Uptempo

Single Sign-On with SAML

November 2024/Version 8.0

EN
10. December 2024

Uptempo.io

Copyright

Amalienbadstraße 41a, 76227 Karlsruhe (Germany), www.uptempo.io

Your feedback is important to us!

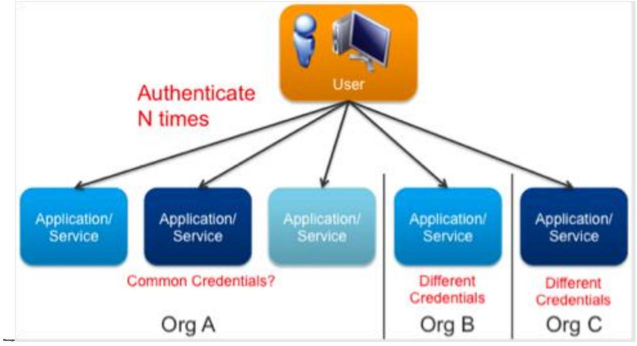
We welcome all comments and would be grateful to be notified of any errors you may discover. Just send us an email to documentation@uptempo.io.

Content

1 Single Sign-On (SSO)

Large organizations and their IT manage dozens or even hundreds of applications across their technology landscape. Each application traditionally requires:

- A separate set of login credentials
- Individual authentication for each access
- Manual login processes for users
- Distinct password policies and requirements



This fragmented approach creates several problems:

- Users must remember multiple passwords
- Time wasted on repeated logins
- Increased security risks from password fatigue
- Higher support costs from password resets
- Reduced productivity from login friction

1.1 The Solution: Single Sign-On with Federation

SSO with federation solves these challenges by:

1. Unifying credentials across applications
2. Authenticating users once per session
3. Securely passing credentials to target applications
4. Managing authorization centrally

How SSO Works

When a user authenticates through SSO:

- They log in once to their primary identity provider
- Their authenticated session is trusted across applications
- Each application receives verified credentials
- Authorization is handled automatically based on user permissions

Benefits

SSO delivers clear advantages:

- One set of credentials for all applications
- Seamless access across authorized systems
- Reduced security risks
- Lower IT support overhead
- Improved user experience
- Enhanced productivity

> Note
>
> The Uptempo application implements SSO through SAML 2.0, ensuring secure and standards-based authentication across your application landscape.

2 Info About SAML

The Uptempo application uses SAML (Security Assertion Markup Language) because it offers significant benefits for enterprise authentication. SAML standards define an XML-based framework for describing and exchanging security information (authentication, authorization, federation) to enable “true” SSO.

> “*Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee; the most recent major update of SAML was published in 2005, but protocol enhancements have steadily been added through additional, optional standards.*
>
> *The single most important requirement that SAML addresses is web browser single sign-on (SSO). Single sign-on is common at the intranet level (using cookies, for example) but extending it beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies.[..]*”
> (Source: Wikipedia, https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language, 18 June 2015)

2.1 Advantages of SAML

Standards and Interoperability

- Open standard protocol for authentication and authorization
- Ensures compatibility across different identity providers
- Allows enterprises to choose and switch vendors freely
- Supports industry-wide integration standards

Enhanced Security

- Implements strong digital signatures for authentication
- Protects data integrity through encryption
- Keeps passwords behind enterprise firewalls
- Reduces attack surface by eliminating multiple credentials
- Prevents credential exposure to external applications
- Provides audit trails for authentication events

Improved User Experience

- Enables single sign-on across multiple applications
- Supports deep linking to specific application pages
- Eliminates password management burden
- Automatically renews sessions when appropriate
- Provides seamless access to authorized resources

Enterprise Benefits

- Reduces IT support costs
- Simplifies compliance and audit processes
- Streamlines user access management
- Enables rapid application integration
- Supports both cloud and on-premises solutions

Implementation Advantages

- Well-documented integration patterns
- Strong vendor and tool support
- Extensive security testing and validation
- Regular protocol improvements and updates
- Large community of implementation experts

Phishing Prevention

If you don’t have a password for an app, you can’t be tricked into entering it on a fake login page.

Web applications with no passwords are virtually impossible to steal, as the user must authenticate against an enterprise-class IdM first that can include strong authentication mechanisms.

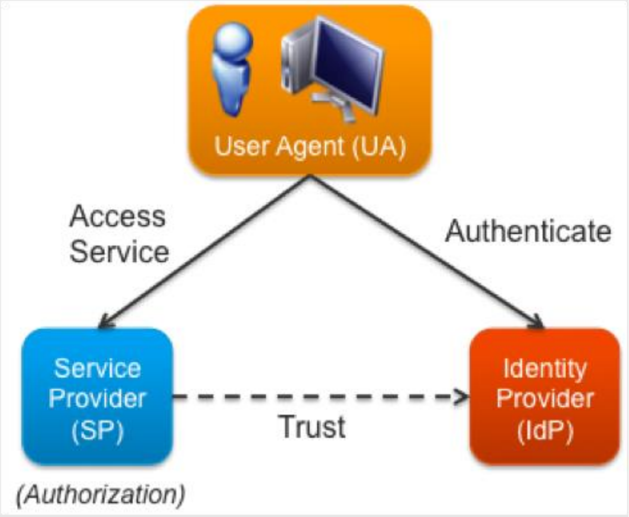
IT Friendly

SAML simplifies life for IT because it centralizes authentication, provides greater visibility and makes directory integration easier.

The Uptempo application leverages these SAML advantages to provide secure, efficient authentication while maintaining flexibility for enterprise customers.

2.2 Roles, Components, and Scenarios

SAML, Security Assertion Markup Language is an OASIS standard for exchanging Authentication and Authorization user data between security domains. The idea being that users authenticate with their identity provider (IdP) in their domain (e.g., Active Directory) once, and SAML 2.0 authenticates their credentials across one or more service providers (SP) (e.g., applications, websites, or services) like the Uptempo application, without having to log in again and again. SAML 2.0 handles the trust between the service providers (SP) and identity providers (IdP) using certificates and passes information about the users from the identity provider to the service providers as part of the SSO process.



Components

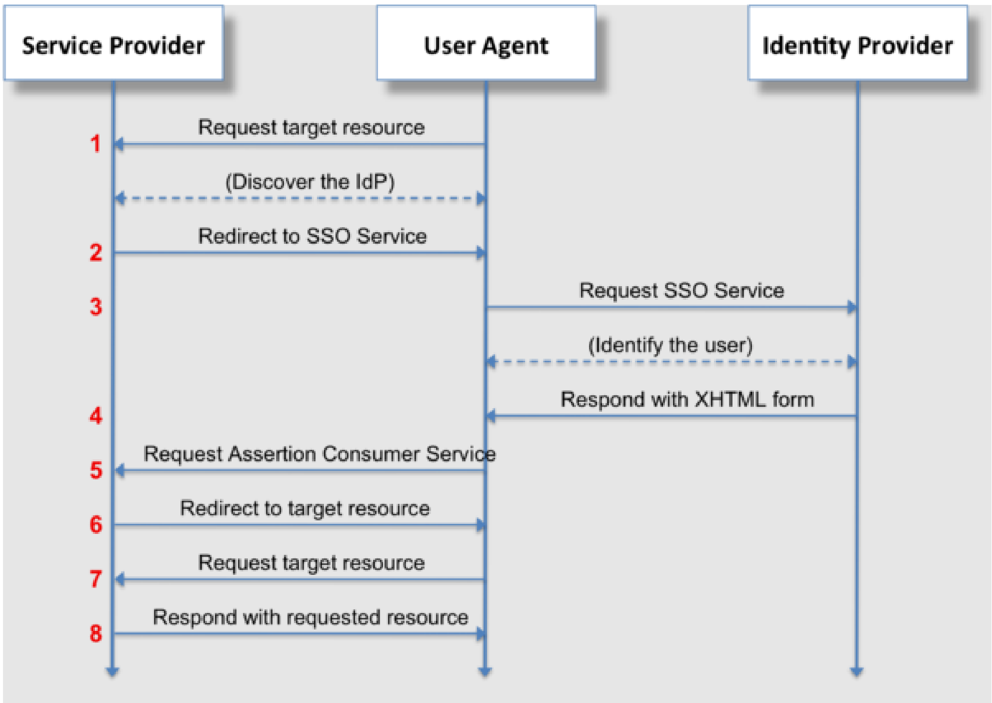
The two main components of a SAML landscape are:

- Service provider *(SP)* – like the Uptempo application**:**
  The service provider is a system entity that provides a set of web applications with a common session management, identity management, and trust management.
- *Identity provider (IdP)* – like Microsoft Active Directory Federation service:
  The identity provider is a system entity that manages identity information for principals and provides authentication services to other trusted service providers.

In other words, the service providers outsource the job of authenticating the user to the identity provider. The identity provider maintains the list of service providers where the user is logged in and can pass requests on logout to those service providers. The client that is trying to access the resource must be HTTP-compliant.

2.3 User SSO Login Flow With SAML

The primary SAML use case is called Web Browser Single Sign-On (SSO). A user wielding a user agent (usually a web browser) requests a web resource protected by a SAML service provider. The service provider (like the Uptempo application), wishing to know the identity of the requesting user, issues an authentication request to a SAML identity provider through the user agent. The resulting protocol flow is depicted in the following diagram. (Source: Wikipedia)



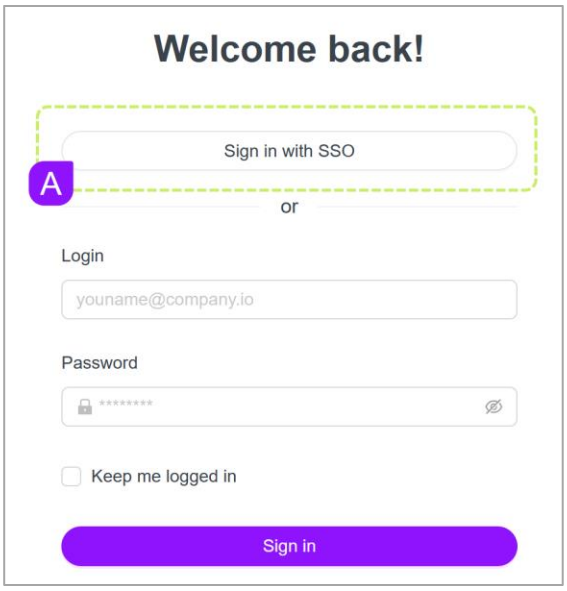
2.3.1 SSO Login Scenarios

The user may experience three different main scenarios:

Case 1: Already Logged in at the SP

If you're already logged into Uptempo in your browser, you'll go directly to your requested page without any additional authentication.

Case 2a: Not Logged into Uptempo but Authenticated With IdP



If you've already authenticated with your Identity Provider (IdP) in another application:

1. Click the *Sign in with SSO* button.
2. The system creates a new SAML assertion.
3. You'll go directly to your requested page.

Case 2b: Not Logged into Uptempo but Remembered and Authenticated With IdP

If you've:

- Already authenticated with your IdP in another application
- Used SSO for your last Uptempo login

The system will:

1. Remember your SSO preference
2. Create a new SAML assertion

3. Log you in automatically
4. Take you to your requested page

Case 3: Not Authenticated with IdP

When you arrive at your IdP's login page:

- If the IdP recognizes you as a known user, it may authenticate you automatically
- After successful authentication, you'll go directly to your requested page in Uptempo

3 Prerequisites & Constraints

3.1 Platform Requirements

- Uptempo: 8.0 or higher
- SSL certificate (HTTPS) enabled
- Valid system administrator account with permission *Manage SAML configuration* added to your role

> Note
>
> In Uptempo 8.0, the SAML endpoint URL pattern has changed from `/secure/saml.do` to `/auth/v1/saml`. This is an important technical detail for proper configuration.

3.2 Network Requirements

- Stable internet connection
- Firewall configuration allowing HTTPS traffic (port 443)
- No proxy restrictions for SAML endpoints
- DNS resolution for both IdP and SP domains

3.3 Prerequisites

- Identity provider with SAML 2.0 support (recommended) or SAML 1.x
- SSL Certificate Requirements Before implementing SAML SSO with Uptempo, ensure your environment meets these SSL certificate requirements:
  - Valid SSL/TLS certificate from a trusted Certificate Authority (CA)
  - Certificate must match your Uptempo instance domain name
  - Minimum 2048-bit key length
  - SHA-256 or stronger signing algorithm
  - Valid certificate chain without any missing intermediate certificates
  - Certificate expiration date at least 6 months in the future
  - Private key in proper format and securely stored
- DNS Configuration Requirements Proper DNS configuration is essential for SAML SSO to function correctly:
  - Public DNS record (A record) pointing to your Uptempo instance
  - Fully Qualified Domain Name (FQDN) matching your SSL certificate

  - DNS propagation completed across all relevant networks
  - No DNS-level redirects that could interfere with SAML assertions
  - Proper PTR records if reverse DNS lookup is needed
  - DNS resolution working consistently across all user networks
  - If using split DNS, ensure both internal and external resolution work correctly
  - Verification Steps Before proceeding with SAML configuration:
  - Verify SSL certificate installation using browser tools
  - Test HTTPS connectivity from all user networks
  - Confirm certificate chain validation
  - Check DNS resolution from various network locations
  - Validate HTTPS without certificate warnings
  - Document all DNS records and certificate details for reference

> Note
>
> These requirements ensure secure and reliable SAML authentication. Missing or incorrect SSL/DNS configuration can lead to authentication failures or security vulnerabilities.

3.4 Constraints

- The Uptempo application cannot be used as an identity provider.
- The Uptempo application Web Services (API) does not support SAML.
- The Uptempo application does not support WS-Trust Security Token Service.
- The Uptempo application supports SP-initiated and IdP-initiated scenarios.
- The Uptempo application introduces basic support for multiple IdPs from the beginning.
- Besides others, the SAML implementation does not support Home Realm Discovery (HRD) and Single Logout now.

3.4.1 Supported Identity Providers

As SAML is an open-standard data format, every SAML identity provider should work. Most Uptempo systems use Okta or Microsoft Azure Entra ID as IdP.

3.5 Identity Provider Landscape

If your organization plans to implement SSO with SAML 2.0, we can recommend looking at well-established identity providers that are known to support SAML 2.0 such as:

1. Azure Active Directory (Entra)
2. Okta
3. OneLogin
4. PingIdentity
5. Auth0

> Note
>
> SAML 1.x does not support all features and security mechanisms of SAML 2.0. We recommend SAML 2.0 therefore.

If you are considering the implementation of SAML 2.0, it is essential to identify a suitable provider that can meet the requirements:

- Support for SAML 2.0 protocol specifications
- Ability to generate and manage X.509 certificates
- Support for different bindings (HTTP POST and Redirect)
- Ability to configure custom attribute mappings
- Support for various NameID formats

Before choosing any SSO provider, we recommend:

- Verify their security certifications and compliance standards
- Check their uptime guarantees and support offerings
- Review their documentation and integration guides
- Test their service with a trial or proof of concept

Use the following table with links to detailed information about the most common identity provider solutions supporting SAML 2.0.

Solution	More information
Microsoft Azure Active Directory	Set up a SAML 2.0 provider with Microsoft Entra ID
Okta	Add a SAML 2.0 IdP
OneLogin	How Does Single Sign-On Work?
Ping Identity	Ping Federate
Salesforce.com	Enable Salesforce as an identity provider: Salesforce as identity provider
Auth0	Learn more.
Broadcom	Siteminder

4 Pre-Implementation Checklist

Before starting the SSO implementation, ensure:

1. Identity Provider Setup
   - SAML-compliant IdP is installed and configured
   - Admin access to IdP configuration
   - Ability to generate/export IdP metadata
   - Certificate management capabilities
2. Uptempo application Setup
   - Administrator access to Uptempo application
   - HTTPS enabled and valid certificate
   - Required ports open in firewall
   - Backup authentication method available
3. User Management
   - User attribute mapping strategy defined
   - Test users available in IdP
   - User migration plan (if applicable)

5 Setup the Uptempo Application as SAML Service Provider

To get single sign-on up and running using SAML, three steps have to be executed:

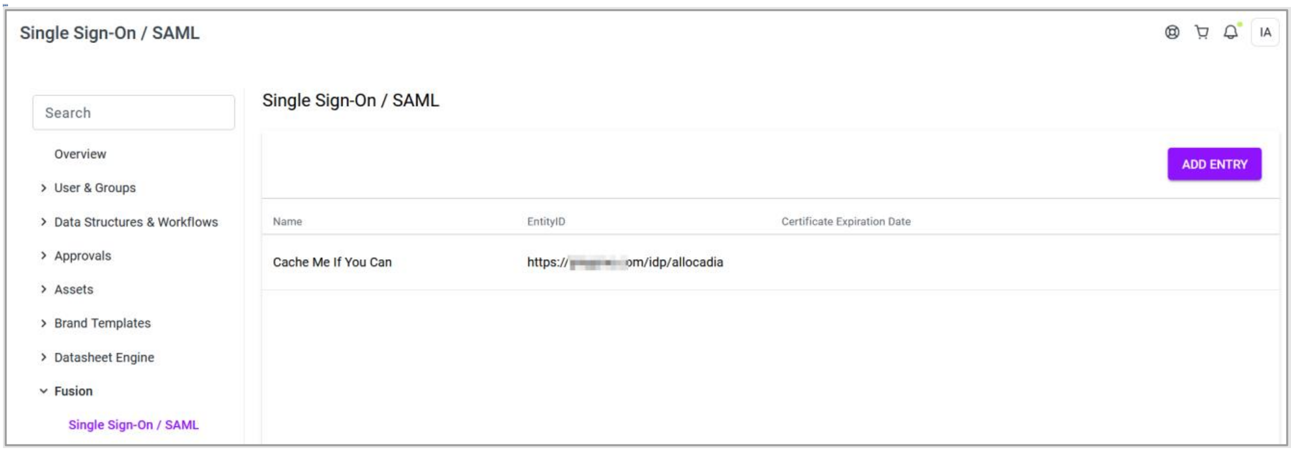
- Set up your identity provider as the authentication service for the Uptempo application. Refer to chapter 3.5 *Identity Provider Landscape*, chapter 7 Example: “Configuring Microsoft Entra ID for SAML Authentication”, and chapter 8 Example: “Configuring Okta for SAML Authentication” for instructions.
- Configure identity attribute mappings between your IdP and the Uptempo application, see chapter 5.2.
- Configure the Uptempo application as service provider, see this chapter.

5.1 Configure the Uptempo Application

To configure the Uptempo application as service provider, log in with administrator permissions.

5.1.1 Configuration of the Identity Providers

1. Go to > *Administration* > *Overview* > *Fusion* > *Single Sign-On / SAML*.



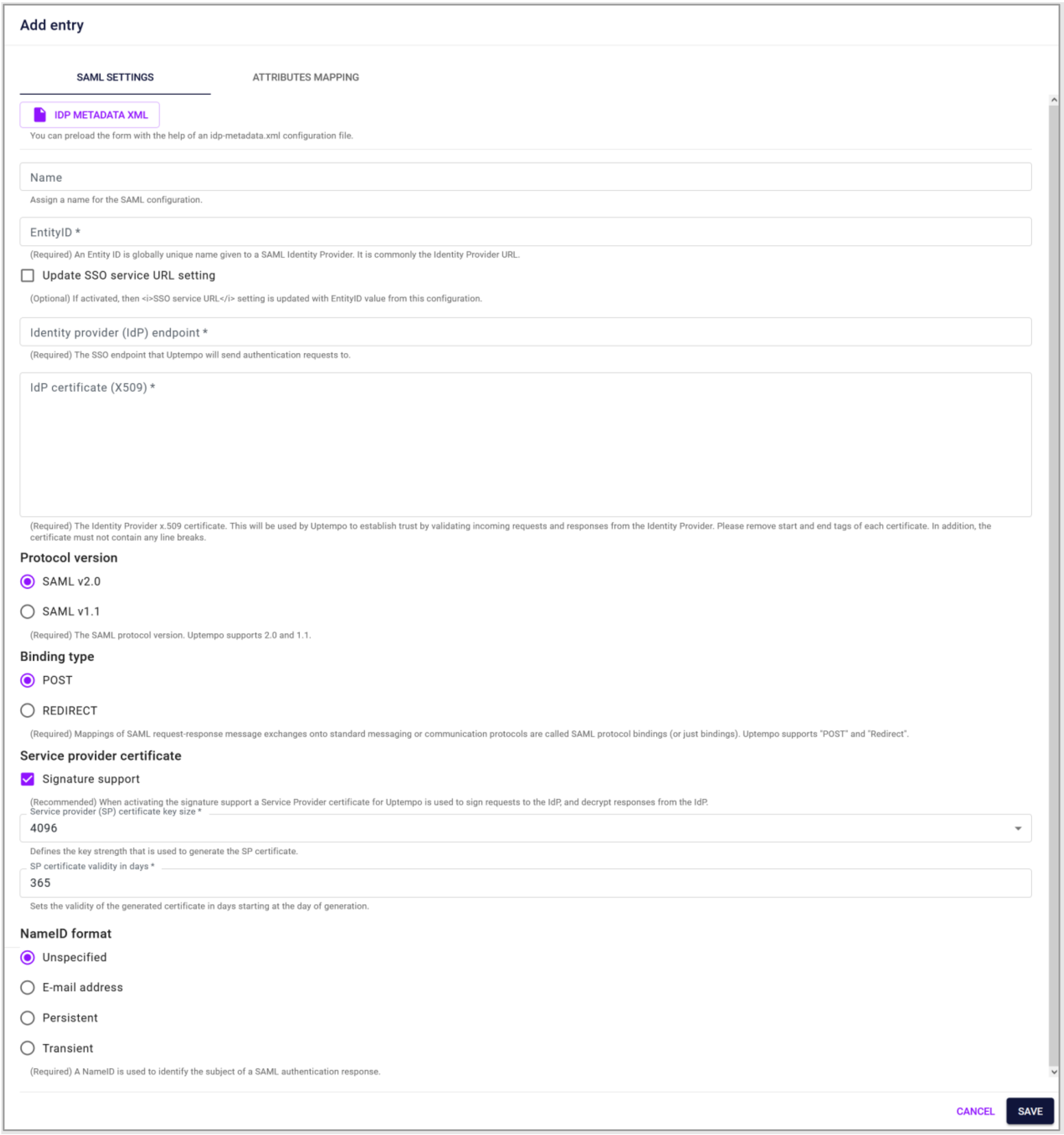
Single Sign-On / SAML

Name	EntityID	Certificate Expiration Date
Cache Me If You Can	https://[redacted]om/idp/allocadia	

In the case that there is an existing configuration, you see a grid as shown above.

2. Click the *Add Entry* button to create a new configuration for an additional identity provider.

> Note
> Each field has helpful explanatory text that provides context about its purpose and requirements, making it easier for administrators to understand and correctly configure the SAML integration.



Add entry

You can preload the form with the help of an idp-metadata.xml configuration file.

Name

Assign a name for the SAML configuration.

EntityID *

(Required) An Entity ID is globally unique name given to a SAML Identity Provider. It is commonly the Identity Provider URL.

□ Update SSO service URL setting

(Optional) If activated, then <i>SSO service URL</i> setting is updated with EntityID value from this configuration.

Identity provider (IdP) endpoint *

(Required) The SSO endpoint that Uptempo will send authentication requests to.

IdP certificate (X509) *

(Required) The Identity Provider x.509 certificate. This will be used by Uptempo to establish trust by validating incoming requests and responses from the Identity Provider. Please remove start and end tags of each certificate. In addition, the certificate must not contain any line breaks.

Protocol version

● SAML v2.0

○ SAML v1.1

(Required) The SAML protocol version. Uptempo supports 2.0 and 1.1.

Binding type

● POST

○ REDIRECT

(Required) Mappings of SAML request-response message exchanges onto standard messaging or communication protocols are called SAML protocol bindings (or just bindings). Uptempo supports "POST" and "Redirect".

Service provider certificate

☑ Signature support

(Recommended) When activating the signature support a Service Provider certificate for Uptempo is used to sign requests to the IdP, and decrypt responses from the IdP.

Service provider (SP) certificate key size *
4096

Defines the key strength that is used to generate the SP certificate.

SP certificate validity in days *
365

Sets the validity of the generated certificate in days starting at the day of generation.

NameID format

● Unspecified

○ E-mail address

○ Persistent

○ Transient

(Required) A NameID is used to identify the subject of a SAML authentication response.

3. Select the metadata file you exported to automate the partner setup, or fill in the fields. Select the appropriate options.

   Please note that the automated population of the form field requires a metadata XML file and not a PEM or CRT file.

   Note: The needed settings depend on the setup of your identity provider.

4. The configuration can get an optional name to identify it easily in the overview of the single sign-on configurations. For example, the name could be *Test connection* if you want to differentiate between test and live configurations.

5. With checking the box *Update SSO service URL setting* the respective setting *Administration: SSO service URL* which is part of the settings table does not need to be changed manually (see chapter 5.1.2.2 *Enable SSO Login Button on Login Page*). Please note that the setting is overwritten every time the box is checked, and the form is saved.
6. After you selected and configured the required settings, press the *Save* button.

Now, the Uptempo application is configured as a service provider for SSO using SAML.

> Note
>
> In case of changes of the IdP configuration, you will have to update your Uptempo application SAML configuration as well.

5.1.1.1 Data for Identity Provider Configuration

Two links appear on the configuration page:

- *Download metadata of Service Provider*
  Download link for the entire configuration data in xml format incl. the SP certificate. The metadata is automatically updated on saved changes.
- *Download certificate of Service Provider*
  Download link for the SP certificate in PEM format.
  Required just for some IdP vendors.

The next step is to set up your service provider with the necessary fundamental objects followed by configuring the identity provider system to cooperate with (and trust) the Uptempo application and to configure the user attribute mappings.

5.1.2 System Configuration and Tweaks for User Guidance

5.1.2.1 Automatic Redirection of all Users to the IdP

If you want to support single sign-on as the only way to access the system, you can automatically redirect each user from the login page to the identity provider. You can activate this with the setting *Administration: SSO service.*

> Note
>
> There’s no way to manually log into the system now – not even for the Uptempo support team. In the case you need help, you must (temporarily) disable this behavior again.

5.1.2.2 Enable SSO Login Button on Login Page

Two additional settings need to be done, to display the *SSO Login* button on the login page to allow SP initiated SAML assertions to one IdP:

1. Click > *Administration* > *Overview* > *System Configuration* > *System Settings*.
2. Edit the following settings:
    - *Administration: SSO button SSO*: Set it to *activated*.
      Turn the login form on the login page on or off. The login form consists of the fields *User name* and *Password*, as well as the button Login.
    - *Administration: SSO service URL*: Enter the URL of the authentication service. Set the URL to:
      https://yourcompany.uptempo.io/auth/v1/saml?issuer=[configuration name / entityId]

   Note: The setting *Administration: SSO service URL* can be set automatically with saving the SAML configuration (see chapter 5.1.1 Configuration of the Identity Providers, step 5).

The *SSO Login* button is enabled for the chosen IdP.

5.1.3 Configuration of Necessary Permissions, Roles, and Groups

The access control to assets, Web-to-Publish documents and other related parts of the Uptempo application is done via different mechanisms. Therefore, the user needs to have defined (module) roles and be part of specific groups. Among others, they are shown in Figure 1: Uptempo application access controls.

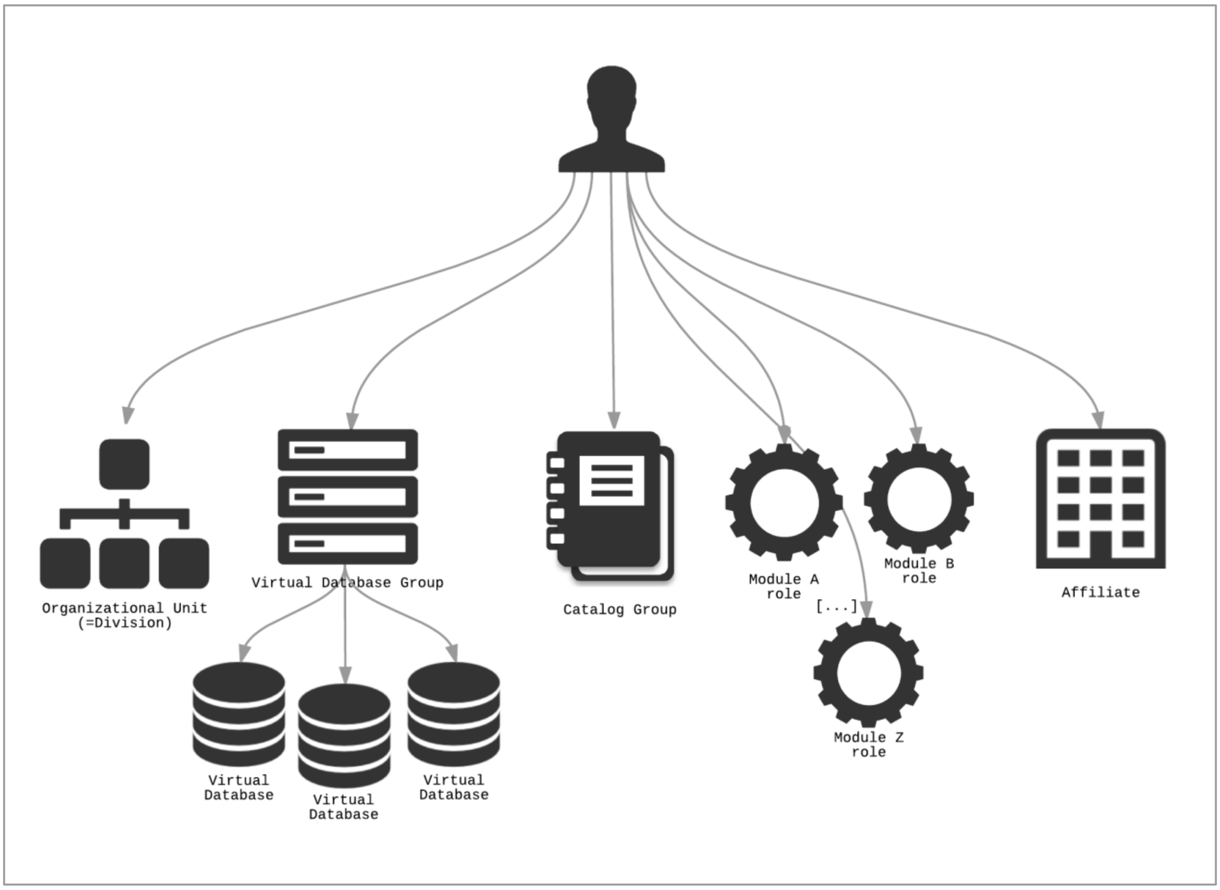


Figure 1: Uptempo application access controls

Most of these relations are indirectly established via Single Sign-On (SSO) Groups and controlled by the optional *SAML_SSO_GROUP* parameter, but some can be set directly with specific parameters. For the complete list of supported parameters, refer to section 5.2 Supported Attributes.

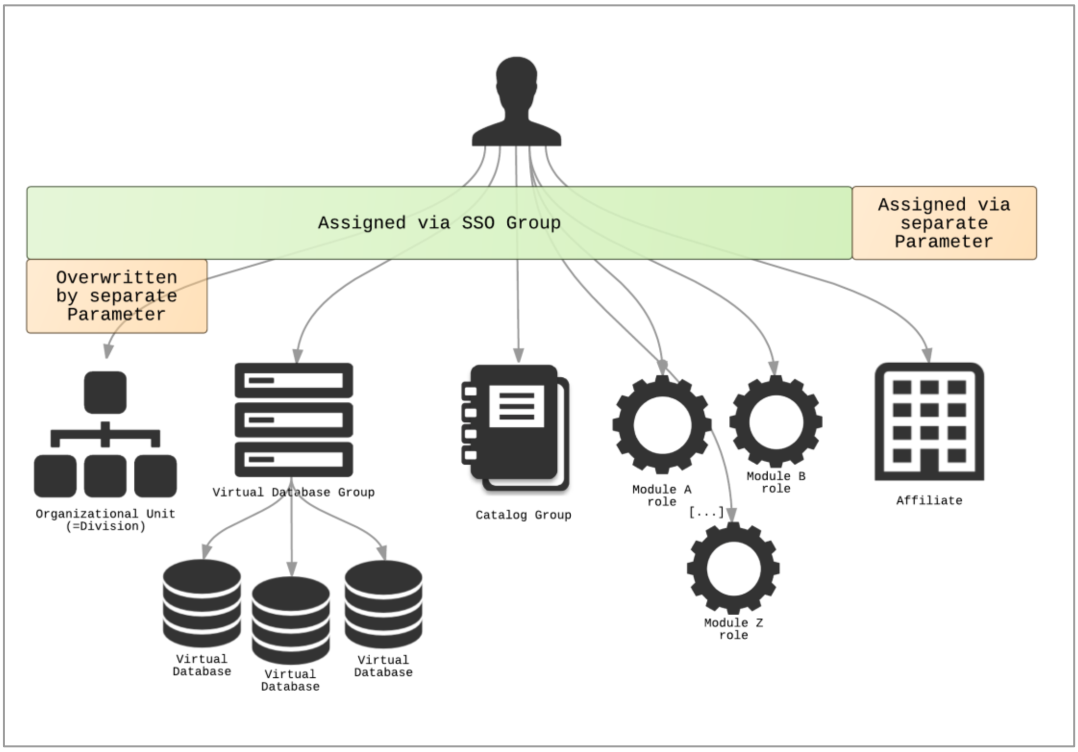


Figure 2: Single Sign-On parameters controlling the Uptempo application access controls

Note: For detailed instructions about how to maintain SSO groups, refer to the general *Administration Manual*.

Users who have no valid group name information are either rejected or logged in using a configurable default SSO group. That behavior can be adjusted by the system setting *Administration: SSO group match.*

To be correct here users are actually not “assigned” to SSO groups inside the Uptempo application. These groups act more like some kind of template for the other linked objects, like roles, virtual database groups, organizational units or catalog groups. Whenever you change an SSO group, it does not directly affect any existing user.

Next to this, there are two crucial parameters that control the persistence of users in the Uptempo application — *SAML_CREATE_USER* and *SAML_UPDATE_USER*.

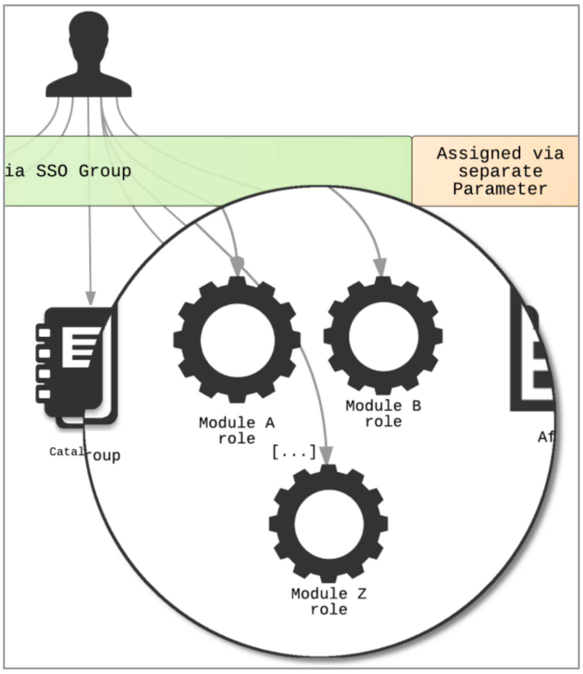
If the parameter *SAML_CREATE_USER* is set to true, it is checked if the user account already exists, means if a login name matches the value of *SAML_USERNAME*. If the user account does not exist, the system checks if all mandatory information has been provided. If so, the account is created automatically. If the account already exists, all given parameters are updated.
SAML_UPDATE_USER on the other hand just updates an existing user account and the process fails in the case of a missing *SAML_CREATE_USER* for non-existent user

accounts; so *SAML_CREATE_USER* includes *SAML_UPDATE_USER.* This can be useful if you want to avoid the generation of new user accounts via SAML.

> Note: For detailed instructions about how to maintain SSO, refer to the general *Administration Manual*.

5.1.3.1 Roles

Module roles are indirectly assigned to the user via SSO groups. You cannot set them directly via SAML.



> Note: For detailed instructions about how to maintain module roles, refer to the general *Administration Manual*.

Please note that for the Uptempo application, one user can only have one role assignment per module. If multiple groups are defined for one user, they are processed sequentially, beginning with the first, then the second etc. in their sequence of the *SAML_SSO_GROUP* parameter. For each group, the defined roles are assigned to the user. If another role was assigned for the same module previously, the assignment is overwritten by the most recent assignment in the parameter sequence.
A complete example of how this process looks like can be found in Figure 3: Complete processing example for multiple SSO groups.

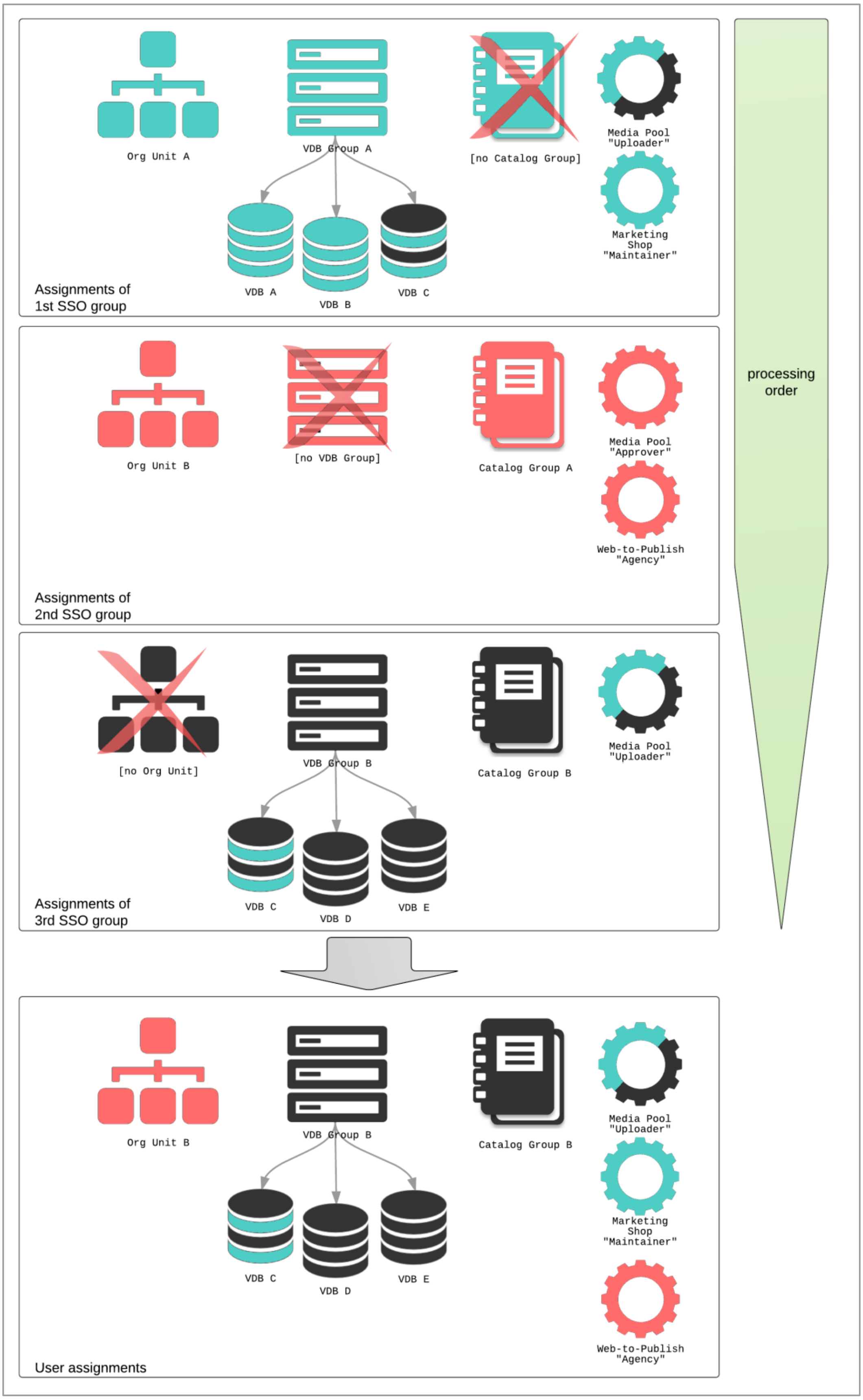
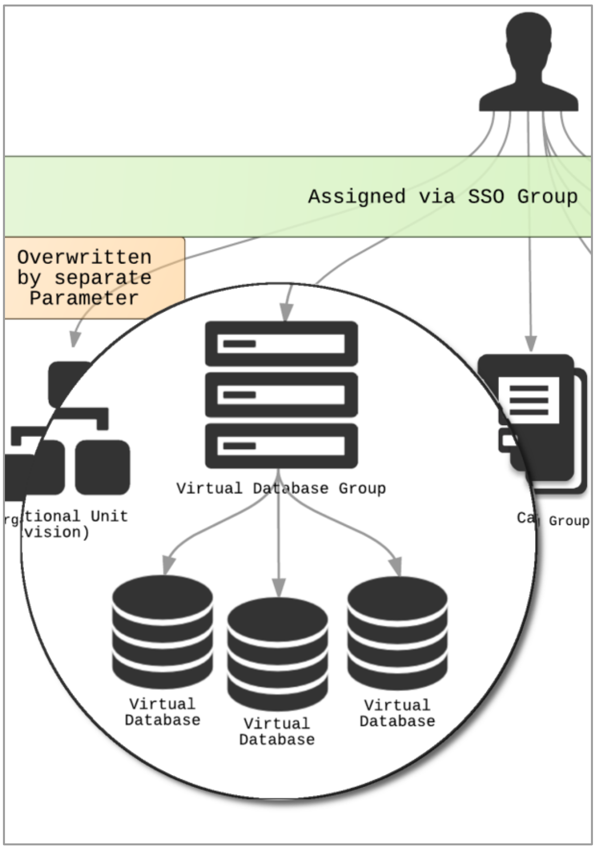


Figure 3: Complete processing example for multiple SSO groups

5.1.3.2 *Virtual Databases*

Virtual Databases are assigned with the help of Virtual Database groups.



Note: For detailed instructions about how to maintain module roles, refer to the general *Administration Manual*.

Please note that for the Uptempo application, one user can only have one VDB group. VDB groups are assigned indirectly via *SAML_SSO_GROUP* parameter and the processing is equal to the one for the module roles. For each group, the defined VDB group is assigned to the user. If another VDB group was assigned previously, the assignment is overwritten by the most recent assignment in the parameter sequence. Please check Figure 3: Complete processing example for multiple SSO groups again.

With the setting *Administration: VDB group auto-generation*, new VDB groups are automatically generated based on given VDBs (via *SAML_SSO_GROUP* → VDB groups) as shown in the following figure.

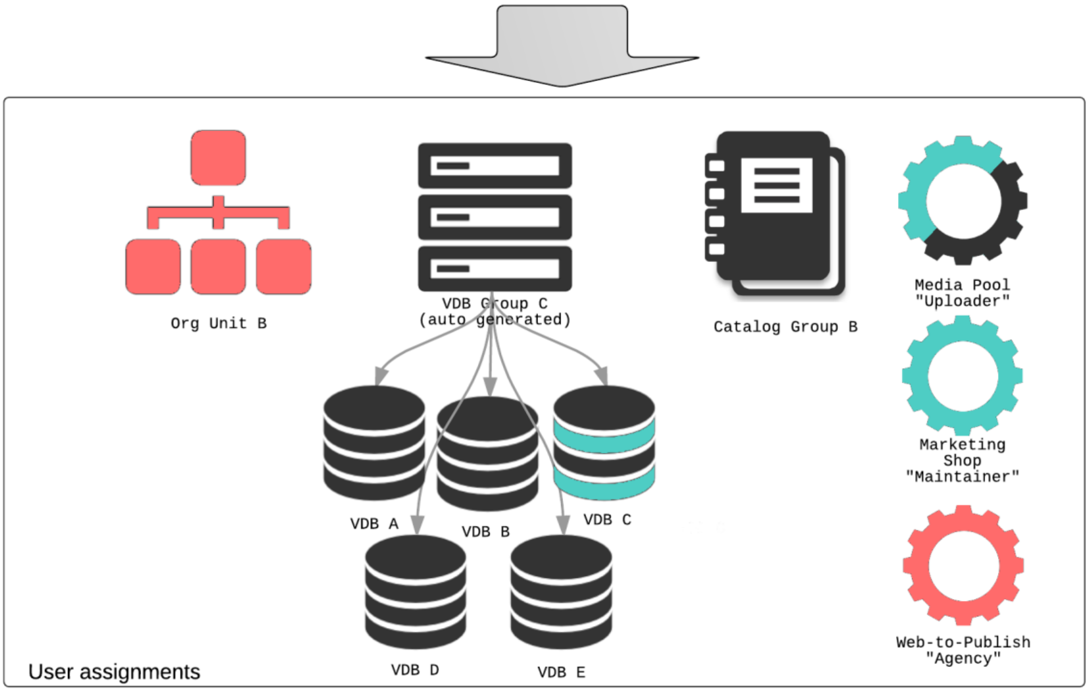
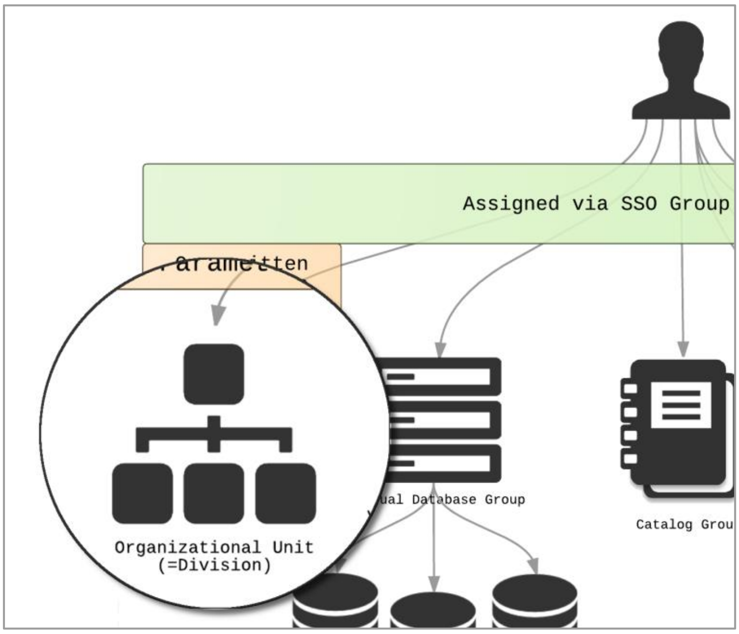


Figure 4: Auto-generated VDB group

But before the generation, the system checks whether a VDB group exists holding exactly the wanted set of all the VDBs. In this case, it is assigned to the user.

5.1.3.3 Organizational Unit



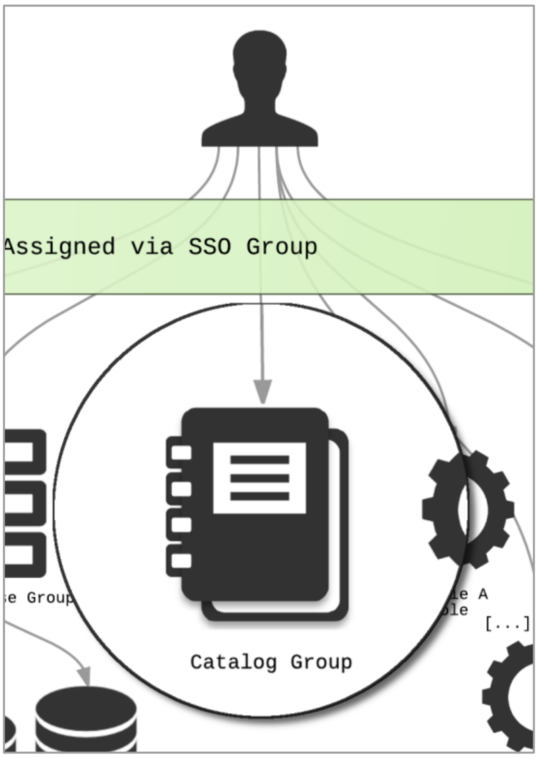
Every user has to have exactly one organizational unit. It can either be assigned with the help of the given SSO groups or directly in the *SAML_OVERRIDE_ORGUNIT* parameter, whereby the separate parameter outweighs the mapping in the SSO group.

As for the VDB group, the assignment is overwritten by the most recent assignment in the parameter sequence. Please check Figure 3: Complete processing example for multiple SSO groups for reference again.

If an organizational unit name is given that does not exist yet, then the organizational unit is created automatically. The attribute *SSO-Key* of the organizational unit is relevant for the identification.

5.1.3.4 Catalog Groups

Catalog groups are used only by the Uptempo Marketing Shop module to restrict access to specific articles and catalogs.

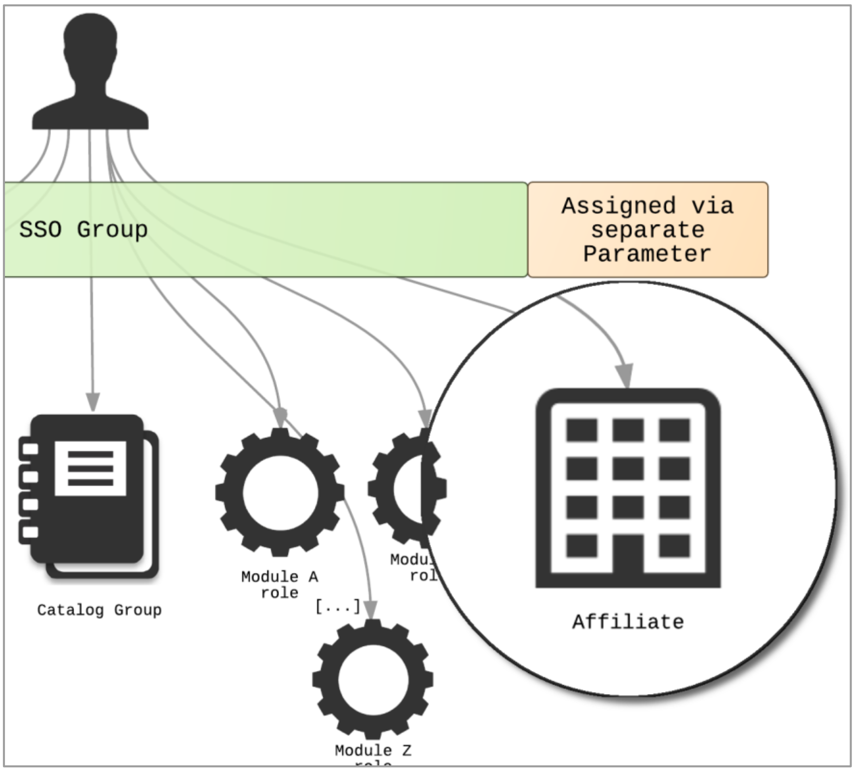


Note: For detailed instructions about how to maintain Catalog Groups, refer to chapter 9.1 of the general *Marketing Shop Administration Manual*.

5.1.3.5 Affiliates

You can only assign affiliates directly via *SAML_AFFILIATEID* parameter. It can be a single value or multiple values separated by commas.

If the user already has a (selected) affiliate set, which is not in that given list, the assignment will be dropped. If the list contains only one affiliate ID, this ID is chosen for both attributes, *selected* and *alternative*.



During the processing, each value from the list is evaluated against the regular expression defined in *Administration: Affiliate ID validation* and dropped in the case of a mismatch.

5.2 Supported Attributes

The Uptempo application supports a comprehensive set of SAML attributes that enable secure user authentication and authorization. This section outlines these attributes and explains how they work together to manage user access.

Mandatory Attributes and Identity Management

The Uptempo SAML endpoint requires specific custom attributes in the SAML assertion from your Identity Provider (IdP) to properly identify and authenticate users. These mandatory attributes (marked in the attribute reference table, section 0) form the foundation of user identification and must be correctly configured for successful authentication.

Role and Permission Management

User permissions and roles in Uptempo are derived from SSO groups. This makes the careful configuration of groups and organizational units essential for proper access control. When setting up these structures, consider your organization's hierarchy and access requirements to create a manageable and secure permission framework.

Attribute Name Matching

For successful SAML integration, attribute names must match exactly between your IdP and Uptempo. This matching is case-sensitive, as are the attribute values—particularly for Boolean values (true/false). For example, if Uptempo expects *SAML_USERNAME*, sending *saml_username* will not work.

Flexible Attribute Mapping

If your IdP cannot use Uptempo's default attribute names, or if you need to map existing attributes differently, Uptempo provides a custom attribute mapping feature. This allows you to maintain your existing IdP attribute names while mapping them to their corresponding Uptempo attributes. See section 6.1.2 for detailed instructions.

Implementation Guidelines

- Work with your IT team: SAML configuration requires expertise in both your IdP system and Uptempo. While Uptempo's support team can guide you through the platform-specific settings, your IT administrators should lead the IdP configuration.

- Plan your structure: Before implementation, map out your desired group structure and permission hierarchy.

- Test thoroughly: Use a staging environment to verify attribute mappings and group assignments before deploying to production.
- Monitor and maintain: Regularly review your SAML configuration to ensure it aligns with your organization's evolving needs.

This foundation ensures secure authentication while maintaining the flexibility to adapt to your organization's specific requirements. The following sections detail the supported attributes and their specific configurations.

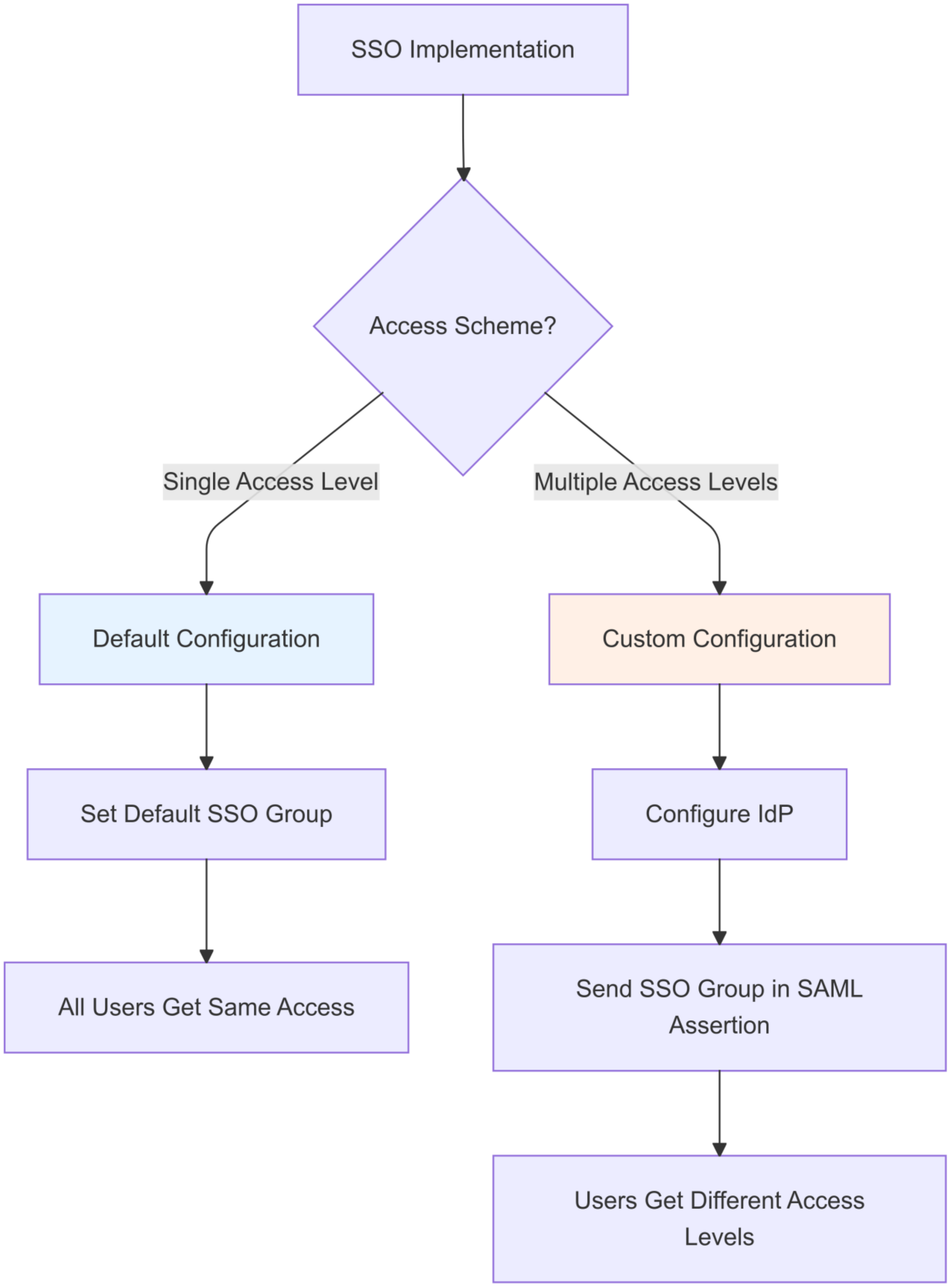
Please keep in mind that all attribute names are case-sensitive. This also applies to most attribute values, especially Boolean values.

Note

All new users created in your IdP will be created in Uptempo as well. If customers want to override this behavior, they must set the *SAML_CREATE_USER* attribute to false. Create and update user are already operational. However, the delete and substitute functions have not yet been implemented. Currently, the minimum requirement is to configure *SAML_USERNA*ME as an attribute.

For a case where all users have the same access:

- The *SAML_SSO_GROUP* attribute can be omitted from the configuration
- The SP should be configured to grant a default access level when no group attribute is present
- This makes it easier to get started while maintaining security


SSO Implementation
Access Scheme?
Single Access Level
Multiple Access Levels
Default Configuration
Custom Configuration
Set Default SSO Group
Configure IdP
All Users Get Same Access
Send SSO Group in SAML Assertion
Users Get Different Access Levels

6 SAML Attribute Reference

Group	Attribute Name	Re-quired	Type	Description
Core Identity and Account Control	*SAML_USERNAME*	Yes	Literal	Primary login identifier. Must be the email. This serves as the user's digital identity within Uptempo, akin to a unique employee ID, which must never be duplicated across your system.
	SAML_EMAIL	Yes	Literal	Primary email address. This essential attribute handles system notifications and can also serve as a login credential. The system's email handling behavior is customizable via Administration settings. Must be mapped into *SAML_USERNAME*
	SAML_CREATE_USER	No	Boolean	Controls user provisioning. With *Default* set to *true*, this attribute acts like an automated onboarding system, creating new user accounts when they don't exist and updating existing ones.
	SAML_UPDATE_USER	No	Boolean	With *Default* set to *true*, this attribute functions as a profile maintenance switch. It works only for existing users unless *SAML_CREATE_USER* is enabled, making it ideal for keeping user information current.
User Profile Information	*SAML_FIRST_NAME*	Yes	Literal	Forms the first part of a user's display name within the system. Combines with *SAML_LAST_NAME* for full identification.

Group	Attribute Name	Re-quired	Type	Description
	SAML_LAST_NAME	Yes	Literal	Completes the user's display name, working with *SAML_FIRST_NAME* for proper identification.
	SAML_FUNCTION	No	Literal	Describes the user's position or role, useful for organizational reporting and workflow assignments.
	SAML_TITLE	No	Literal	Captures professional designations like Dr. or Prof., enhancing formal communications.
	SAML_GENDER	No	Literal	Accepts either m/f or Male/Female, used for personalization and reporting.
Access Control and Groups	*SAML_SSO_GROUP*	No	Literal	Determines a user's base permissions through group assignments. Like building security clearances, multiple groups are processed in order, with later assignments taking precedence.
	SAML_OVERRIDE_ORGUNIT	No	Literal	Places users within your organizational hierarchy. If an organizational unit doesn't exist, it will be created automatically using the SSO-Key for identification.
	SAML_AFFILIATEID	No	Literal	Associates users with specific business divisions. Supports multiple assignments using commas, with values validated against your Affiliate ID pattern.
	SAML_OVERRIDE_SMARTACCESS_ROLE	No	Literal	Determines a user's ability to manage access controls and permissions within the system.
	SAML_OVERRIDE_SHOP_ROLE	No	Literal	Controls user permissions within the Marketing Shop module, managing e-commerce capabilities.

Group	Attribute Name	Re-quired	Type	Description
	SAML_OVERRIDE_PIM_ROLE	No	Literal	Defines user permissions for Product Information Management, controlling product data handling capabilities.
	SAML_OVERRIDE_PORTAL_ROLE	No	Literal	Sets permissions for brand portal management, controlling user access to portal features.
	SAML_OVERRIDE_EVENTMGR_ROLE	No	Literal	Manages permissions for event planning and coordination features.
	SAML_OVERRIDE_REVIEWMGR_ROLE	No	Literal	Controls access to review and approval workflow features.
	SAML_OVERRIDE_DMC_ROLE	No	Literal	Determines user permissions within the Digital Media Center.
Contact Information	*SAML_COMPANY*	No	Literal	Identifies the user's company, crucial for multi-organization environments.
	SAML_STREET	No	Literal	Part of the complete address profile. Applied to postal, delivery, and invoice addresses simultaneously.
	SAML_STREET_NUMBER	No	Literal	Use underscores (_) for spaces in building numbers; other special characters may be removed.
	SAML_ZIP	No	Literal	Supports alphanumeric formats for international compatibility.
	SAML_CITY	No	Literal	Used for geographical grouping and address completion.
	SAML_COUNTRY	No	Literal	Influences regional settings and reporting categorization.
	SAML_WORK_PHONE	No	Literal	Primary professional contact number for the user.
	SAML_MOBILE_PHONE	No	Literal	Alternative contact method for more immediate communication needs.

Group	Attribute Name	Required	Type	Description
System Preferences	*SAML_USER_LANGUAGE*	No	Literal	A two-letter language code (e.g., EN, DE) that determines the user's interface language.
	SAML_USER_TIME_ZONE	No	Literal	Example format: "America/New_York". Affects all time-based features and displays.
	SAML_STARTURL	No	Literal	Takes highest priority for user navigation, overriding any deep links. Format: startURL=/path/to/page
	SAML_PREFERRED_UNIT_OF_LENGTH	No	Literal	Accepts mm, cm, or inch, affecting all measurement displays throughout the system.
Custom and Generic Attributes	*SAML_ADD_GENERIC_ATTRIBUTES*	No	Literal	JSON format for adding custom attributes without overwriting existing ones.
	SAML_GENERIC_ATTRIBUTES	No	Literal	JSON format that completely replaces all existing custom attributes.

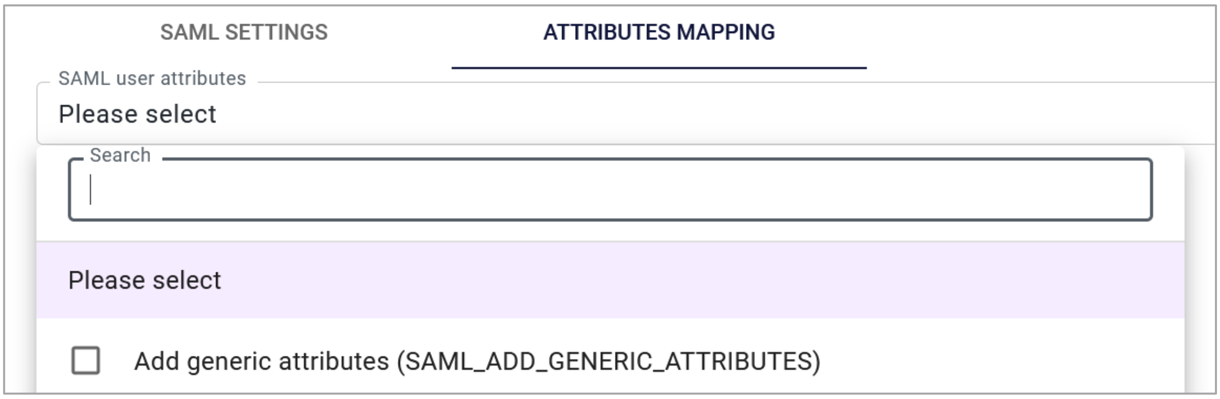
6.1.1 Additional Data via SAML

SAML can transmit various additional user data to your Uptempo system. To handle this efficiently, administrators must use our mapping tool to correctly align incoming SAML data with internal user attributes and settings.

6.1.2 Mapping of Custom Attribute Names

If it is not feasible to alter the attribute names on the IdP side, it is possible to map the names of the Uptempo application with those of the IdP. Consequently, a separate tab is available in the configuration of a Single Sign-On setup.

1. To begin, navigate to > *Administration* > Overview > *Fusion* > *Single Sign-On / SAML*. From there, search and select the configuration you wish to modify.



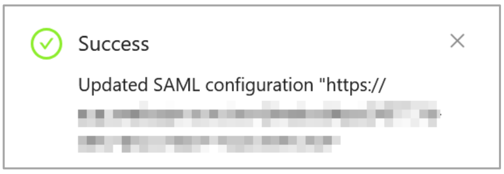
2. Navigate to the *Attributes Mapping* tab at the top of the configuration screen.

3. If no mappings have been defined, use the search filter for available Uptempo application attributes.

   The search field allows for the convenient retrieval of attributes.

   Once you have selected one or more attributes, they will be displayed under the *Attributes Mapping* tab. For each attribute, you can enter the name on the side of the IdP.

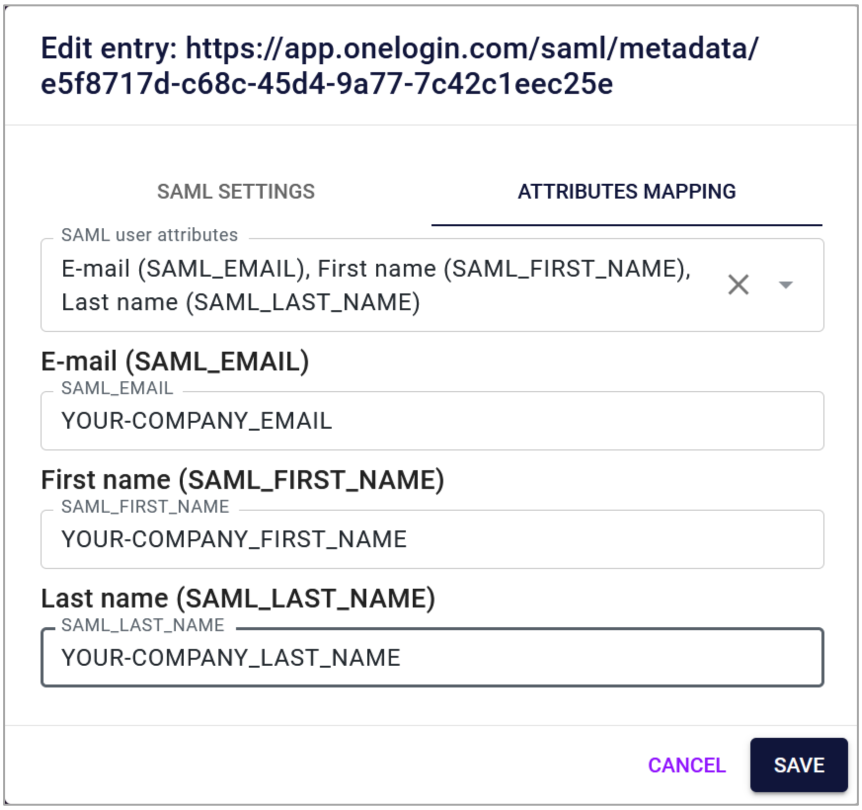
4. Click *Save* to finish editing.



Success

Updated SAML configuration "https:// [redacted]

The following screen shows this in the form of exemplary names like “YOUR-COMPANY_FIRST-NAME”.



Edit entry: https://app.onelogin.com/saml/metadata/e5f8717d-c68c-45d4-9a77-7c42c1eec25e

SAML user attributes: E-mail (SAML_EMAIL), First name (SAML_FIRST_NAME), Last name (SAML_LAST_NAME)

E-mail (SAML_EMAIL)

SAML_EMAIL: YOUR-COMPANY_EMAIL

First name (SAML_FIRST_NAME)

SAML_FIRST_NAME: YOUR-COMPANY_FIRST_NAME

Last name (SAML_LAST_NAME)

SAML_LAST_NAME: YOUR-COMPANY_LAST_NAME

6.1.3 Technical Setup Remarks

In the event of technical difficulties during the SAML configuration process, please verify that the length of the SAML_SSO_GROUP attribute does not exceed the limit of vchar255. Exceeding this limit by the SAML identity provider may result in an error.

Additionally, all Boolean values must be in lowercase to ensure optimal functionality. It is essential that your IdP adheres to this requirement.

6.2 Security

There are (at least) two different things to consider when talking about SAML security:

- Securing the transport (incl. SAML requests) via HTTPS (SSL/TLS) which is mandatory in the Uptempo hosting environment.
- Using digital signatures to sign the SAML assertions to ensure trust between the IdP and SP
  - This can be easily achieved via certificate exchange and appropriate configuration on both sides.

7 Example: Configuring Microsoft Entra ID for SAML Authentication

This comprehensive guide provides detailed instructions for configuring Microsoft Entra ID (formerly Azure AD) as a SAML Identity Provider (IdP) and integrating it with Uptempo as a service provider (SP).

> Attention
>
> Uptempo does not support the IdP setup in detail. The information below describes an ideal use case. Also refer to Microsoft documentation for the latest changes and updates. Learn more.

Prerequisites

Before beginning the configuration, ensure:

- You have administrator access to Microsoft Entra Admin Center
- Your Uptempo application is accessible via HTTPS
- You have administrator access to your Uptempo application
- You understand your organization's requirements for user attribute mapping

7.1 Service Provider (SP) Configuration

First, configure Uptempo to enable SAML authentication:

7.2 Access SAML Configuration

1. Log in to Uptempo.
2. Go to > *Administration* > *Overview* > *Fusion* > *Single Sign-On / SAML*.
3. If multiple configurations are supported, create a new entry for this integration. See section 5.

7.2.1 Prepare Service Provider Information

You'll need the following information from your SP for the Entra ID configuration:

- Entity ID (Identifier)

- Assertion Consumer Service (ACS) URL
- SP Certificate (usually in PEM format)
- Required attribute mappings

Uptempo offers a metadata XML file containing this information. Download it for easier configuration in Entra ID.

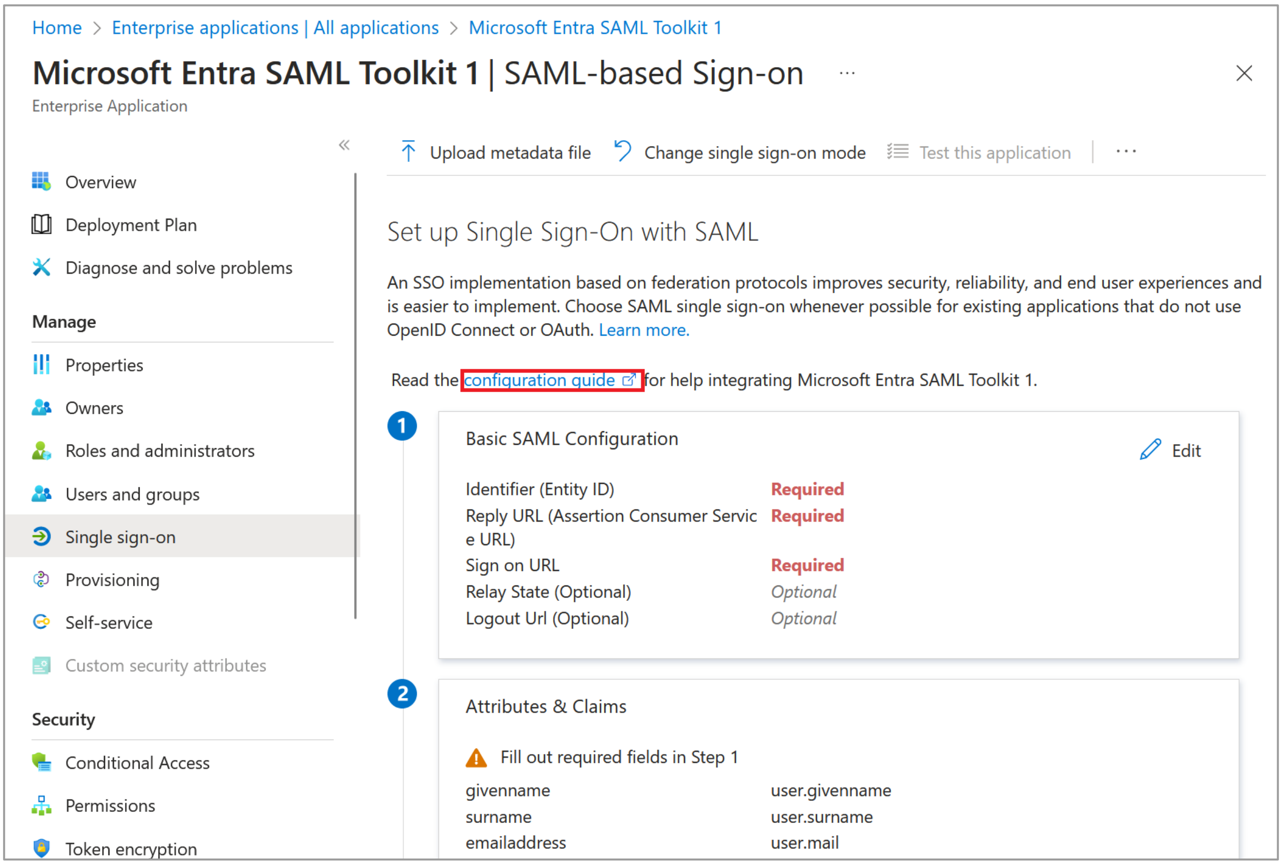
7.3 Microsoft Entra ID Configuration

7.3.1 Create Enterprise Application

1. Sign in to the Microsoft Entra Admin Center.
2. Go to “Enterprise applications”.
3. Click “New application”.
4. Select “Create your own application”.
5. Provide a meaningful name for your application.
6. Choose “Integrate any other application you don’t find in the gallery”.
7. Click “Create”.

7.3.2 Configure SAML Authentication

1. In the new application, navigate to “Single sign-on”.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Microsoft Entra SAML Toolkit 1.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Required
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

⚠ Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail

2. Select “SAML” as the authentication method.

3. Configure the Basic SAML Configuration:

   - Identifier (Entity ID): Enter Uptempo application’s entity ID.
   - Reply URL (ACS URL): Enter your Uptempo application’s assertion consumer service URL.
   - Sign on URL (optional): Your Uptempo application’s login page URL.
   - Relay State (optional): Is required by Uptempo application.

7.3.3 Setup Relay Party Trust

To configure a Relying Party Trust, we need to establish a trust relationship between your Identity Provider and Uptempo (the Service Provider). Think of this like creating a secure handshake agreement between two systems - they need to know how to recognize and trust each other.

Here's the detailed process:

Start in your Identity Provider's management console and search for the option to add a new Relying Party Trust. The exact location varies by provider, but it's typically under federation or application settings.

First, you'll be asked how you want to configure the trust. You have two options:

1. Import metadata file from Uptempo (recommended)
2. Enter the data manually

If using the metadata file:

- Download Uptempo's metadata XML file from your Uptempo SAML configuration
- Import this file into your IdP
- The system will automatically configure most settings

If entering manually, you'll need to configure these essential components:

1. Display Name Choose a meaningful name that identifies this as your Uptempo integration. This helps administrators recognize the application in your IdP's interface.
2. Protocol Selection Select "SAML 2.0" as the protocol. This is crucial because Uptempo specifically supports SAML 2.0 for secure authentication.
3. Service Provider Information Enter Uptempo's details:
    - Entity ID: `https://[your-instance].uptempo.io/auth/v1/saml`
    - Reply URL (Assertion Consumer Service URL): Same as Entity ID
    - These URLs tell your IdP where to send authenticated users
4. Certificate Configuration Import Uptempo's service provider certificate. This certificate enables encrypted communication between your IdP and Uptempo, ensuring security.
5. Identifier Configuration Add the Entity ID as a trusted identifier. This helps your IdP recognize legitimate requests from Uptempo.

After basic configuration, you'll need to set up claim rules. These rules determine what information about your users gets sent to Uptempo. Think of claims as pieces of user information that your IdP “claims” to be true about each user.

The final step is configuring access permissions — deciding which users in your directory should have access to Uptempo.

Remember, this trust configuration is bilateral — after setting up the Relying Party Trust in your IdP, you'll need to configure the corresponding trust settings in Uptempo using your IdP's metadata or certificate.

7.3.4 Set up Claim Rules for Your Relying Party Trust

This is essential for passing user information from your Identity Provider to Uptempo. Think of claim rules as translation instructions. They tell your Identity Provider how to convert your internal user information into a format that Uptempo can understand and use. Let's walk through setting up these rules step by step:

First Rule - Basic User Attributes:

1. In your Identity Provider's management console, find your Relying Party Trust for Uptempo
2. Open the "Edit Claim Rules" dialog
3. Choose “Add Rule”
4. Select “Send LDAP Attributes as Claims” as the rule template

For this first rule, you'll map fundamental user attributes:

- Active Directory attribute “User-Principal-Name” → Claim: “*SAML_USERNAME*”
- Active Directory attribute “Given-Name” → Claim: “*SAML_FIRST_NAME*”
- Active Directory attribute “Surname” → Claim: “*SAML_LAST_NAME*”
- Active Directory attribute “E-Mail-Addresses” → Claim: “*SAML_EMAIL*”

Second Rule – Group Memberships:

1. Add another rule
2. Select “Send Group Membership as Claims”
3. Choose the groups you want to map to Uptempo roles
4. Map these to the “*SAML_SSO_GROUP*” claim

Third Rule – User Management Controls:

This rule needs to be a “Transform an Incoming Claim” or “Send Claims Using a Custom Rule.” Here's the custom rule syntax:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"]

 => issue(Type = "SAML_CREATE_USER", Value = "true");

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"]

 => issue(Type = "SAML_UPDATE_USER", Value = "true");
```

Fourth Rule - Optional Attributes:

Create another LDAP attributes rule for additional information:

- Department → *SAML_FUNCTION*
- Company → *SAML_COMPANY*
- Country → *SAML_COUNTRY*
- Preferred Language → *SAML_USER_LANGUAGE*

Important Considerations:

To send both SAML_USERNAME and NameID with the user’s email address, add these claim rules in your Identity Provider:

1. For *SAML_USERNAME*:

   Email Address → *SAML_USERNAME*

2. For *NameID*:

   Email Address → *Name ID* (Email format)

Both rules should map to the same email address value (e.g., user@company.com). This ensures Uptempo can consistently identify users through either attribute.

- All claim names must exactly match Uptempo's expected attributes
- Boolean values must be lowercase ("true" or "false")
- String values are case-sensitive

- If you're using custom attribute names in your directory, map these carefully

Testing Your Rules:

After setting up your claim rules, it's crucial to test them:

1. Enable SAML tracing in your Identity Provider
2. Perform a test login
3. Review the SAML assertion to verify all attributes are being sent correctly
4. Check in Uptempo that the user information appears as expected

Common Issues to Watch For:

- Missing mandatory attributes
- Case mismatches in attribute names
- Incorrect value formats
- Group mapping misalignments

7.3.5 Export and Configure the Token Signing Certificate

The IdP X.509 token signing certificate is like a digital seal of authenticity. It allows Uptempo to verify that SAML responses genuinely come from your Entra identity provider.

Here's how to obtain and manage it:

1. Access the Certificate in Entra Admin Center:
    - Navigate to your Enterprise Application
    - Select "Single sign-on" from the left menu
    - Scroll to the "SAML Signing Certificate" section
    - You'll see your active certificate listed here
2. Download the Certificate:
    - Look for the "Certificate (Base64)" download option
    - Click to download the .cer file
    - This is your IdP X.509 certificate in Base64 format

   - The file contains the certificate between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” tags

3. Certificate Management:

   - Note the certificate start and end dates
   - Set up calendar reminders 30-60 days before expiration
   - You can have multiple active certificates during rotation
   - Consider creating a new certificate before the current one expires

4. Using the Certificate:

   - Open the exported file in a text editor and copy the Base64 content into the clipboard for the next step. If you're copying this certificate, you must include:
     - The BEGIN line
     - All the encoded certificate content, which will look like a long string of letters, numbers, and sometimes +/= characters.
     - The END line

     ```
     -----BEGIN CERTIFICATE-----
     [Certificate Content]
     -----END CERTIFICATE-----
     ```

   - Paste the encoded Token Signing Certificate into the Uptempo application SAML configuration (> *Administration* > *Overview* > *Fusion* > *Single Sign-On / SAML* > *IdP certificate (X509)* field).

The Uptempo application now trusts your configured identity provider.

5. Handling Multiple Certificates:

   - During certificate rotation, you may see both old and new certificates
   - The “Status” column shows which certificate is primary
   - Keep the old certificate active until all systems are updated

7.3.6 Configure User Attributes & Claims

1. Navigate to the “Attributes & Claims” section.

2. Configure the Name Identifier claim:

   - Select the appropriate source attribute (typically user.mail or user.userprincipalname)
   - Set the format as specified by Uptempo

3. Add additional claims as required:
   - First Name (user.givenname)
   - Last Name (user.surname)
   - Email (user.mail)
   - Groups (group.memberships)
   - Any custom attributes needed by your SP

7.3.7 Complete Uptempo SP Configuration

Return to Uptempo's SAML configuration to:

1. Import the Entra ID metadata file or configure manually:
   - IdP Entity ID
   - SSO URL
   - IdP Certificate
2. Configure attribute mappings to match the claims configured in Entra ID.
3. Save the configuration.
4. Enable SAML authentication.

7.4 Testing the Integration

7.4.1 SP-Initiated Testing

1. Access the Uptempo application login page.
2. Click the *SSO login* option.
3. Verify successful redirection to Microsoft login.
4. Complete authentication.

5. Confirm successful return to Uptempo with proper authorization.

7.4.2 IdP-Initiated Testing

1. In Entra Admin Center, locate your enterprise application.
2. Select “Single sign-on”.
3. Click “Test” under “Test single sign-on”.
4. Choose a test user.
5. Verify successful authentication and SP access.

7.5 Troubleshooting Guide

Common issues and solutions:

7.5.1 Authentication Failures

- Verify certificate validity and proper installation.
- Check clock synchronization between IdP and Uptempo.
- Confirm HTTPS configuration.
- Review browser console for JavaScript errors.
- Check Entra ID sign-in logs for error messages.

7.5.2 Attribute Mapping Issues

- Verify claim configurations match Uptempo requirements.
- Check attribute transformation rules.
- Confirm source attributes contain expected values.
- Review Uptempo logs for received SAML assertions.

7.5.3 Certificate Issues

- Ensure certificates are in the correct format (Base64).
- Verify certificate dates are valid.
- Check certificate key usage attributes.

- Confirm proper certificate installation on both sides.

7.6 Security Best Practices

1. Always use HTTPS for all endpoints.
2. Implement appropriate session timeout values.
3. Configure secure cipher suites.
4. Monitor authentication logs regularly.
5. Implement access reviews for authorized users.
6. Plan for certificate rotation before expiration.

7.7 Maintenance Considerations

- Document your configuration settings.
- Set calendar reminders for certificate expiration.
- Regularly review access permissions.
- Keep Service Provider metadata and certificates updated.
- Monitor Microsoft Entra ID updates and changes.

For additional support, consult Microsoft Entra ID documentation.

8 Example: Configuring Okta for SAML Authentication

This comprehensive guide walks you through setting up Okta as your SAML Identity Provider (IdP). While we use examples that reference typical service provider requirements, the principles apply broadly to any SAML integration with Okta.

> Attention
>
> Uptempo does not support the IdP setup in detail. The information below describes an ideal use case. Also refer to Okta SAML/SSO documentation for latest changes and updates. Learn more.

8.1 Prerequisites

Before beginning your Okta SAML configuration, ensure you have:

- Administrator access to your Okta organization
- Your service provider's SAML requirements documentation
- HTTPS endpoints for your service provider
- Administrator access to your service provider
- A clear understanding of required user attribute mappings

8.2 Initial Okta Configuration

8.2.1 Access Your Okta Organization

First, you'll need to access your Okta administrative interface:

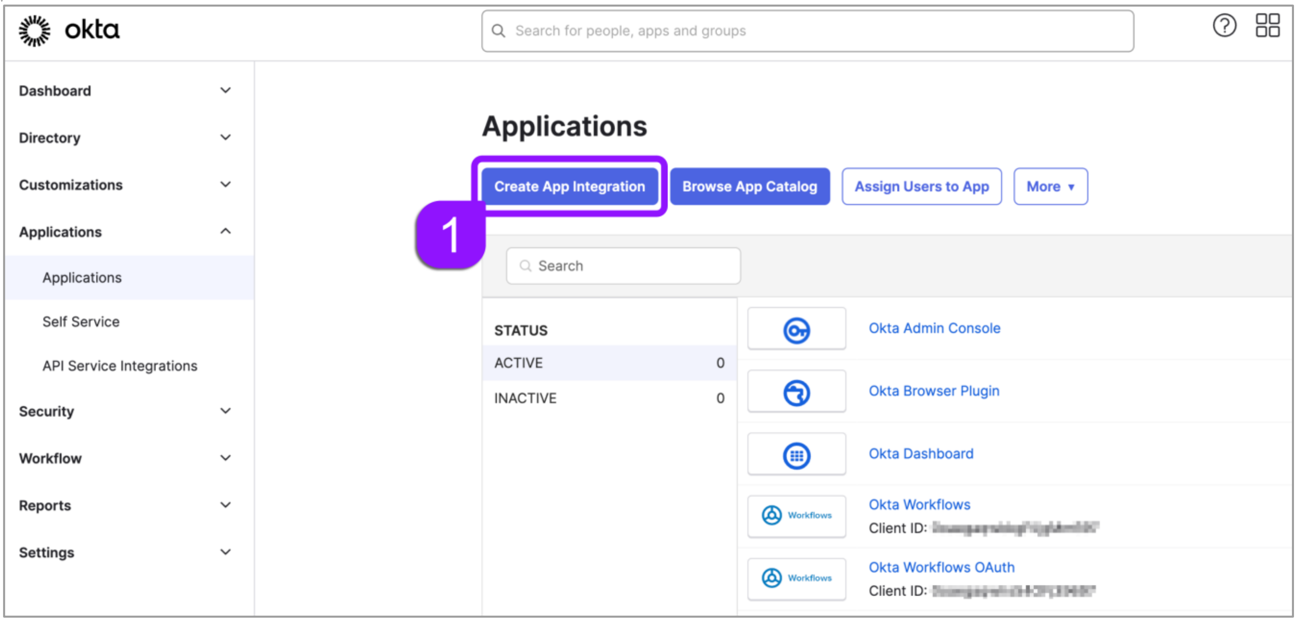
1. Sign in to your Okta organization admin portal (typically https://your-domain.okta.com/admin)
2. If this is your first time, verify your admin credentials and complete any required security steps
3. Familiarize yourself with the Admin Console layout, as you'll be using it extensively

8.3 Create the SAML Integration

Navigate to the application integration area:

1. In the Admin Console, select “Applications” > “Applications”

2. Click the “Create App Integration” button



3. In the creation dialog:

   - Select “SAML 2.0” as the Sign-in method
   - Give your integration a meaningful name
   - Click “Next” to proceed to the configuration

8.4 Configure SAML Settings

8.4.1 General SAML Settings

The SAML configuration requires several key pieces of information:

1. Configure the Basic Settings:

   - App name: A recognizable name for your integration
   - App logo (optional): Upload your application’s logo
   - App visibility: Control who sees the app in their Okta dashboard

2. Configure SAML Settings:
   - Single sign-on URL: Your SP’s Assertion Consumer Service (ACS) URL
   - Audience URI (SP Entity ID): Your SP’s unique identifier
   - Default RelayState (optional): Landing page after authentication
   - Name ID format: Usually Email or Persistent
   - Application username: How Okta identifies users to your SP

8.4.2 Advanced SAML Settings

Configure additional settings based on your SP’s requirements:

1. Signature Settings:
   - Response: Always signed
   - Assertion: Always signed
   - Choose the signing algorithm (SHA-256 recommended)
2. Authentication Context:
   - AuthnContextClassRef: Configure as required by your SP
   - Request Compression: Enable if your SP requires it

8.4.3 Certificate Management and Export

The IdP X.509 certificate is essential for your Service Provider to verify SAML assertions from Okta. Here’s a detailed guide on managing and obtaining this certificate:

1. Accessing Your Certificate:
   - Sign in to the Okta Admin Console
   - Navigate to “Applications” > Your Application
   - Select the “Sign On” tab
   - Locate the “SAML Signing Certificates” section
   - The active certificate will be displayed here

2. When to Export the Certificate:
    - During initial SAML setup with your Service Provider
    - When setting up a new application integration
    - Before the current certificate expires
    - When rotating certificates for security purposes
    - If your Service Provider requests certificate renewal
3. Downloading the Certificate:
    - In the “SAML Signing Certificates” section
    - Click “Actions” next to the active certificate
    - Select “Download Certificate”
    - Choose the format Uptempo requires:
        - Base64 encoded
4. Certificate Details and Options:
    - Validity Period: Usually 1-3 years
    - Encryption Options: Enable if SP requires encrypted assertions
    - Key Size: 2048-bit RSA is the secure standard
    - Algorithm: SHA-256 signing recommended
5. Using the Certificate:
    - Open the exported file in a text editor and copy the Base64 content into the clipboard for the next step. If you're copying this certificate, you must include:
        - The BEGIN line
        - All the encoded certificate content, which will look like a long string of letters, numbers, and sometimes +/= characters.
        - The END line

```
-----BEGIN CERTIFICATE-----
```

```
[Certificate Content]
-----END CERTIFICATE-----
```

  - Paste the encoded Token Signing Certificate into the Uptempo application SAML configuration (*> Administration > System Configuration > Single Sign-On / SAML > IdP certificate (X509)* field).

The Uptempo application now trusts your configured identity provider.

8.4.4 Configure Attribute Statements

Attribute statements map Okta user attributes to your SP's expected fields:

1. Basic Attribute Mapping:
   - Map standard attributes like FirstName, LastName, Email
   - Use the Okta Expression Language for complex mappings
   - Configure the NameID format and value
2. Custom Attribute Mapping:
   - Create custom expressions for special requirements
   - Use group memberships for role mapping
   - Configure any SP-specific attributes

Example mappings:

```
Name: user.firstName

EmailAddress: user.email

Group: contains(user.groups, "AdminGroup")
```

8.4.5 Assign Users and Groups

Control access to your SAML-enabled application:

1. User Assignments:
   - Navigate to the "Assignments" tab
   - Click "Assign" and choose "Assign to People"
   - Select users or groups for access

- Configure any user-specific attributes

2. Group Assignments:
    - Create groups if needed
    - Assign groups to the application
    - Configure group-level attribute overrides

8.5 Testing and Verification

8.5.1 SP-Initiated Testing:

- Access Uptempo’s login page
- Click *Sign in with SSO*
- Verify successful authentication
- Check attribute passing

8.5.2 IdP-Initiated Testing:

- Use Okta’s “View Setup Instructions”
- Test using the provided IdP-initiated URL
- Verify successful login flow
- Check landing page behavior

8.6 Troubleshooting Tools

Okta provides several troubleshooting features:

1. System Log:
    - Navigate to *Reports* > *System Log*
    - Filter for your application
    - Review authentication attempts
    - Identify configuration issues
2. SAML Tracer:

  - Use browser extensions like “SAML-tracer”
  - Capture and analyze SAML messages
  - Verify attribute statement content
  - Check signature validation

8.7 Security Best Practices

Implement these security measures:

1. Session Management:
   - Configure appropriate session timeouts
   - Enable session monitoring
   - Implement sign-out behavior
2. Access Policies:
   - Create sign-on policies
   - Configure MFA requirements
   - Set IP range restrictions
   - Enable adaptive authentication

8.8 Ongoing Maintenance

Plan for long-term management:

1. Regular Tasks:
   - Monitor certificate expiration
   - Review user assignments
   - Audit access patterns
   - Update attribute mappings
2. Documentation:
   - Record all configuration choices

- Document custom expressions
- Maintain testing procedures
- Keep SP requirements updated

8.9 Additional Features

Consider these advanced Okta features:

1. API Access:
    - Enable API integration
    - Generate API tokens
    - Configure rate limits
    - Monitor API usage
2. Monitoring:
    - Set up alert conditions
    - Configure notification rules
    - Monitor usage patterns
    - Track error rates

8.10 Support Resources

- Okta Developer Dashboard: https://developer.okta.com/
- Okta Support Portal: https://support.okta.com/
- SAML Troubleshooting Tools: Browser extensions and online decoders
- Okta Community Forum: For peer assistance and best practices

Keep this guide updated as Okta releases new features and security recommendations change. Regular reviews of your SAML configuration ensure continued secure operation of your single sign-on implementation.

9 Additional Info and Links

For further information regarding SSO groups, please consult the relevant sections of the Administration Manual.

For further information about SAML the following articles may be interesting:

Wikipedia:
https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Integrating Third-Party SAML Solution Providers with AWS:
http://docs.aws.amazon.com/IAM/latest/UserGuide/identity-providers-saml-solution-providers.html