



<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This article has been generated from the online version of the documentation and might be out of date.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

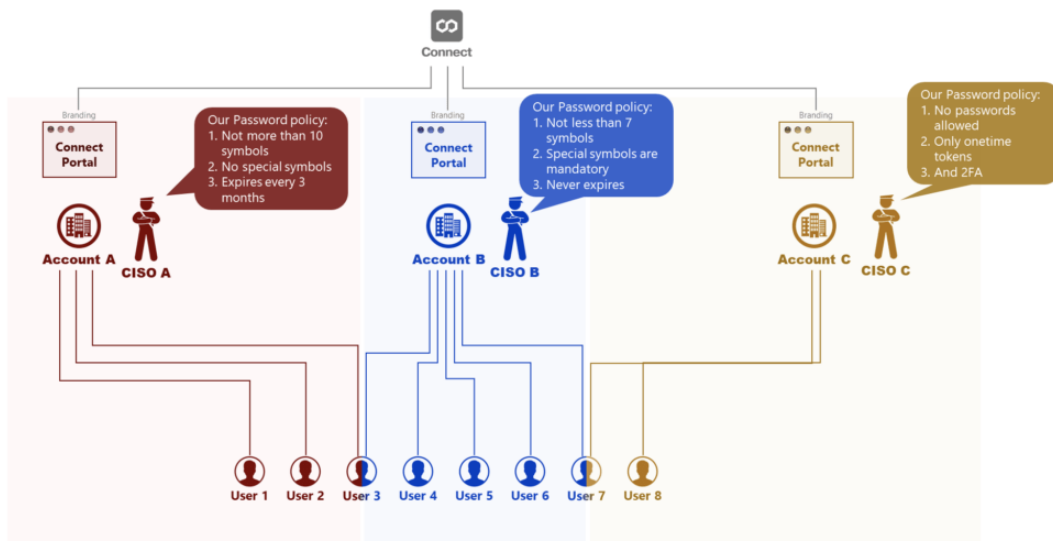


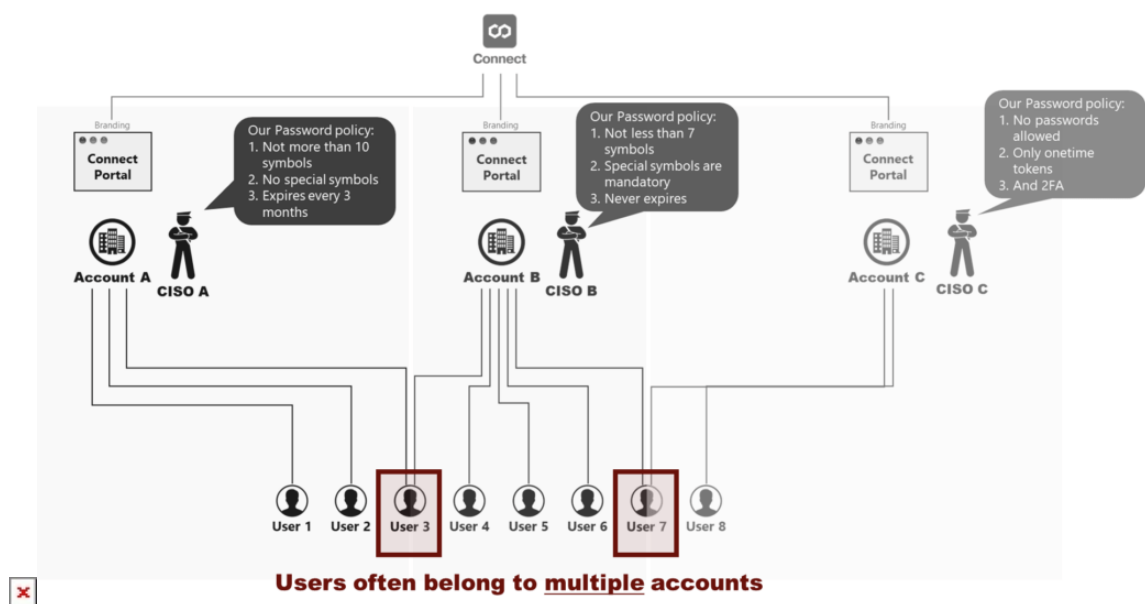
Access the **Single Sign-On (SSO)** section of the Account module to implement single sign-on authentication and manage your domains on the CloudBlue Connect platform. This section provides a comprehensive set of settings that can be increasingly helpful for security departments and Chief Information 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:



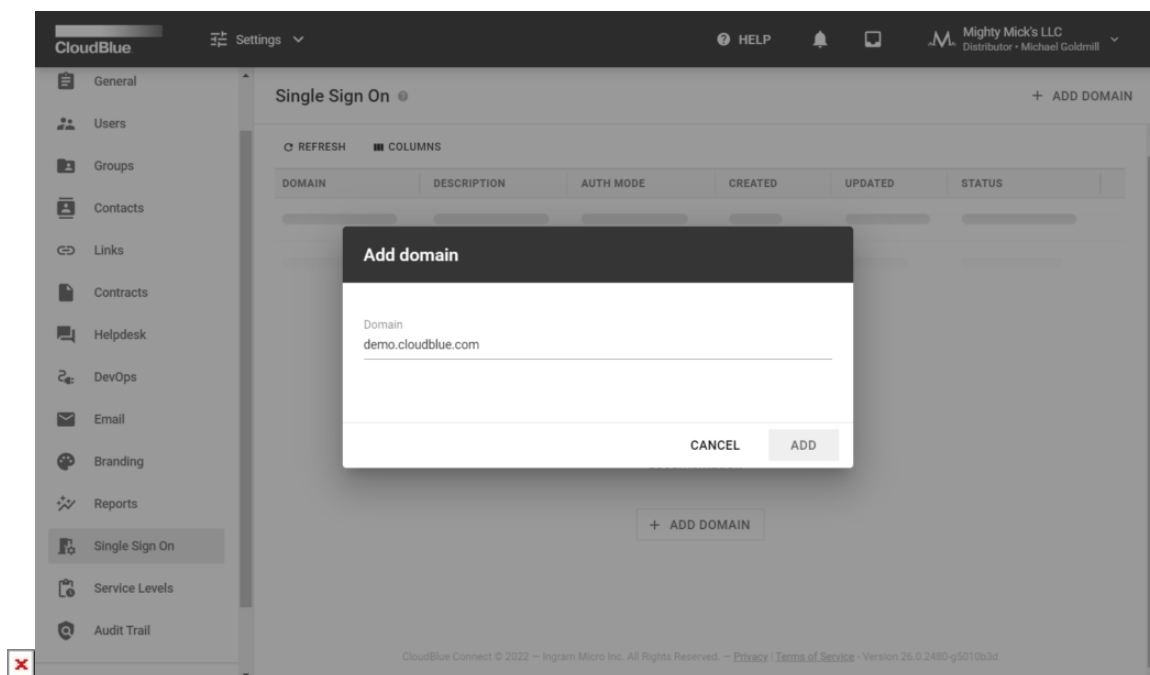
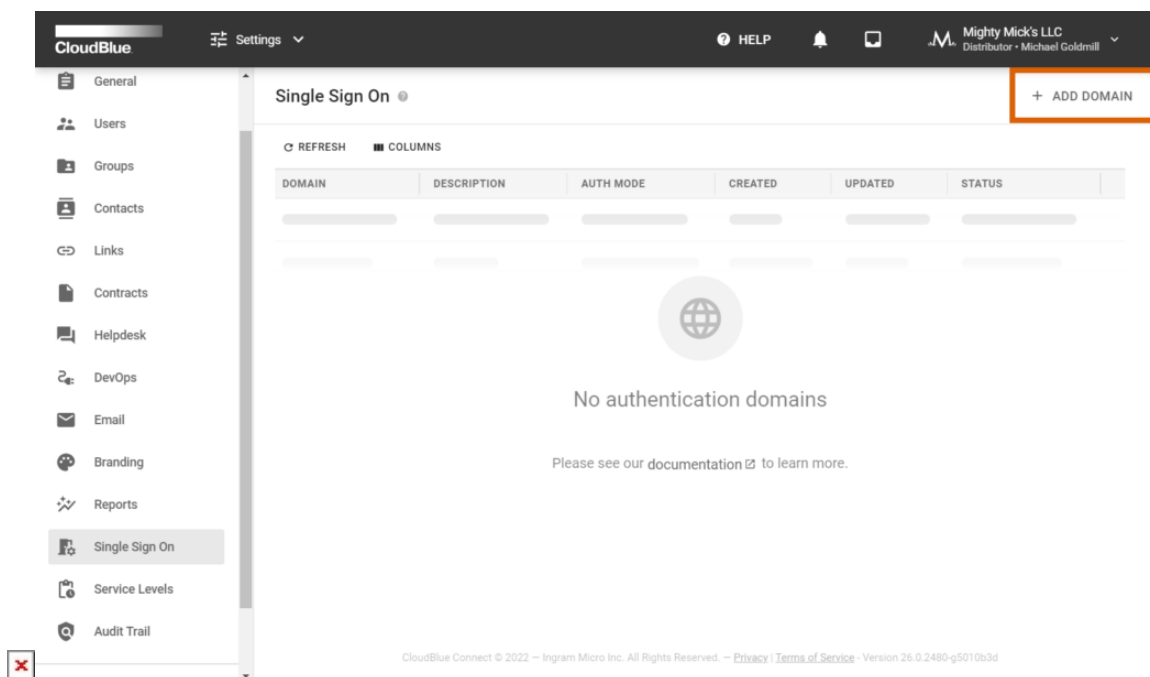


These diagrams introduce Connect accounts (A, B, and C) that collaborate by using the Connect platform. Each account incorporates own password policy that contradicts with the policies of other accounts. For example, *CISO A* doesn't allow using special symbols, while *CISO B* requires to include at 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.



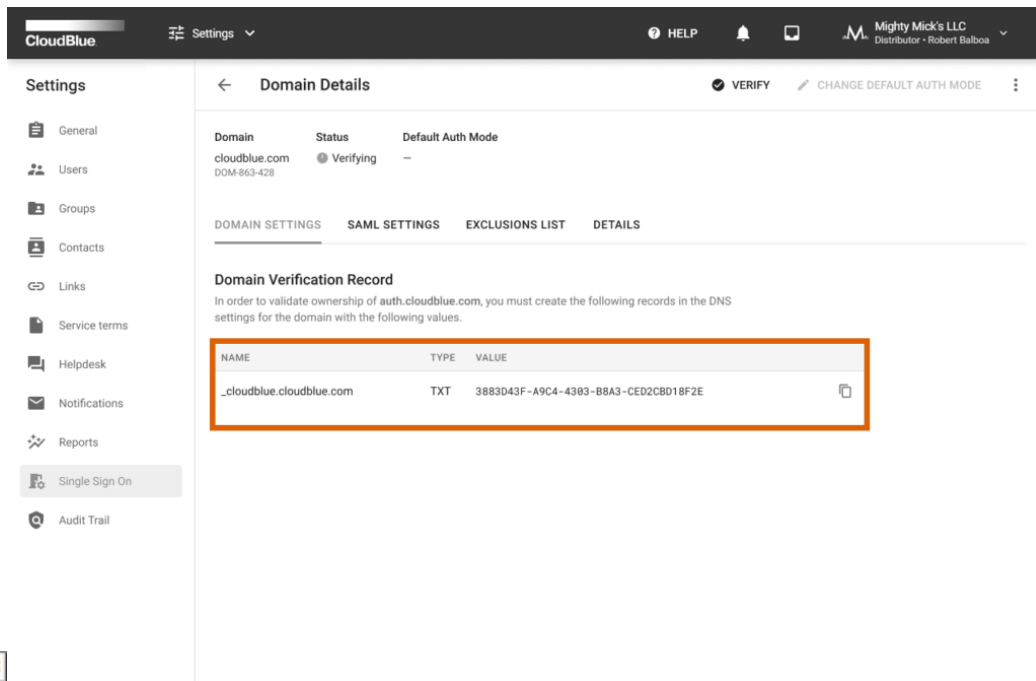
Specify your domain in the following form and click the **Add** button. Once your domain is successfully added, the system assigns the *Verifying* status to your domain instance. It is necessary to verify your domain as described below.



## 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.

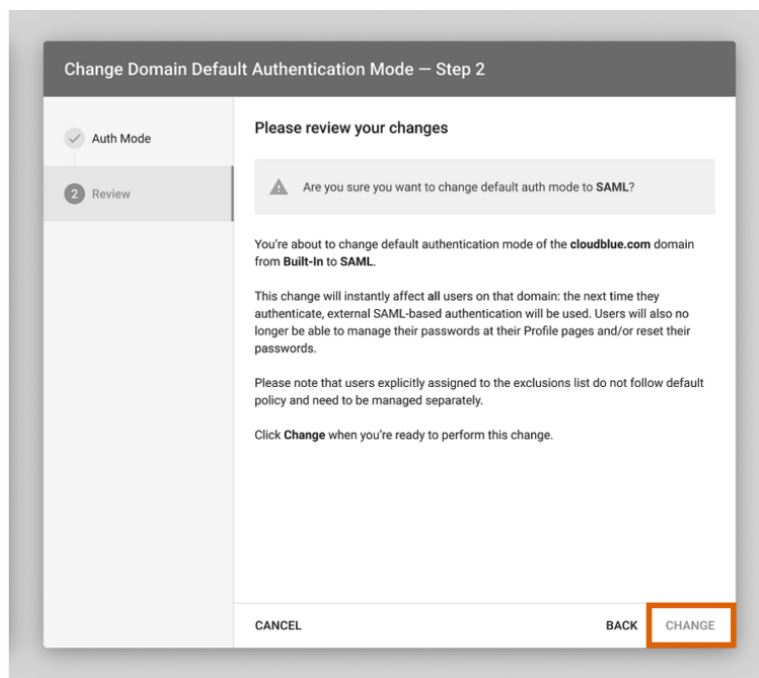
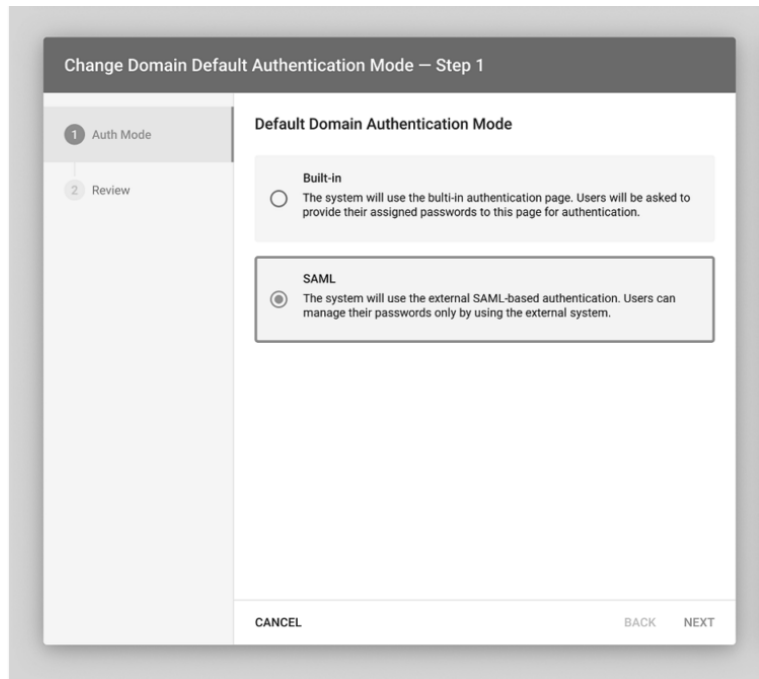
Note that users that are assigned to the *Exclusions List* will not follow the selected authentication mode. Such users should be managed via the Exclusions List tab of the Domain Details screen.

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:

The screenshot shows the CloudBlue interface for 'Domain Details'. The top navigation bar includes 'CloudBlue', 'Settings', 'HELP', and 'Mighty Mick's LLC'. The left sidebar lists various settings categories. The main content area shows the domain 'cloudblue.com' with a 'Verified' status and 'Built-In' as the default auth mode. Below this, there are tabs for 'DOMAIN SETTINGS', 'SAML SETTINGS', 'EXCLUSIONS LIST', and 'DETAILS'. A 'Domain Verification Record' section provides instructions and a table of DNS records.

NAME	TYPE	VALUE
._cloudblue.cloudblue.com	TXT	3883D43F-A9C4-4393-B8A3-CED2CB018F2E





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:

The screenshot shows the CloudBlue interface for SAML Settings. The left sidebar contains a 'Settings' menu with 'Single Sign On' selected. The main content area is titled 'Domain Details' and shows a table with columns for Domain, Status, and Default Auth Mode. Below this, there are tabs for 'DOMAIN SETTINGS', 'SAML SETTINGS', 'EXCLUSIONS LIST', and 'DETAILS'. The 'SAML SETTINGS' tab is active, displaying two panels: 'Service Provider Details' (highlighted with an orange border) and 'Identity Provider Details'. The 'Service Provider Details' panel includes the following information:

- Entity ID:** <https://connect.cloudblue.com/saml/IDP-391-324-781/metadata>
- Single Sign On Service URL:** <https://connect.cloudblue.com/saml/IDP-391-324-781/login>  
Binding: HTTP-POST - Assertions: signed and encrypted
- Single Logout Service URL:** <https://connect.cloudblue.com/saml/IDP-391-324-781/logout>  
Binding: HTTP-Redirect
- SP Certificate File:** [sp\\_cert.cer](#)
- SP Metadata File:** [sp\\_metadata.xml](#)

The 'Identity Provider Details' panel includes the following information:

- ID:** IDP-391-324-781
- Issuer (Entity ID):** <https://okta.com/fh298734y23iu4h23iu4h>
- Single Sign On Service URL:** <https://cloudblue.com/login>  
Binding: HTTP-Redirect
- Single Logout Service URL:** <https://cloudblue.com/logout>  
Binding: HTTP-Redirect
- IDP Certificate File:** [idp\\_cert.cer](#)



- **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.

The screenshot shows the CloudBlue Settings page for a domain named 'cloudblue.com'. The 'SAML SETTINGS' tab is selected. The 'Identity Provider Details' section is highlighted with an orange border and contains an 'EDIT' button. The details include:

Service Provider Details	Identity Provider Details
<b>Entity ID</b> https://connect.cloudblue.com/saml/IDP-391-324-781/metadata	<b>ID</b> IDP-391-324-781
<b>Single Sign On Service URL</b> https://connect.cloudblue.com/saml/IDP-391-324-781/login Binding: HTTP-POST • Assertions: signed and encrypted	<b>Issuer (Entity ID)</b> https://okta.com/ft298734y23iu4h23iu4h
<b>Single Logout Service URL</b> https://connect.cloudblue.com/saml/IDP-391-324-781/logout Binding: HTTP-Redirect	<b>Single Sign On Service URL</b> https://cloudblue.com/login Binding: HTTP-Redirect
<b>SP Certificate File</b> sp_cert.cer	<b>Single Logout Service URL</b> https://cloudblue.com/logout Binding: HTTP-Redirect
<b>SP Metadata File</b> sp_metadata.xml	<b>IDP Certificate File</b> idp_cert.cer





Edit Identity Provider Details

**Data Fill**

Upload Metadata XML

Drag file here or [browse](#)

Manually

**CANCEL**    **SAVE**



Edit Identity Provider Details

**Data Fill**

Upload Metadata XML

Manually

**Issuer (Entity ID)**

https://okta.com/fh298734y23iu4h23iu4h

**Single Sign On Service URL**

https://cloudblue.com/login

Binding: HTTP-Redirect

**Single Logout Service URL (optional)**

https://cloudblue.com/logout

Binding: HTTP-Redirect

**IDP Certificate File**

```

MIIGBzCCA++gAwIBAgIUrdPs1RjghBaZd8hNzz8kgSnMeCswDQYJKoZIhvcN
AQELBQAwgZIx CzA JBgNVBAYTAJJVMQ8wDQYVQIQIDAzNB3Njb3cxZzANBgNV
BAcMBk1vc2NvdzELMAkGA1UECgwCSU8x E J AQBgNVBAsMCUNsb3VxYmx1ZTEU
MBIGA1UEAwMLK35jbnN8Lm1uZm8xKjAoBgkqhkiG9w0BCQEwG2Nvb51Y3Qt
b3BzOQ1uZ3JhbW1pY3JvLmNvbTAeFw0yMTA1MDcwNzQxNDdaFw0yMTA1MDYw
a79yK+/2BKt/g1oLS6gzu4=
          
```

**CANCEL**    **SAVE**



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.

The screenshot shows the CloudBlue interface for SAML Settings. The left sidebar contains a 'Settings' menu with options: General, Users, Groups, Contacts, Links, Service terms, Helpdesk, Notifications, Reports, Single Sign On, and Audit Trail. The main content area is titled 'Domain Details' for 'cloudblue.com' (Status: Verified, Default Auth Mode: Built-In). Below this are tabs for 'DOMAIN SETTINGS', 'SAML SETTINGS', 'EXCLUSIONS LIST', and 'DETAILS'. The 'SAML SETTINGS' tab is active, showing a 'Users Management' section. This section includes a table for mapping user attributes to SAML attributes and a 'Password Management Notice'.

USER ATTRIBUTE	SAML ATTRIBUTE NAME	
<b>External ID</b> Unique identifier of a user in the IDP	uid	
<b>Email</b> Unique immutable email of a user	<input checked="" type="radio"/> No attribute	
<b>Full Name (optional)</b> Non-unique full name of a user	—	

**Password Management Notice**  
Your password is managed externally, please visit <https://example.com> to change your password or contact your support team.





**Edit User Attribute Mapping**

**User Attribute**  
**External ID**  
Unique Identifier of a user in the IDP

**SAML Attribute name**  
uid

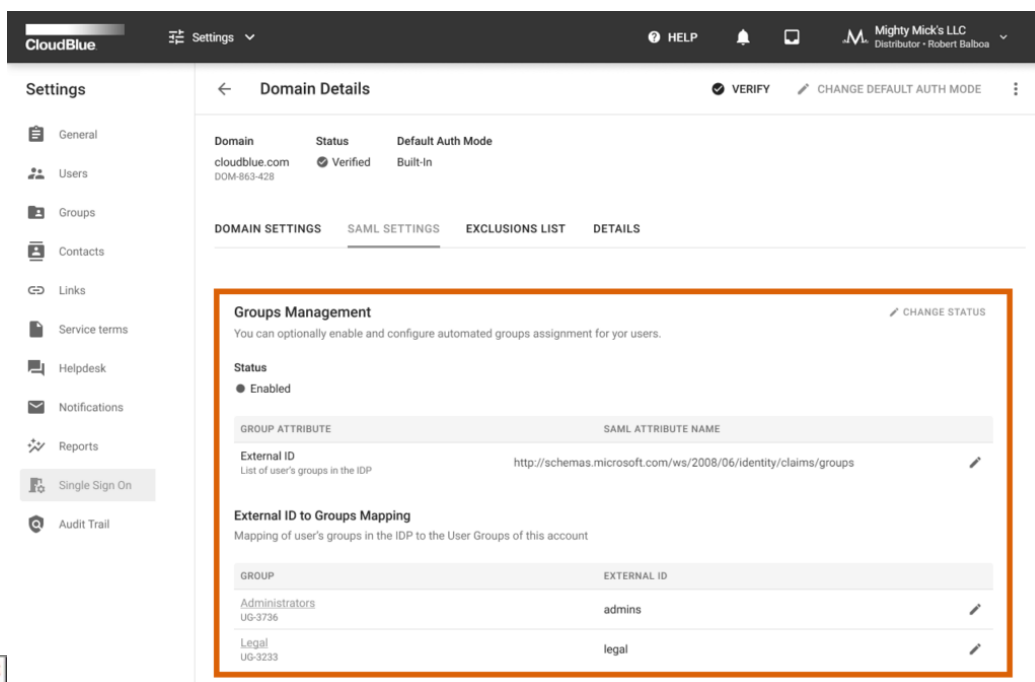
CANCEL SAVE



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.



**Groups Management** CHANGE STATUS

You can optionally enable and configure automated groups assignment for your users.

**Status**  
● Enabled

GROUP ATTRIBUTE	SAML ATTRIBUTE NAME
External ID List of user's groups in the IDP	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

**External ID to Groups Mapping**  
Mapping of user's groups in the IDP to the User Groups of this account

GROUP	EXTERNAL ID
Administrators UG-3736	admins
Legal UG-3233	legal

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.

**CloudBlue** Settings HELP Mighty Mick's LLC  
Distributor - Robert Balboa

**Settings**

- General
- Users
- Groups
- Contacts
- Links
- Service terms
- Helpdesk
- Notifications
- Reports
- Single Sign On**
- Audit Trail

**Domain Details** VERIFY CHANGE DEFAULT AUTH MODE

Domain	Status	Default Auth Mode
cloudblue.com DOM-863-428	Verified	Built-In

**DOMAIN SETTINGS** **SAML SETTINGS** **EXCLUSIONS LIST** **DETAILS**

The following list of users will use the specified authentication mode, regardless of the domain defaults.

REFRESH + ADD

USER	EMAIL	AUTH MODE
Christopher Hicks USR-3473-9325	terra.hamilton@example.com A05F0CC6-9C58-11E8-A8B3-0242AC130003	Built-in
Frank Bowen USR-9127-4885	anthony.hoffman@cloudblue.com A05F0F46-9C58-11E8-A8B3-0242AC130003	SAML

Rows per page: 10 | 1-2 of 2





### Add Domain User Exclusion Policy

**Authentication Mode**

**Built-in**  
User will use built-in authentication method regardless of the domain authentication defaults.

**SAML**  
User will use SAML authentication method regardless of the domain authentication defaults.

Search for user

John Doe USR-3415-1677	John.Doe@cloudblue.com	<input checked="" type="radio"/>
Leslie Ball USR-9917-6140	logan.hopkins@cloudblue.com	<input type="radio"/>
Helen Brown USR-2010-8444	anthony.hoffman@cloudblue.com	<input type="radio"/>
Lucille Leonard USR-8671-8524	levi.wagner@cloudblue.com	<input type="radio"/>
Bobbie Arnold USR-4111-3192	ralph.phillips@cloudblue.com	<input type="radio"/>
Becky Long USR-2729-1705	pamela.foster@cloudblue.com	<input type="radio"/>
Dave Griffith USR-6649-2220	greg.neal@cloudblue.com	<input type="radio"/>
Allan Stewart USR-6652-3556	debbie.baker@cloudblue.com	<input type="radio"/>

CANCEL SAVE

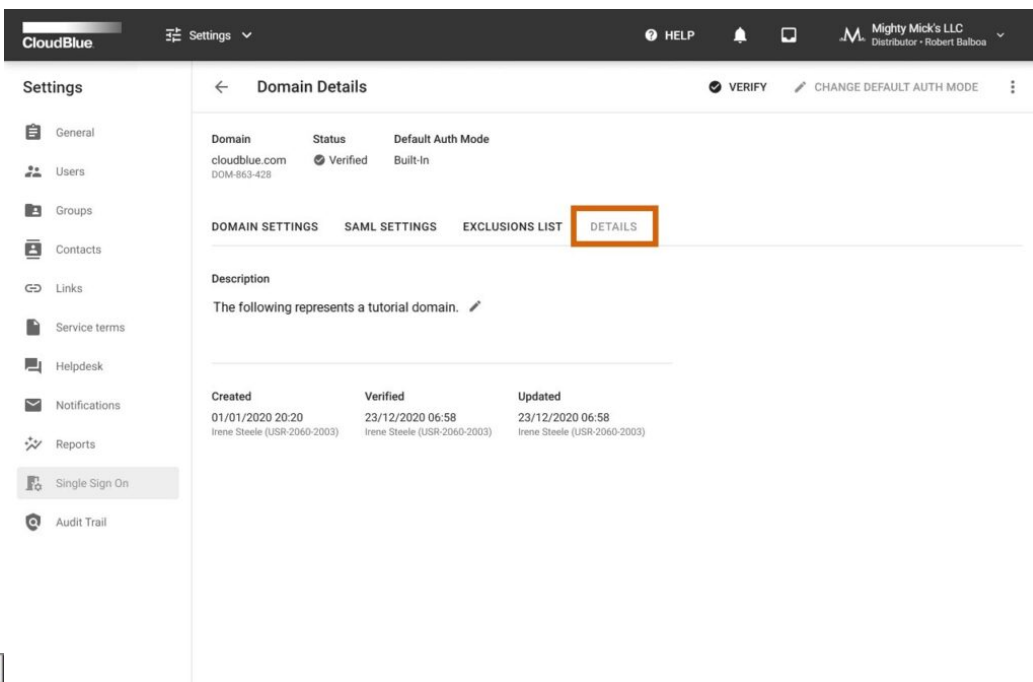


Click the **Add** button to add new users to the Exclusions List. Specify a required authentication mode and select required users from the list. Thereafter, click the Save button to save your adjustments.

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.



The screenshot shows the CloudBlue interface. At the top, there is a navigation bar with the CloudBlue logo, a Settings dropdown, and user information for 'Mighty Mick's LLC'. A left sidebar contains various settings categories, with 'Single Sign On' highlighted. The main content area is titled 'Domain Details' and shows information for the 'cloudblue.com' domain. A table at the bottom tracks the domain's creation, verification, and update history.

Domain	Status	Default Auth Mode
cloudblue.com DOM-863-428	Verified	Built-In

Navigation tabs: DOMAIN SETTINGS | SAML SETTINGS | EXCLUSIONS LIST | **DETAILS**

Description: The following represents a tutorial domain.

Created	Verified	Updated
01/01/2020 20:20 Irene Steele (USR-2060-2003)	23/12/2020 06:58 Irene Steele (USR-2060-2003)	23/12/2020 06:58 Irene Steele (USR-2060-2003)