https://cloudblue.com

Documentation Modules Account Settings

Single Sign-On

This article has been generated from the online version of the documentation and might be out of date. Please, make sure to always refer to the online version of the documentation for the up-to-date information.

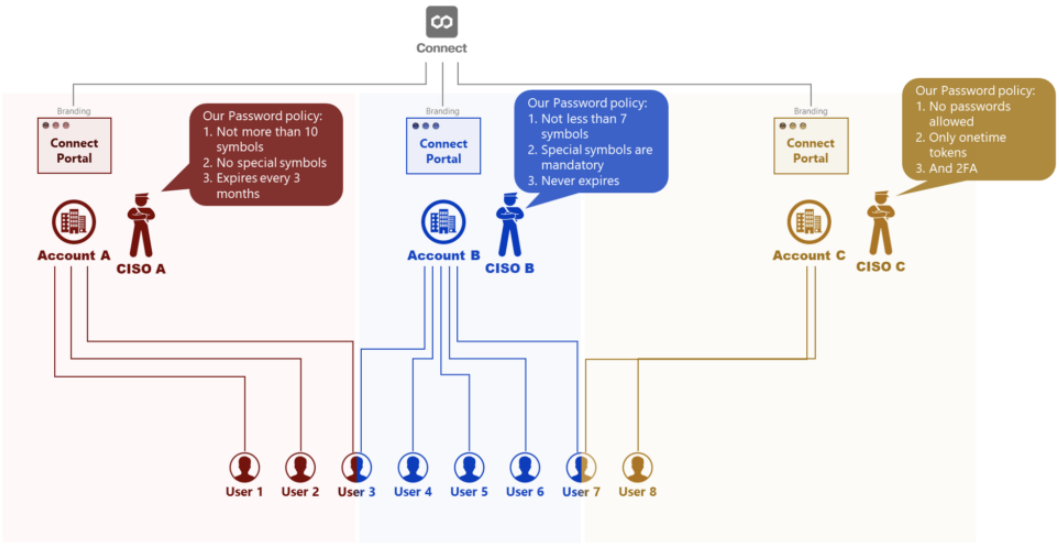
Auto-generated at November 21, 2024

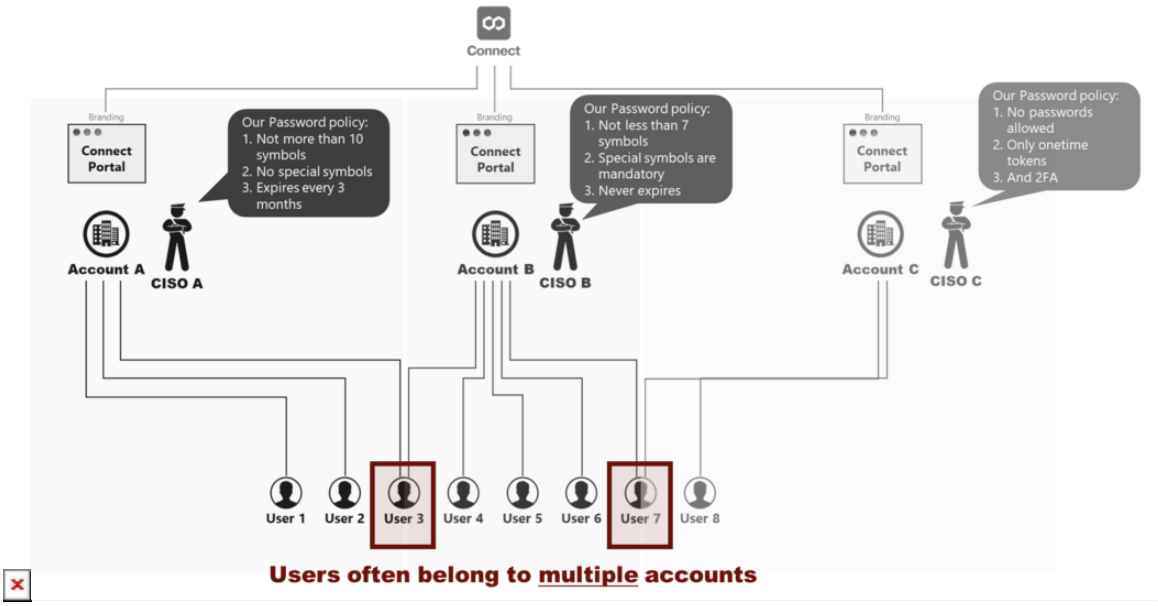
Access the **Single Sign-On** (SSO) section of the Account module to implement single sign-on authentication and manage your domains on the CloudBlue Connect platform. This section provides a comprehensive set of settings that can be increasingly helpful for security departments and Chief Information Security Officers (CISO). The following outlines the SSO concept and provides instructions on how to successfully configure a SSO domain on the Connect platform.

Why SSO is Important?

Single Sign-On represents a centralized session and user authentication scheme in which same credentials can be used to login into the CloudBlue Connect platform along with other services and systems. Thus, the SSO schema can be greatly beneficial for companies. For example, SSO reduces password fatigue and drastically improves security across organizations.

It is important to note that each organization often includes security policies that can be incompatible with the policies of another organization. The following diagrams showcase such examples:



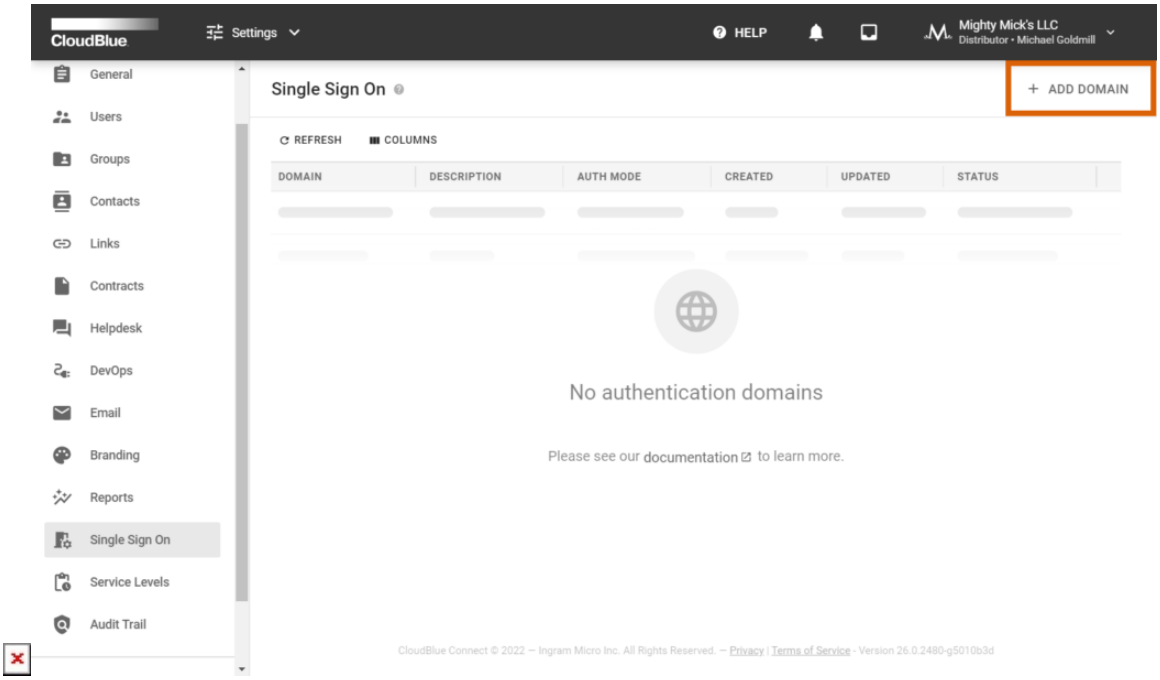


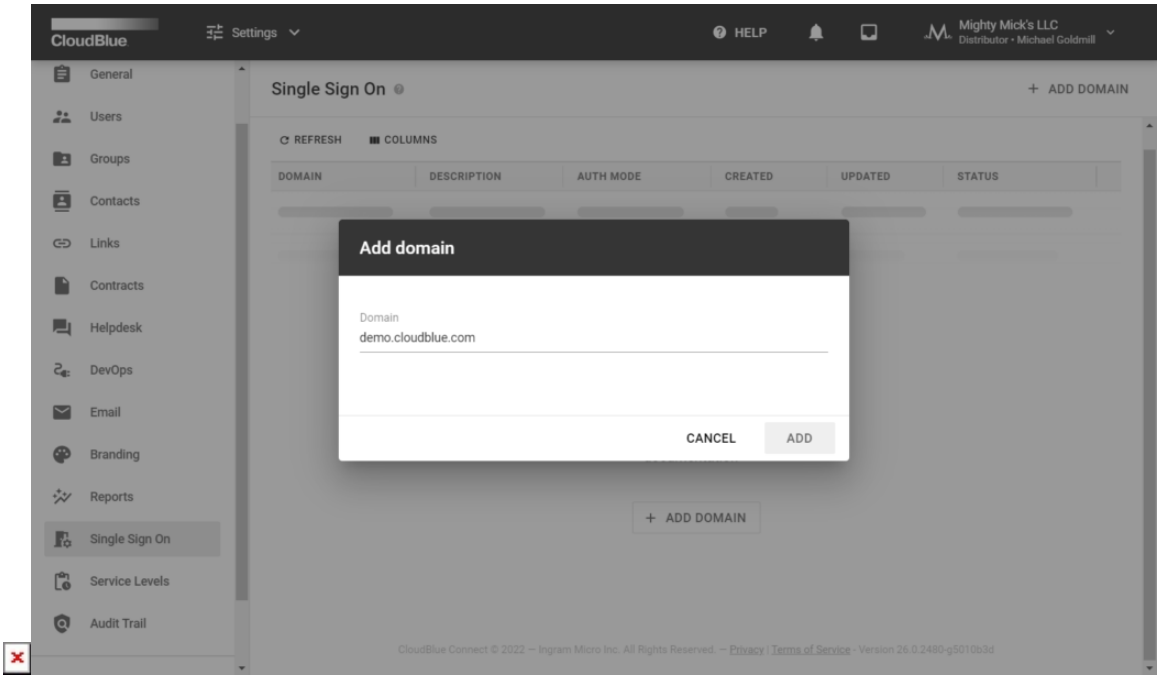
These diagrams introduce Connect accounts (*A*, *B*, and *C*) that collaborate by using the Connect platform. Each account incorporates own password policy that contradicts with the policies of other accounts. For example, *CISO A* doesn't allow using special symbols, while *CISO B* requires to include at least one special symbol to a password. In addition, *CISO C* doesn't allow specifying any passwords to begin with. Note that certain users (such as *User 3* and *User 7*) often belong to multiple Connect account. Therefore, deploying the SSO schema can be essential for many business scenarios.

Note that one Connect account can also include several domains. In addition, multiple Connect accounts can also belong to the same domain. Follow the instructions below to configure your domain for SSO authorization.

Adding Domains

Access the **Single Sign-On** section from the Accounts module. Thereafter, click **Add Domain** to specify your authentication domain on the Connect platform.



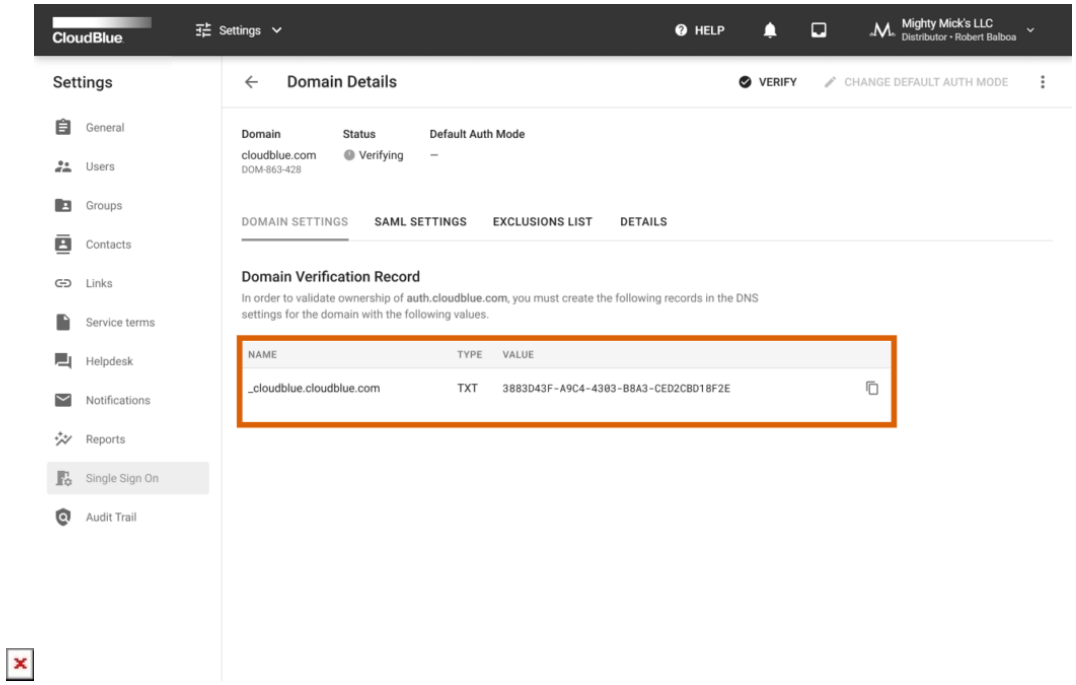


Specify your domain in the following form and click the **Add** button. Once your domain is successfully added, the system assigns the *Verifying* status to your domain instance. It is necessary to verify your domain as described below.

Domain Verification

Validate the ownership of your added domain by creating a **DNS Record**. Your DNS record should contain specific values that are provided within the Domain Details screen. The following steps showcase how to access required values and verify your domain:

1. Click on your domain to access the **Domain Details** screen.
2. Create a TXT DNS record that should be named as it is displayed in the **Domain Settings** tab.
3. Copy-paste the provided **Value** to your created TXT record.
4. Click the **Verify** button at the top-right corner of the **Domain Details** screen.



As a result, the system assigns the *Verified* status to your domain once the verification operation is complete. Otherwise, the system may return an error.

General Recommendations

In case the system returns an error, make sure that your specified values are correct. Furthermore, note that DNS changes can take a while to be applied. It is recommended to wait a few hours, reopen your domain and try to verify it again. If the system still fails the verification operation, try to add a different DNS TXT record.

In addition, once your domain is verified successfully, it is highly recommended to systematically reverify your domain on Connect platform in order to prevent possible issues with your SSO authorization.

Default Auth Modes

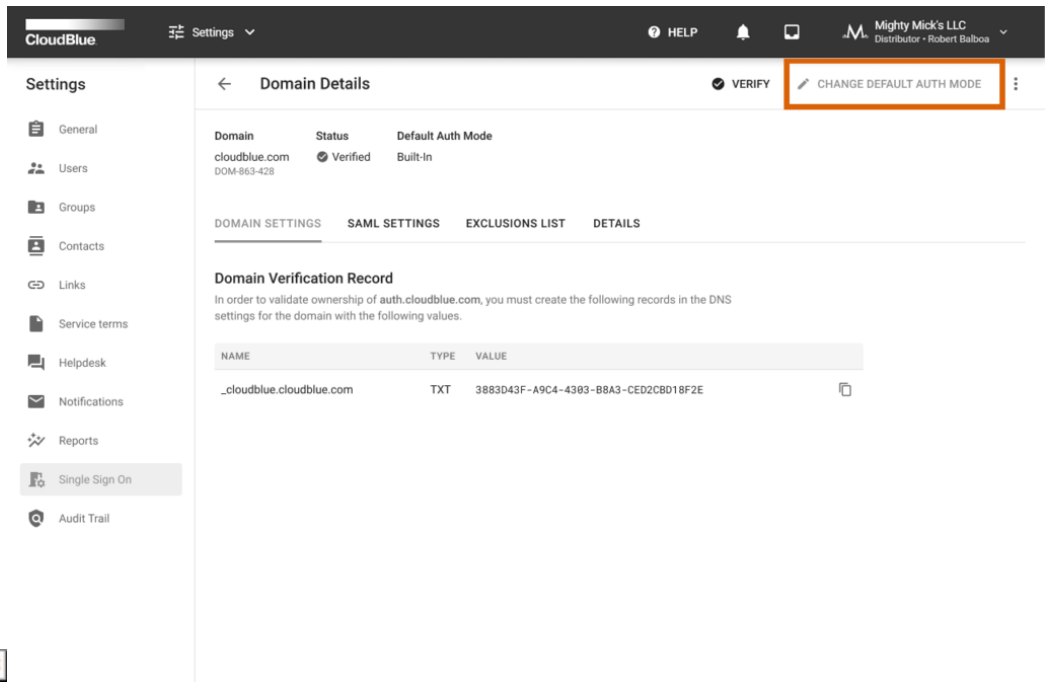
Once your domain is successfully verified, the Connect platform allows changing your default authentication modes. These default authentication modes represent using the *Built-In* authentication page and using the external *SAML-based* authentication.

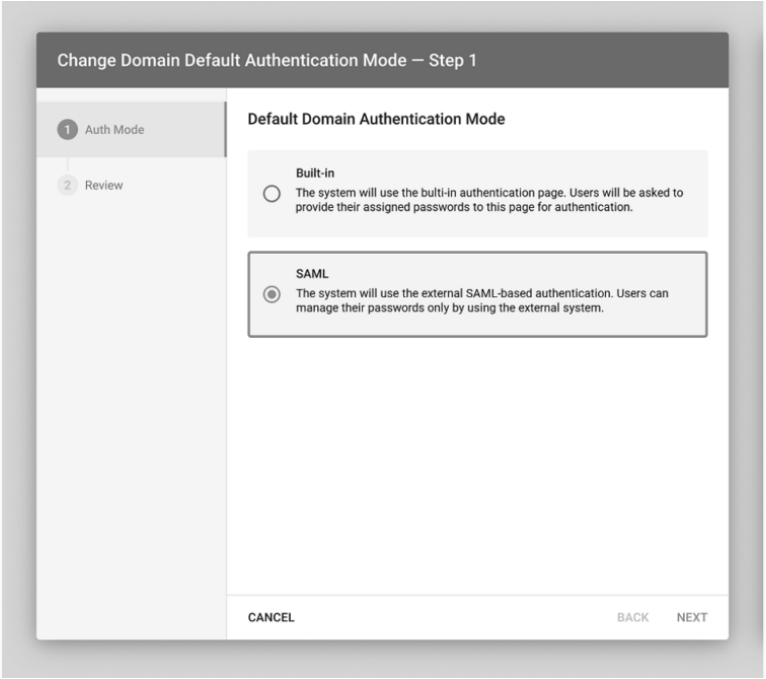
Built-In vs. SAML-based auth modes

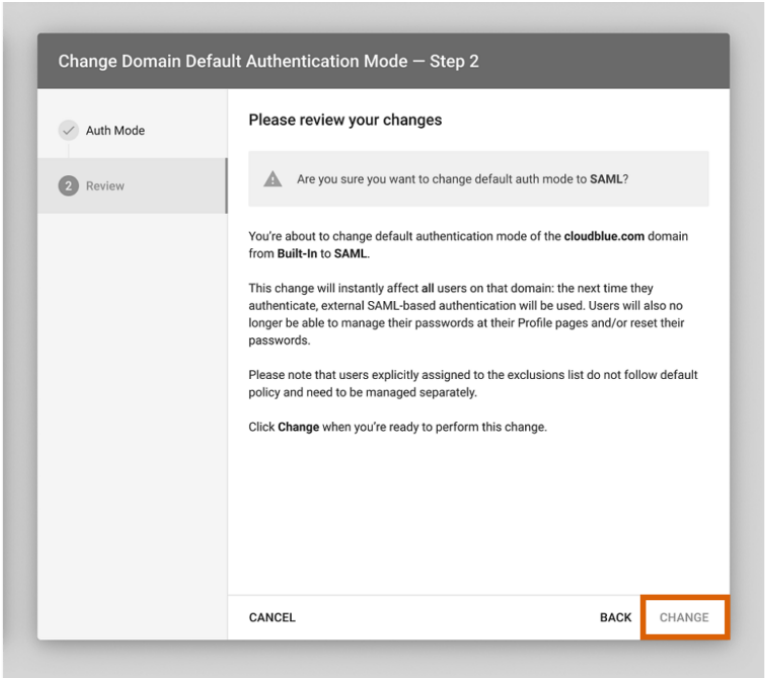
In case the *Built-In* mode is selected, the system uses the built-in authentication page. Therefore, your users will be asked to provide their passwords for authentication. Users that don't have passwords will be asked to assign them for the first use.
If the *SAML-based* mode is selected, the system uses the external SAML-based authentication. Thus, your users will not be able to manage their passwords via the Profile page and reset their passwords. Such operations should be performed by contacting external system administrators.

Note that users that are assigned to the *Exclusions List* will not follow the selected authentication mode. Such users should be managed via the Exclusions List tab of the Domain Details screen.

The system requires to provide required configurations within the SAML Settings before switching your default mode. Once all required configurations are presented, switch your authorization mode as follows:







1. Click the **Change Default Auth Mode** button at the top-right corner of the Domain Details screen.
2. Thereafter, select your default authorization mode by using the following wizard.
3. The system allows reviewing the selected mode. Confirm your decision by clicking the **Change** button.

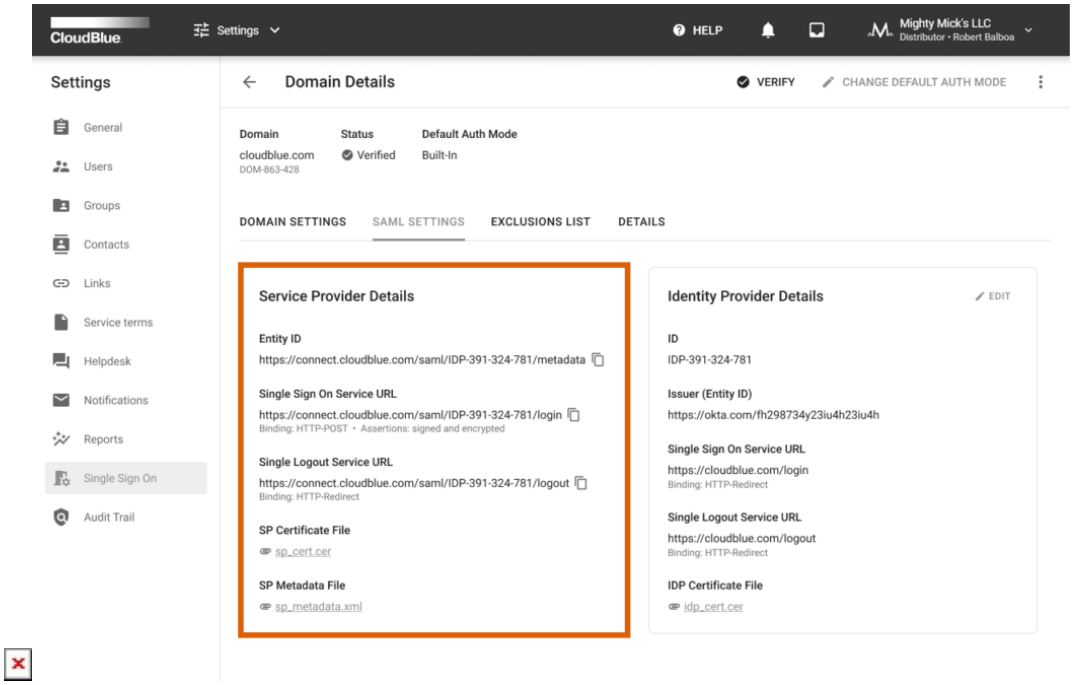
As a result, the system will successfully change your default authentication mode.

SAML Settings

The Security Markup Language (SAML) settings are available once your domain is successfully *verified*. Navigate to the **SAML Settings** tab from the Domain Details screen to access the following data and configuration options:

Service Provider Details

The SAML Settings tab allows you to view the Service Provider details that are used to handle SAML assertions. Service Provider represents the CloudBlue Connect platform. Thus, the system provides a quick access to the following details:



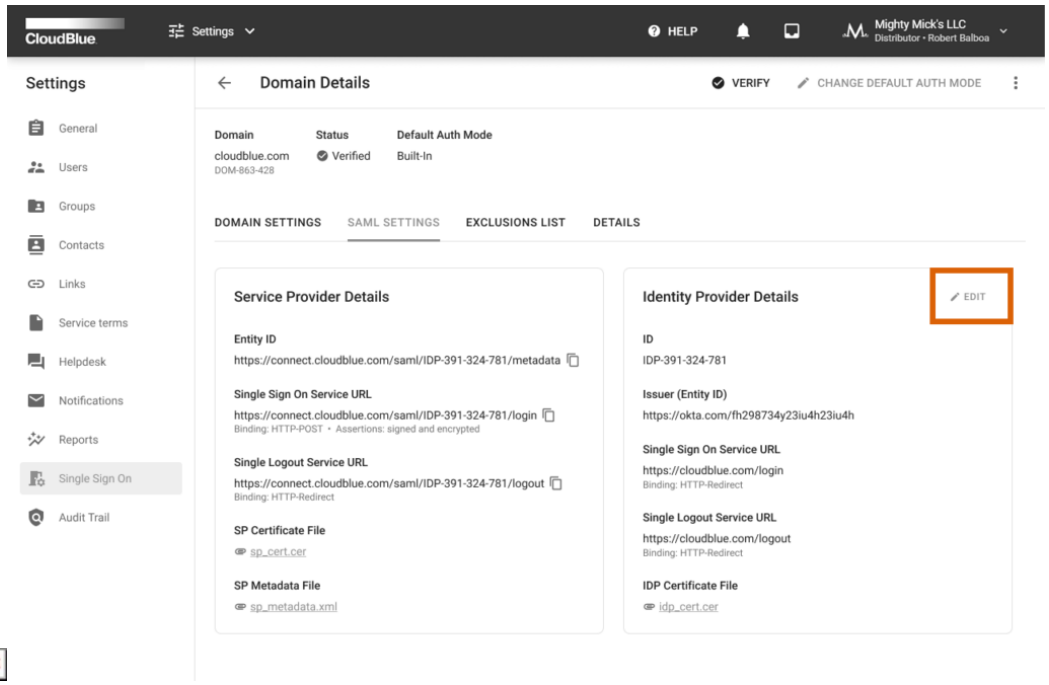
- **Entity ID**: Displays the Service Provider Entity ID URL.
- **Single Sign-On Service URL**: Specifies the SSO Service URL, its binding and assertions.
- **Single Logout Service URL**: Provides the Single Logout service URL and its binding.
- **SP Certificate File**: Download the Service Provider certificate file by using this link.
- **SP Metadata File**: Access the Service Provider metadata file by using this link.

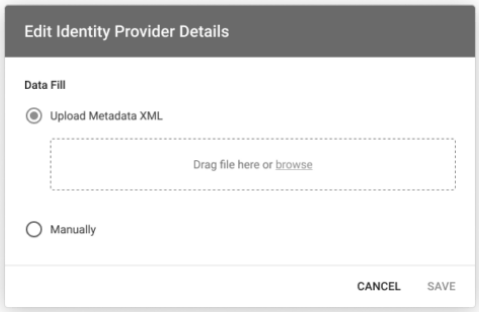
> ●
> Information
>
> Note that Service Provider metadata differs for each verified domain.

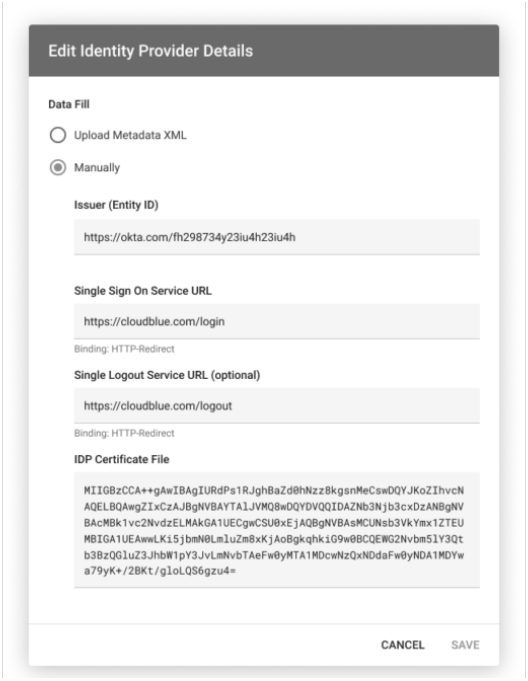
Identity Provider Details

The SAML Settings tab enables you to access and change the identity provider details. Click the **Edit** button to launch a wizard and specify your selected identity provider details.

> Azure Active Directory Example
>
> You can use Azure Active Directory as your *Identity Provider*. Refer to the Azure Active Directory documentation for instructions on how to use your configured Active Directory as SSO domain on the Connect platform.







Upload a metadata XML file with your specified identity provider values. Alternatively, select the manual option to specify required details by using the provided form.

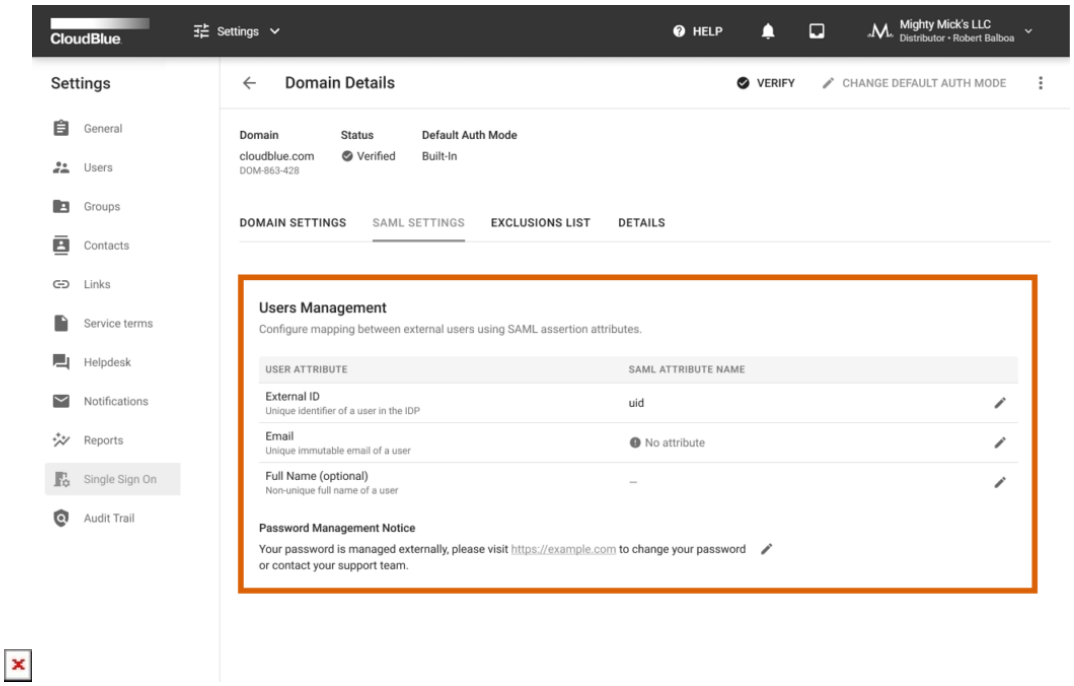
- **Issuer (Entity ID)**: Specify the issuer in this field. This value should contain the Entity ID URL.
- **SSO Service URL**: Enter your Single Sign-On URL in this field.

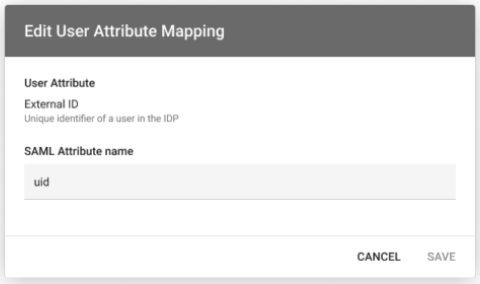
- **Single Logout Service URL**: Enter your Single Logout Service URL (if supported).
- **IDP Certificate File**: Provide the Identity Provider certificate in the PEM format (base64 encoded)

Note that the Connect platform supports only the *HTTP-Redirect* binding for the Identity Provider (IDP) setup. Once your file is uploaded or the provided form is filled out, click the **Save** button to save your adjustments.

Users Management

The SAML Settings tab is used to configure mapping between external users via the SAML assertion attributes. Namely, it is required to specify SAML attribute names for **External ID** and **Email**. Connect users can also specify **Full Name** attribute if necessary. Furthermore, this tab allows specifying password recovery links and other password management notifications for the external SAML authentication.

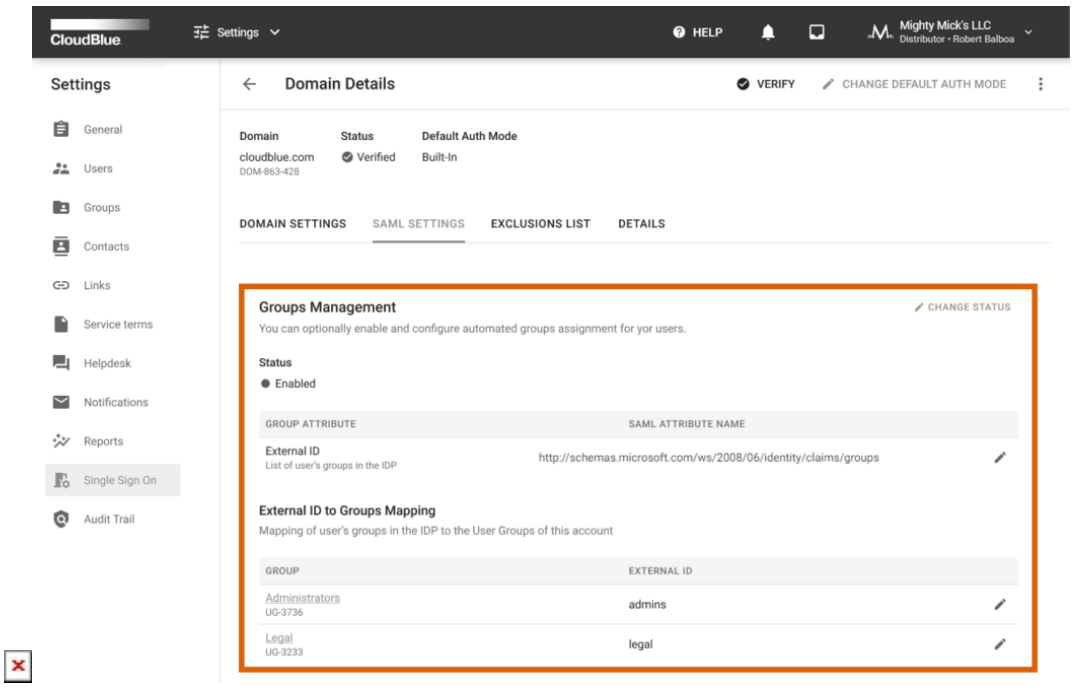




Click on the *edit* icon next user attribute to change its SAML attribute name. In addition, click on the edit icon under **Password Management Notice** to provide a required message or password management instructions for the SAML-based authentication.

Groups Management

The SAML Settings tab allows enabling and configuring automated groups assignment for your users. Namely, the groups management feature is especially helpful to automatically map your new users to required groups on Connect. Once your domain is successfully verified, click the **Change Status** button and switch **Enable Groups Mapping** on to activate the groups management.



In case the group management is enabled, use the corresponding *edit icon* to change the **SAML Attribute Name** for your group attributes. This attribute name is required to define your URI address for SAML assertions. For example, this may include your group claim from Azure Active Directory.

In addition, the provided interface also enables you to map user groups within your IDP to user groups of your Connect account. Namely, you can assign external identifiers to your account groups by using the corresponding *edit icons*. For instance, your assigned external IDs may represent email addresses of your users.

> ▲
> Warning
>
> Note that your IDP cannot be used to manage your groups on the Connect platform. Your Connect groups will not be automatically created or removed within your IDP. Thus, in case it is necessary to remove your group from the mapping operations, you can simply remove its external ID.
>
> Furthermore, new users that are presented within your IDP and that are not registered on Connect will be signed into the Connect platform in the *restricted* mode.

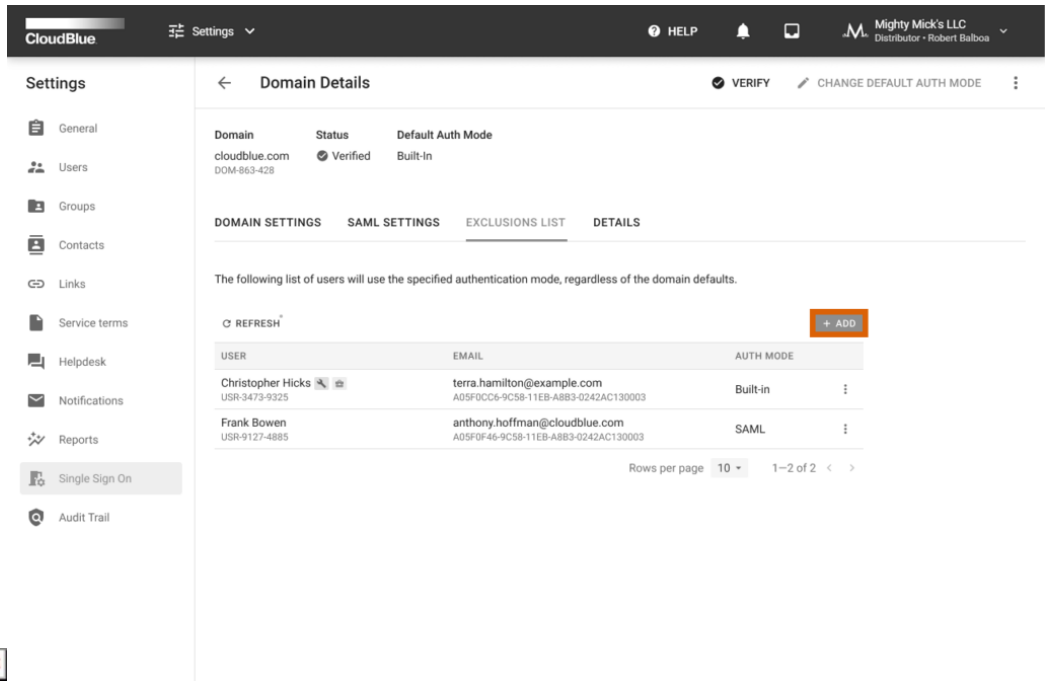
Exclusions List

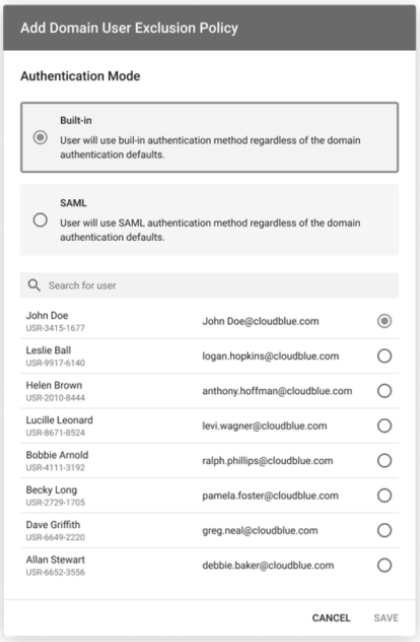
Access the **Exclusions List** tab to add users that will use your specified authentication mode, regardless of your default authentication mode. Therefore, the system allows combining both authentication modes and assign specific mode for certain users. Note that using the exclusions list is available only if your domain is successfully verified.

Information

Switching to the SAML-based authorization mode requires to have at least one user in the Exclusions list with the Built-In authentication. Therefore, in case of an error with your SSO system, you will have access to the Connect platform as this user.

It is also recommended to add one or several users to the Exceptions list to test out your SSO system. Thereafter, you can safely switch your domain from the Built-In mode to the SAML mode.





Click the **Add** button to add new users to the Exclusions List. Specify a required authentication mode and select required users from the list. Thereafter, click the Save button to save your adjustments.

In case you need to remove a user from the Exclusions List. Click on the vertical ellipsis (⋮) icon next to your selected user from the **Exclusions List** tab. Thereafter, click the **Remove** button to remove this user from the list.

Details

The **Details** tab displays your domain description. Edit the domain description by clicking on the corresponding edit icon. In addition, use this tab to review your domain *creation*, *update* and *verification* operation time and date.