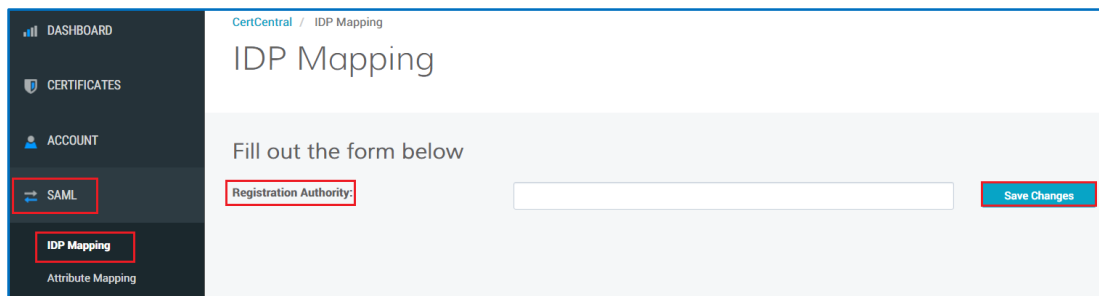
- When you are finished, click **Save Changes**.

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)

- In your account, in the sidebar menu, click **SAML > IPD Mapping**.



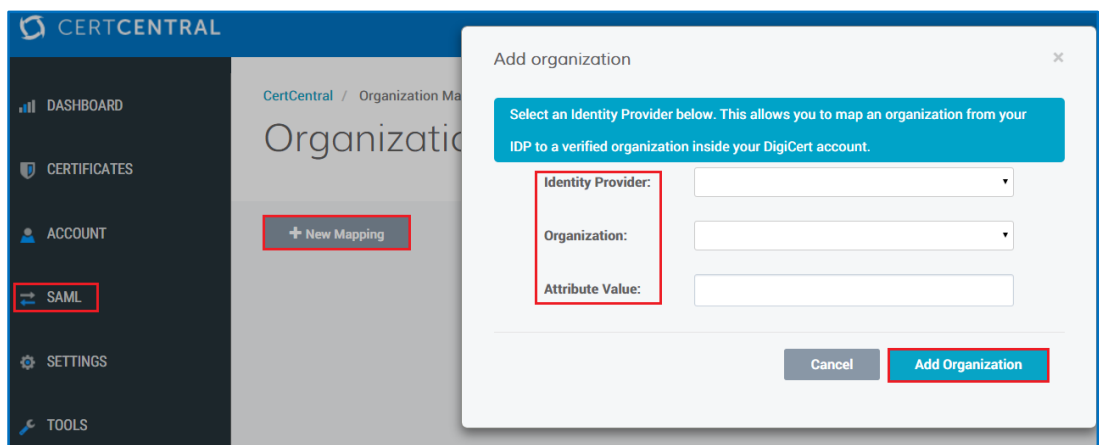
2. On the **IDP Mapping** page, in the **Registration Authority** box, enter the straight string match from the value entered in the UI form and the *registrationAuthority* in IPD metadata.
3. When you are finished, click **Save Changes**.

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., *schachHomeOrganization*). When the Participant SAML Admin adds a mapping, they can select their IDP, their DigiCert Organization, and enter in their *schachHomeOrganization* 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



© 2015 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.