SAMLベースの単一サインオン

SAMLタイプの統合プロファイルを構成するには、次の役職が必要です。

- 統括システム管理者

AlmaはSAML 2.0 Webブラウザ SSOプロファイルをサポートしています。これにより、Almaは認証および承認情報を交換できるようになり、ユーザーは外部システムにサインインまたはサインアウトしたり、Almaに自動的にサインインまたはサインアウトすることが可能になります。

Alma プロファイルの有効化とサードパーティの設定後、該当する教育機関のサポートスタッフが、Alma ログインショートカットを次のURLに変更します（Alma ドメイン名を参照）：`https://<Almadomain>/SAML`。

SAMLベースのSSOの詳細な概要については、https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/samlを参照してください。

Note

本番サーバーとサンドボックスが同じSAML IDプロバイダーを使用する場合、Ex Librisは両方の環境で同じ認証プロファイルを使用することをお勧めします。この場合は 、SAMLの追加設定は、サンドボックスの更新後のサンドボックス上で必要とされません。本番サーバーとサンドボックスが、異なるSAML　IDプロバイダを利用している場合、サンドボックスの更新を考慮した推奨設定で詳細を確認してください。

SAMLタイプの統合プロファイルを構成するには：

1. 統合プロファイルリストページ（**設定メニュー > 一般 > 外部システム > 統合プロファイル**）で、**統合プロファイルを追加**を選択します。統合プロファイルウィザードの最初のページが表示されます。
2. 統合プロファイルのコードと名前を入力します。
3. 統合タイプドロップダウンリストから**SAML** オプションを選択します。
4. システムドロップダウンリストから、Shibbolethなどの認証に使用するシステムを選択します。
5. **[次へ]**を選択します。次のページに移動します。

SAML定義

このページでは、次の情報を入力します。

SAML統合プロファイル ページ - アクション タブ

フィールド	説明
メタデータアップロード方法	メタデータからプロファイル情報を入力できます。これを行うには、**[メタデータリンク]**オプションを選択し、**[メタデータファイルのリンク]**フィールドにリンクの場所を入力します。メタデータアップロードを使用するには、**メタデータアップロード**オプションを選択し、**IdP メタデータファイルの更新**フィールドでファイルを選択します。
メタデータファイルリンク	
自動更新	Almaが2つのIdP証明書を同時に管理することによるロールオーバープロセスを円滑化するために選択します。これにより、IdPによって修正された場合に統合プロファイルがメタデータを取得するための統合プロファイルを設定できます。 **自動更新**を有効化すると、「プロファイルの作成」ボタンをクリックした場合と同様の方法で、統合プロファイル内の情報を2時間ごとに上書きします。適用前にSSOがうまく機能しているかテストすることが推奨されます。

フィールド	説明
	Note プロファイルの自動入力は現在、自己署名 IdP 証明書でのみサポートされています。IdP が署名に信頼のチェーンの証明書を使用する場合は、JKS ファイルを手動でアップロードする必要があります。
デフォルトSAMLプロファイル	このプロファイルをデフォルトとして構成する場合に選択します。 **Note** デフォルトではないプロファイルを使用するには、Alma URLで`/SAML/idpCode/[profile code]`サフィックスを使用します。
ForceAuthN	AlmaがSAML経由でユーザーを認証する際に、強制的に認証を行うかどうかを選択します。SAML ForceAuthN の詳細については、こちらを参照してください。 このチェックボックスが選択されていない場合、AlmaがSAMLを介してユーザーを認証すると、機関のIDPを介して直接認証されるため、エンドユーザーにSSOエクスペリエンスが提供されます。
IdP発行者 IdP ログインURL IdP IDの場所 ユーザーID属性名 IdP ログアウトURL Idp シングルログアウトサービス シングルログアウトリクエストにサイン	プロファイルに（上記のフィールドで）自動的にメタデータが移入されなかった場合は、**IDP発行者**、**IDPのログインURL**、**ユーザーID場所**、**ユーザーID属性名**、**IDP ログアウトURL**、および**IDPシングルログアウトサービス**、および**シングルログアウトリクエストにサイン**の設定を入力します。 これらのフィールドの詳細については、https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/samlを参照してください。
SHA1署名を適用する(デフォルトSHA2)	この署名を使用してログアウトリクエストに署名するには、**[SHA1署名の適用（デフォルトはSHA2）]**を選択して、プロファイルの署名をSHA1（SHA128とも呼ばれる）署名に変更します。 2020年7月以降に作成されたプロファイルの場合、デフォルト は SHA2（SHA256とも呼ばれる）ですが、必要に応じて SHA1に変更できます。 2020年7月に SHA2が導入される前に存在していたプロファイルの場合、デフォルトは SHA1ですが、必要に応じて SHA2に変更できます。
Alma メタ	**Alma** メタデータファイル バージョンを選択します。新しいプロファイルを作成する場合、自己署名された バージョ

フィールド	説明
データファイルバージョン	ン**20XX** と **署名済み証明書**の2つのオプションを利用できます。既存のプロファイルを編集する場合、自己署名されたバージョン**20XX**、**署名済み証明書**、および 以前に使用していた証明書の 3つのオプションを使用できます。 証明書を選**択**するときは有効期限をメモし、その日付より前に必ず置き換えることが重要です。 以前の証明書を使用することを選**択**した場合、Almaは有効期限後も引き続きそれを許可します。既存のプロファイルを編集して新しい証明書を選**択**した場合、プロファイルを保存すると、過去の証明書は使用できなくなります。 証明書を**変**更する前に、IT部門に確認しなければなりません。
IdP証明書1/2	Almaは、2つの 証明書を同時に保持できるようにし 、 両方の証明書を使用して認証を試みます。 これは、SAML IdPが（セキュリティ上の理由から）証明書を**変**更する場合に役立ちます。 証明書は統合プロファイルでアップデートする必要があります。2つの証明書を同時に保持することで、機関はIDPが切り替えを行うまで古い証明書を削除することなく、前もって新しい証明書を追加することができます。1つの証明書だけを保持すると、 両方のシステムで同時に証明書が更新されない場合 、Almaは「間違った」証明書で署名されたIDP からの**応**答を信用しないため、ダウンタイムが発生します。 証明書は循環型で、3番目 の証明書を追加すると1番目 の証明書が削除され、新しい証明書は2番目の証明書になります。2枚目の証明書のアップロードは必須ではありません。 各証明書について、**「証明書のアップロード方法」**で、アップロードする証明書の種類を選**択**します（ https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/inst_idp/saml を参照）。Almaでは、ファイルのアップロード、フリーテキストによる証明書の入力、JKS ファイルの入力が可能です。 **JKS**ファイル または **フリーテキスト証明書ファイル** を選**択**した場合は、ユーザーのファイルシステムからファイルを選**択**する欄が表示されます。 **フリーテキスト証明書** を選**択**すると、証明書のテキストを入力するフィールドが表示されます。 フィールドの横には、証明書がすでにアップロードされているかどうかを示すメモが表示されます。 **Note** 2017年1月1日をもって、AlmaはMD5withRSA暗号化アルゴリズムを使用した証明書をサポートしなくなりました。詳細については、 https://blogs.oracle.com/java-platform-group/entry/strengthening_signatures を参照してください。

有効
ユーザーグループ
リソースシェア図書館
統計カテゴリ
ログイン時にユーザーを更新
ログイン時にユーザー役職を再作成
Almaフィールドへのアサーション
	既存のAlmaのユーザーを持っていない認証**済**みSAMLユーザがログインしたときに、新しいAlmaのユーザーを自動的に作成したい場合は、自己登**録**のセクションで**アクティブ**を選**択**します。
	
	1. 自動的に作成されたユーザーに割り当てたい**ユーザグループ**、**リソースシェア図書館**、および**統計カテゴリー**を入力します。
	2. また、 **Alma**フィールドにアサーションフィールドをマッピングリンクを選**択**することで、Almaで**対応**するユーザーフィールドにSAML属性のマッピングを定義することができます。
	    1. コードフィールドにAlmaのフィールド名を入力します。**説明**でSAML アサーションコードを入力します。
	    2. カスタマイズを選**択**します。

フィールド	説明
フィールドのマッピング	
設定ファイルを編集	

6. **[保存]**を選択します。

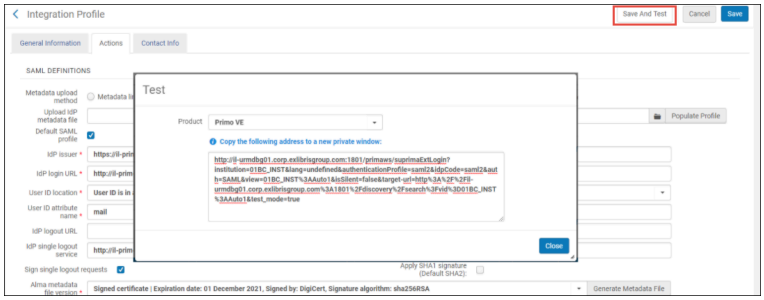
SAML統合プロファイルでの認証のテスト

SAML 設定ページ から直接SAML統合をテストすることができます。これにより、Almaからログアウトして再度ログインする必要がなくなり、 認証に失敗した場合 は何が問題だったのかを明確に示すことができます。

SAML 統合プロファイルをテストする前に、プロファイルを保存してください。これにより、必要に応じて既存のプロファイルに 戻すことができます。プロファイルを保存しない場合、Alma は既存のプロファイルを新しい プロファイルバージョンで置き換えます。

SAML統合 プロファイルの認証をテストするには：

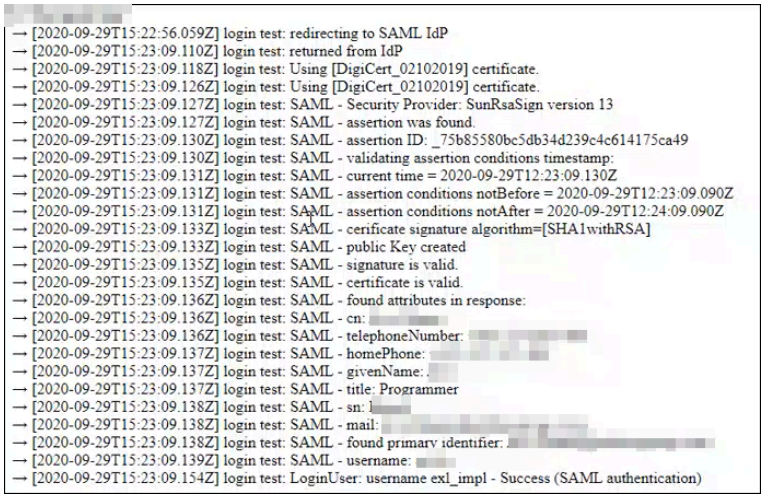
1. SAML 統合プロファイルの関連情報をすべて入力したら、テスト ボタンをクリックしてください。ポップアップ ウィンドウが開きます。
2. ポップアップウィンドウで、所属機関の利用可能な製品のリストから 製品を選択します。これにより、統合プロファイルに設定されたIdPへの テストリンクが生成 されます。
   bc.almaで作業していて、同じドメインを設定したい場合は、 代わりにna03.almaにログインしてください。



3. このリンクをコピーして、別のブラウザ（Chromeをお使いの場合はIncognito タブ）に貼り付けてください。SAML ログインページが開く。
4. 資格情報を送信します。認証結果と、何が起こったのか、何が間違っていたのかを説明する追加メッセージが表示された 新しいページにリダイレクト されます。

Note

この 資格情報はテストのためだけ に使用され、ここで資格情報 を入力したユーザーが実際にログインすることはありません。



5. テストウィンドウを閉じて、Almaに戻ります。 必要に応じて、統合プロファイル/IdPを更新し、 再度テストを行います。 変更する必要がなければ、プロファイルを保存します。

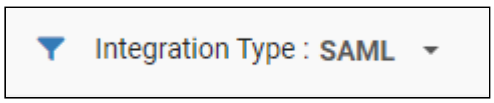
期限切れの証明書の置き換え

2025年に期限が切れる自己署名証明書を置き換える必要がある場合は、次のガイドを参照してください。

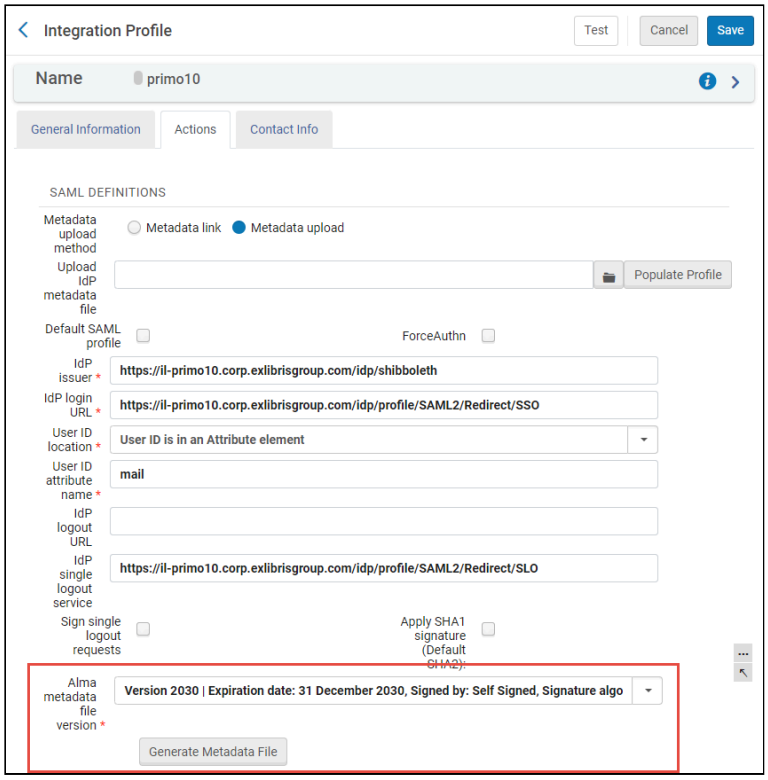
SAML SSO は通常、期限切れの証明書でも機能します。一部の IDP では期限切れでない証明書を強制する（またはそのように設定できる）ので、蔵書では確実に最新の証明書が追加され、それらの IDP を持つ顧客が証明書を更新することができます。

Alma メタデータ ファイル バージョン：

1. 統合プロファイルリスト 画面にアクセスしてください（**Alma設定 > 一般 > 外部システム > 統合プロファイル**）。
2. 統合タイプドロップダウン メニューで、**SAML**を選択します。



3. 既存の統合プロファイルを選択し、 行アクションボタンで**編集**を選択します。
4. 統合プロファイル画面で、アクションタブを選択します。
5. **Alma**メタデータ ファイルバージョンドロップメニューで、新しい証明書を選択します。
6. メタデータ ファイルの生成ボタンを選択して、ファイルをダウンロードします (または、そのファイルを指すリンクを取得します)。メタデータはIDPに アップロードされます。



統合プロファイル画面の、**Alma**メタデータファイルバージョンのドロップメニュー

Note

ダウンタイムを回避するには、AlmaとIDPの変更を同時に行う必要があります。IT部門との間で、AlmaとIDPで変更が行われる正確な時間を調整します。

追加の証明書を追加：

上記のプロセス（Almaのメタデータファイルバージョン）を調整せずに証明書を変更したい場合は、 次の手順を完了します。

Note

各ステップは都合の良い時間に行うことができます **(ただし、古い証明書の有効期限が切れる前に行う必要があります）**。

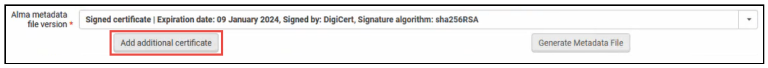
ユーザーは、新しい証明書を削除することで、以前に署名された証明書に戻すことができます。たとえば、新しく追加された 証明書（例: IDP証明書1）および以前に署名された証明書（例: IDP証明書2）がAlmaにロードされます。証明書の削除（

Remove certificate

）ボタンを使用して、IDP証明書1を削除するだけです。

---

1. 統合プロファイル画面 **>** アクションタブで、**証明書を追加**ボタンを選択します。別のドロップダウンが表示され、新しい証明書を選択できます。**[保存]**を選択します。



2. メタデータファイル（両方の証明書を含む）を生成し、IDP にアップロードします。
3. Almaから古い証明書を削除し、**保存**を選択します。
4. 再度、Almaからメタデータファイル（新しい証明書のみが含まれる）を生成し、IDPにアップロードします。

IdP署名 証明書の置き換え

Note

このセクションは、お客**様**の機関が統合プロファイルの 「IdP証明書1/2」セクションで1つの証明書しか保持していない場合にのみ関係します。両方の証明書がアップロードされている場合、2つの証明書を同時に保持することで、IDPが切り替えを行うまで古い証明書を削除せずに、機関が先に新しい証明書を追加することができます。 IdP署名証明書の自動ロールオーバー を参照してください。

Alma SAML プロファイルのIdP署名証明書が**変**更されようとしている場合は、サポートされている3つの方法のいずれかを使用して新しい証明書をアップロードします:

- フリーテキスト証明書、
- 証明書ファイル、
- JKS ファイル。信頼チェーン証明書にはJKSが必要です。

IdPが新しい証明書に切り替わると同時に、この**変**更を実行して**[保存]**をクリックしてください。そうしないと、この期間中にSAML認証は失敗します。

Note

AlmaでSAMLプロファイルを更新せずに、新しい署名証明書に 自動的に切り替えると、 システムがダウンする恐れがあります。

IdP 署名証明書の自動ロールオーバー

1. 統合プロファイルが自動的に更新されるよう設定されていること、およびリンクが有効であることを確認します。
2. IdP で追加の証明書を設定します。
3. Alma（および存在する場合は他のSP）が新しいメタデータを読み取るまで待ちます。
4. IdP から古い証明書を削除します。