

セキュリティ

AlmaへのログインをIPレンジで制限する

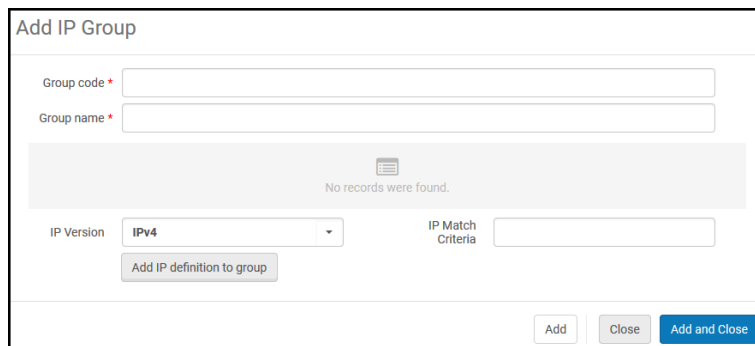
IPグループを設定するには、下記の役職が必要です：

- 総合システム管理者

IPアドレスに応じて、ユーザーがAlmaにログインするのを制限できます。この機能を設定するには2つのステップがあります。まずIPグループを作成してから、これらのグループのログインアクセスを設定します。これらのIPグループのみが、Almaへのログインを許可されます。

IPグループによるログインを制限するには：

1. IPグループ設定ページ (設定メニュー > 一般 > セキュリティ > IPグループ設定) から、IPグループを追加を選択します。「IPグループを追加」パネルが表示されます。



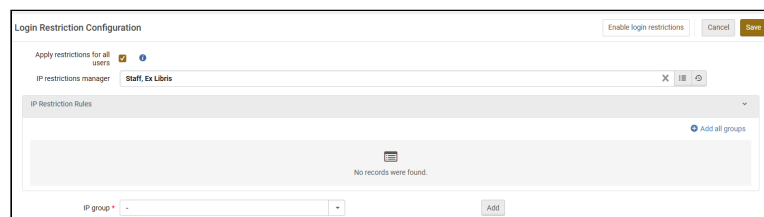
IPグループを追加

2. 以下を入力します：
 - グループコード – IPグループのコード
 - グループ名 – 後で変更できるIPグループの名称
 - IPバージョン – IPv4またはIPv6
 - IP一致基準 – 特定のIPアドレスまたはIPレンジ (有効な2つのIPアドレスをハイフンで区切ってください)
3. グループにIPの定義を追加を選択します。IPレンジがグループに追加され、テーブルに表示されます。
4. 各グループについて複数のIPレンジを定義できます。必要に応じてステップ2と3を繰り返します。IPレンジを削除するには、その行のアクションリストで削除を選択します。
5. IPレンジの追加が完了したら、追加して閉じるを選択します。IPグループが追加されます。

グループを編集するには、その行のアクションリストで編集を選択します。グループを削除するには、その行のアクションリストで削除を選択します。

6. 「ログイン制限設定」ページを開きます (設定メニュー > 一般 > セキュリティ > ログイン制限設定)。ログイン制限

は、このページで有効にするまでは無効です。ご注意ください。



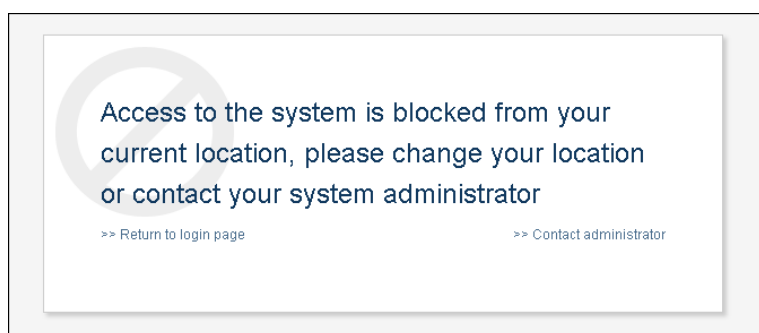
ログイン制限設定

7. ユーザーを編集する際に「すべてのログイン制限を無効化する」を選択することで、特定のユーザーに対するログイン制限を無効化することができます（[「ユーザーの編集」](#)を参照）。
（5月の新着情報）【すべてのユーザーに制限を適用する】チェックボックスを選択すると、ユーザーレベルの無効化をキャンセルし、また、一般システム管理者の役割を持つユーザーに対してログイン制限も適用します。以前の設定は削除されず、チェックボックスの選択を解除すると元に戻ります。
8. ログインアクセスを許可したいIPアドレスのIPグループからIPグループを選択し、追加を選択します。すべてのIPグループを追加するには、全グループを追加を選択できます。
IPグループが選択されると、他のすべてのIPアドレスはログインが制限されます。
9. IP制限マネージャーボックスからマネージャーを選択します（必須）。制限されたIPアドレスからログインが試行された際に、このマネージャーはユーザーが送信したメッセージを受入します。
10. ログイン制限の有効化を選択する。ログイン制限を有効や無効にすることなく変更を保存するには、保存を選択します。

Note

- IPログイン制限を有効にするには、ログイン制限の有効化を選択する必要があります。
- 総合システム管理者の役職が割り当てられているユーザーは制限されません。
- 後でログイン制限を無効にするには、ログイン制限の無効化を選択します。

制限されたIPアドレスのユーザーがAlmaにログインしようとする時、下記のメッセージが表示されます：



アクセスがブロックされました

ユーザーは、上記のように設定されたIP制限マネージャーに連絡するため、管理者へコンタクトを選択できます。

CSP (コンテンツセキュリティポリシー) ヘッダー設定

CSPヘッダーディレクティブを有効にして構成し、Webアプリケーションのセキュリティポリシーを微調整できます。この設定にアクセスするには、設定 > 全般 > CSPヘッダー設定に移動します。

Name	Explain	Active	Initial Allowed List	Allowed List - Additions
frame-ancestors	Specifies valid parents that may embed a page using <iframe> etc.	<input checked="" type="checkbox"/>	'self' https://*.exlibrisgroup.com https://*.exlibrisgroup.com.cn	Fine tune in "Frame Embedding Options"
object-src	Specifies valid sources for the <object> and <embed> elements	<input type="checkbox"/>	blob: 'self' *exlibrisgroup.com *exlibrisgroup.com.cn www.google-analytics.com stats.g.doubleclick.net s3.amazonaws.com www.youtube.com youtube.com artic.contentdm.oclc.org	
worker-src	Specifies valid sources for Worker, SharedWorker, or ServiceWorker scripts	<input type="checkbox"/>	blob: 'self' *exlibrisgroup.com *exlibrisgroup.com.cn www.google-analytics.com stats.g.doubleclick.net s3.amazonaws.com www.youtube.com youtube.com artic.contentdm.oclc.org	
upgrade-insecure-requests	Instructs browsers to treat all of a site's insecure URLs (those served over HTTP) as though they have been replaced with secure URLs (those served over HTTPS)	<input type="checkbox"/>	-	
script-src	Valid sources for JavaScript	<input type="checkbox"/>	'self' 'unsafe-inline' 'unsafe-eval' *exlibrisgroup.com *google-analytics.com *cookielaw.org *googletagmanager.com *librarything.com *amazonaws.com *hathitrust.org *salesforcevegent.com *pendo.io	
form-action	Restricts the URLs that can be used as the target of form submissions	<input type="checkbox"/>	'self' *exlibrisgroup.com *googleapis.com	
frame-src	Specifies valid sources for nested browsing contexts loading using elements such as <frame> and <iframe>	<input type="checkbox"/>	'self' *exlibrisgroup.com	

Preview:
Content-Security-Policy: frame-ancestors 'self' https://*.exlibrisgroup.com https://*.exlibrisgroup.com.cn; report-uri /r/https/CSPReportEndpoint.jsp; report-to: csp-report-endpoint;

CSPヘッダー設定

下部のプレビュー ペインにはヘッダーが表示され、設定が変更されると自動的に更新されます。

最初の4つのディレクティブ (frame-ancestors、object-src、worker-src、upgrade-insecure-requests) はデフォルトでアクティブになっており、無効にすることはできません。ただし、許可リスト - 追加カラムにドメインを追加することもできます。

最後の5つのディレクティブ (以下で説明) はデフォルトで無効になっていますが、最初の4つのディレクティブとは異なり、有効にすることができます。許可リスト - 追加カラムで、許可リストに追加ドメインを追加できます。

1. form-action:

- フォーム送信のターゲットとして使用できるURLを制限します (`<form action="..." />`)。フォームが悪意のあるサイトに送信されるのを防ぐのに役立ちます。

2. base-uri:

- 文書の `<base>` 要素内で使用できるURLを指定します `<base>` 要素は、ドキュメント内のすべての相対URLに使用するベースURLを指定するので、これを制御することで、攻撃者がベースURLを変更して、リンクを悪意のあるサイトにリダイレクトすることを防ぐことができます。

3. script-src:

- このディレクティブは、JavaScriptの有効なソースを指定します。信頼できるソースからのスクリプトのみをページ上で実行できるようにすることで、XSS攻撃を軽減するのに役立ちます。たとえば、スクリプトを独自のドメインまたは信頼できるCDNからのみ読み込むように指定できます。

4. frame-src:

- このディレクティブは、`<frame>`、`<iframe>`、`<object>`、`<embed>`、および`<applet>` を使用して、コンテンツを埋め込むための有効なソースを指定します。これは、フレーム内に埋め込むことができるソースを制御し、クリックジャッキングやその他のフレームベースの攻撃を防ぐのに役立ちます。

5. connect-src:

- このディレクティブは、XMLHttpRequest、Fetch、WebSocket、およびEventSourceのような

メカニズムを使用して、ドキュメントが取得できるURLを制限します。スクリプトがデータを送信できる場所を制御し、データ流出のリスクを軽減するのに役立ちます。

6. style-src:

- HTTP `コンテンツセキュリティ ポリシー` (CSP) `style-src` ディレクティブは、スタイルシートの有効なソースを指定します。

7. img-src:

- HTTP `コンテンツセキュリティ ポリシー` `img-src` ディレクティブは、画像とファビコンの有効なソースを指定します。

8. font-src:

- HTTP `コンテンツセキュリティ ポリシー` (CSP) `font-src` ディレクティブは、`@font-face` を使用して読み込まれるフォントの有効なソースを指定します。

9. child-src:

- HTTP `コンテンツセキュリティポリシー` (CSP) `child-src` ディレクティブは、`<frame>` や `<iframe>` などの要素を使用して読み込まれる `ウェブワーカー` とネストされたブラウジングコンテキストの有効なソースを定義します。ワーカーの場合、非標準のリクエストはユーザーエージェントによって致命的なネットワークエラーとして扱われます。

10. default-src:

- HTTP `コンテンツセキュリティポリシー` (CSP) `default-src` ディレクティブは、他のCSP `フェッチ ディレクティブ` のフォールバックとして機能します。存在しない各ディレクティブについては、ユーザーエージェントは `default-src` ディレクティブを作成し、この値を使用します。

ログインリダイレクト許可リスト

潜在的なセキュリティ問題（オープンリダイレクトの脆弱性）を回避するために、信頼できるサイトのリストを作成できます。

信頼できるサイトのリストを作成するには、以下のようにします:

1. `limit_login_redirects`（設定 > 一般 > その他の設定）パラメータが、必ずtrueに設定されているようにします。
2. 設定 > 全般 > リダイレクト許可リストに移動します。
3. 信頼されたドメインごとに新しい行を追加します。このコードは説明のみを目的としており、Almaでは使用されません。

Note

Ex Librisに属するドメイン (*.exlibrisgroup.com) をリストする必要はありません。

Redirect Allowed List				
Values	Notes			
1 - 1 of 1	Code			
<div style="text-align: right;"> Import Add Row </div>				
Enabled: All				
Enabled	Code	Domain	Updated By	Last Updated
<input checked="" type="checkbox"/>	ezproxy	primio-lib-edu.ezproxy.lib.edu	ex_lmpl	10/07/2024

クリックジャッキングの防止

iFrameの埋め込みオプションを制御するには、次の役割でなければなりません。

- 統括システム管理者

クリックジャッキングとは、機密性の高いページから実際の管理を含む無害なページを表示して、ユーザーをだます攻撃です。これらの制御は、制御以外のすべてをマスクする背景フレームを使用して偽装されており、ユーザーは、他のWebサイトで機密機能をクリックしていることを実際に認識できません。これにより、ユーザーは無意識のうちにマルウェアをダウンロードしたり、資格情報や機密情報を提供したり、送金したり、オンラインで製品を購入したりする可能性があります。

ExLibris 製品を介したクリックジャッキングを防ぐために、ExLibris はポリシーに基づく緩和手法を採用しています。これにより機関は、サイトがiframe内に含まれている場合に実行する適切なアクションについてブラウザに指示できます。

Note

このページを変更すると、他の製品からのUI統合が壊れる可能性があります。このページの使用方法について疑問がある場合は、[ExLibrisカスタマーサポート](#)にご相談ください。

サイトがiframe

内に含まれている場合に実行するアクションを設定するには：

1. **iFrame埋め込みオプション**テーブルを開きます (**構成>一般>セキュリティ>iFrame埋め込みオプション**)。
2. 目的の製品とコンポーネントについては、行アクションで**[カスタマイズ]**を選択します。

Note

- Alma管理とEsploro 管理はフレーム化できません。この構成は編集できません。
- Azure IDPを使用している場合、iFrameの埋め込みはサポートされません。

3. **[アクション]**列で、サイトがiFrame内に含まれている場合に実行する適切なアクションを選択します。
 - **すべて許可** (デフォルトオプション) - すべてのページがこのページをiFrame内に読み込めるようにします。
 - **保護を許可 - 信頼** できるページのみ このページをiFrame内にロードすることが許可されています。このオプションを選択した場合は、安全なドメイン列は信頼できるURLを示します (指定できるURLの数に制限はありません。複数のURLを、それらの間に空白を入れてリストしてください)。

Note

https://*.WEBSITEHERE.comを追加することをお勧めします。例えば、https://*.amazon.com”。

- **すべてブロック** — ページをフレーム化するすべての試みを拒否します。

4. **【保存】**を選択します。