Ex Libris アイデンティティサービス

Ex Libris アイデンティティサービスは、専用のID管理ソリューションに基づいています。このサービスは、これまでAlmaのお客様が使用していた内部認証方法に代わるものです。内部のAlmaユーザーのすべてのパスワードは、Ex Libris アイデンティティサービスに保存されます。Ex Libris アイデンティティサービスは、Ex Librisがデータセンターでホストしています。このサービスの詳細については、 https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/exl_identity_serviceを参照してください。

Ex Libris アイデンティティサービスでは、次のパスワードに関する考慮事項が適用されます。

- パスワードの強度は設定できません。
- パスワードの 有効期限はありません。
- 15回ログインに失敗すると、パスワードは30分間ロックされます。
- スタッフユーザーがAlmaのログインページで間違ったユーザーとパスワードの組み合わせを入力すると、パスワード初期化ページにリンクされている **パスワードを忘れた場合** リンクを含むエラーメッセージが表示されます。Primo/PrimoVEで「パスワードを忘れた場合」オプションを表示するには、 設定 のアップデートが必要です。詳細については、ナレッジ記事 認証のためにAlmaを使用する際に、新しいUIのログインページに「パスワードを忘れた場合」リンクを追加する方法を参照してください。

アイデンティティサービスラベルは、内部ログインメッセージコードテーブルで設定できます。アイデンティティサービスラベルを参照してください。

Almaのユーザーの場合 、ユーザー詳細ページの **メッセージを送信** ドロップダウンリスト内の **アイデンティティサービスのためにパスワードを初期化** オプション選択することによって、パスワードの初期化レターが個々のユーザーに送信されます。このレターは、アップデート/通知ユーザージョブを実行し、ジョブパラメータページの **ユーザへの通知を送信** ドロップダウンリストから、 **アイデンティティサービスメール** オプションを選択することにより、ユーザーのグループに送信されます。

Note

- 新しいパスワードは8文字以上に設定する必要があり、ユーザーネームや、パスワードによく使われる単語の使用はできません。
- パスワードのリセットレターが**ユーザーへのアップデートまたは通知**ジョブから、またはメッセージを送信のドロップダウンリストから送信された後、そのリンクは24時間有効となります。レターが**パスワードをお忘れですか？**のリンクから送信されると、 そのレターは1時間有効です。
- パスワードの初期化画面で、ユーザーはユーザー名またはEメールアドレスを入力するように求められます。ユーザーがユーザー名を入力すると、ユーザーの優先アドレスにEメールが送信されます。ユーザーがEメールアドレスを入力すると、システムは指定されたEメールアドレスを検索し、見つかった場合は、優先アドレスではなくてもそのEメールアドレスを使用します。Eメールアドレスが見つからないか、複数のユーザーに帰属している場合、Eメールは送信されません。

Almaへのログインの詳細については、ユーザーインターフェイスへのログイン/ログアウトを参照してください。

多要素認証 (MFA)

Note

この機能を使用するには、**mfa_for_alma_hep**パラメータを有効にする必要があります（ユーザー設定を参照）。

Almaを設定して、多要素認証 (MFA) の使用を推奨 (または強制) することができます。

MFA（多要素認証）をサポートするには、**「ワンタイム・トークン・レターを使用したログイン」** を有効にする必要があります（「Almaレターの設定」を参照）。

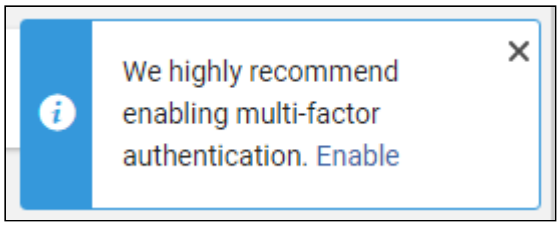
MFAの推奨

Note

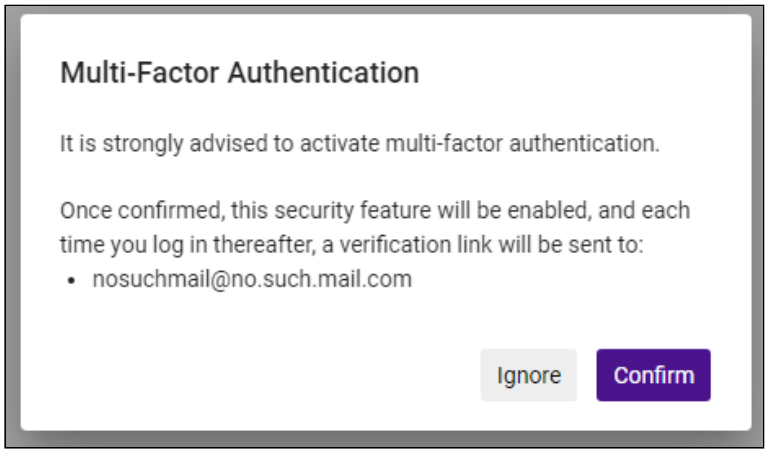
これには、 **mfa_for_alma_hep**パラメータを 「suggest 」に設定する必要があります（ユーザー設定を参照）。

MFAを推?するには、以下のようにします:

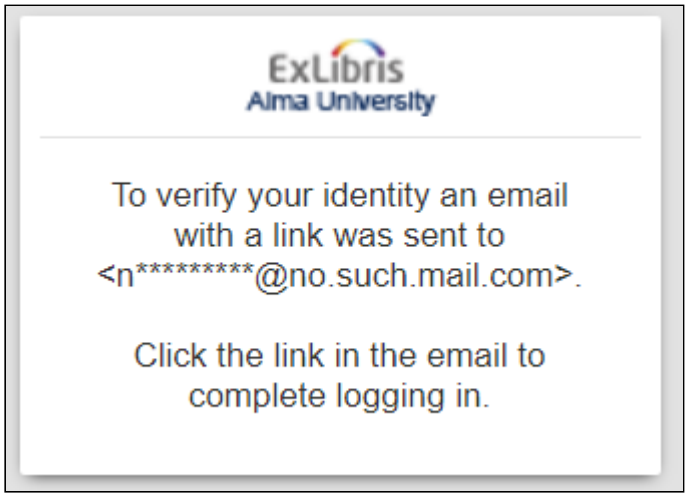
1. 設定後に初めてログインする場合、**mfa_for_alma_hep** パラメータを「suggest」に設定すると、ユーザーには通常のユーザー名とパスワードの入力が求められます。
2. ログイン後、ユーザーに多要素認証を有効にするよう推奨するメッセージが表示されます。



3. ユーザーはメッセージを無視したり、Xボタンでキャンセルしたり、あるいは、**有効にする**を選択することができます。
4. ユーザーが**有効を選択した場合、 無視**または **確認**を促すメッセージが表示されます。このメッセージには、ログインリンクが送信されるユーザーの電子メールアドレス（複数）が含まれます。

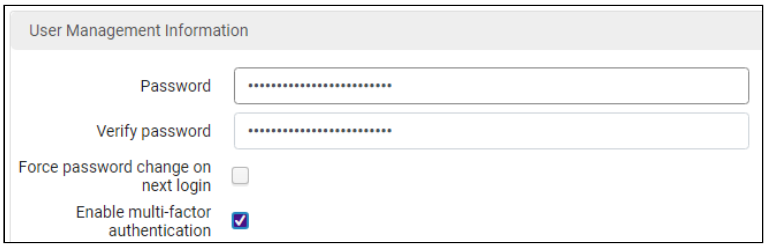


5. ユーザーが**確認**を選**択**すると、次回ログイン時にログインリンクが電子メールに送信され、リンクが送信されたことを知らせるメッセージが表示されます。



ユーザーが**無視**を選**択**した場合、 MFA推**奨**メッセージはユーザーがログインするたびに**毎**回表示されます。

6. 今後、ユーザーがログインするたびに（ユーザー名とパスワードの**検**証後）、このメッセージが表示されます。（5月の新機能） このリンクは 10分間 有効です。リンクをアクティブ化すると、ユーザーは製品のホームページに移動します。（**5月の新機能**） このリンクは、ログイン操作を開始した同じブラウザでのみ使用可能であることに注意してください。
7. ユーザーは、**[管理者] > [ユーザー管理] > [スタッフ] > [ユーザー管理情報]**のユーザー管理情報ページから、MFAの有効化／無効化を行うこともできます。



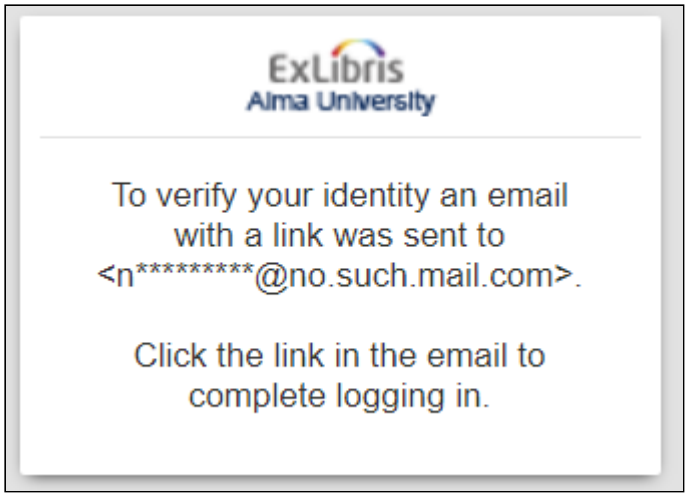
MFAの強制

Note

これには、 **mfa_for_alma_hep**パラメータを 「force 」に設定する必要があります（ユーザー設定を参照）。

MFA を強制するには、以下のようにします:

1. **mfa_for_alma_hep**パラメータを 「force 」に設定すると、すべてのユーザーにMFAによる認証が要求されます。
2. ログインすると、通常のユーザー名とパスワードの認証が求められます。
3. 製品に入る前に（ログインページから）、ユーザーの電子メールにリンクが届き、メッセージが表示されます。



4. （**5月の新機能**）このリンクは 10分間有効です。リンクをアクティブ化すると、ユーザーは自分の製品ホームページにリダイレクトされます。（**5月の新機能**）リンクは、ログインフローを開始した同じブラウザでのみ使用できる点にご注意ください。

Note

この **mfa_for_alma_hep**パラメータが「force」に設定されている場合、特定ユーザーのMFAフローを オフにする方法はありません。
