Sicherheit

Einschränkung des Alma-Logins nach IP-Bereich

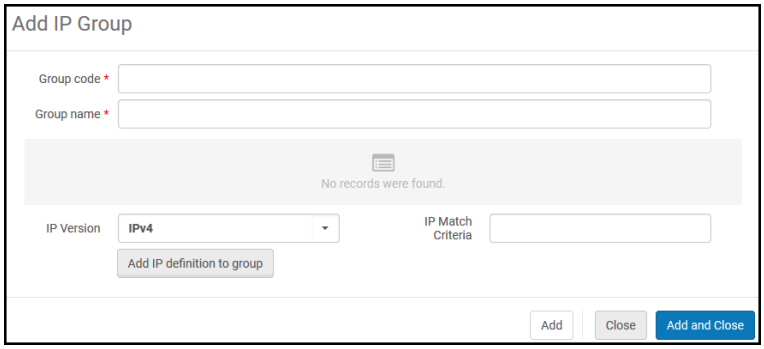
Um die IP-Gruppen-Konfiguration zu konfigurieren, müssen Sie die folgende Rolle innehaben:

- Allgemeiner Systemadministrator

Sie können Benutzern den Login aufgrund der IP-Adresse verbieten. Diese Funktion wird in zwei Schritten konfiguiert. Sie definieren zunächst IP-Gruppen und konfigurieren danach den Login-Zugriff für diese Gruppen. Danach sind nur diese IP–Gruppen zur Anmeldung in Alma autorisiert.

Um den Login nach IP-Gruppen einzuschränken:

1. Klicken Sie auf der Seite IP-Gruppenkonfiguration (**Konfigurationsmenü > Allgemein > Sicherheit > IP-Gruppenkonfiguration**) auf **Neue IP-Gruppe**. Die Seite Neue IP-Gruppe erschient.

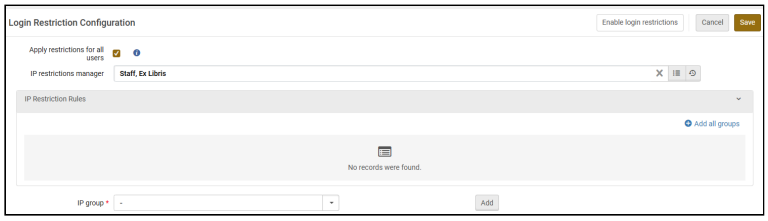


Neue IP-Gruppe

2. Geben Sie Folgendes ein:
   - Gruppen-Code – Ein Code für die IP-Gruppen
   - Gruppenname – Ein Name für die IP-Gruppe, welcher später geändert werden kann
   - IP-Version – IPv4 oder IPv6
   - IP-Übereinstimmungskriterien - eine spezifische IP-Adresse oder ein IP-Bereich (zwei gültige IP-Adressen, getrennt durch einen Bindestrich).
3. Klicken Sie auf **IP-Definition zu Gruppe hinzufügen**. Der Bereich wird zur Gruppe hinzugefügt und erscheint in der Tabelle.
4. Sie können mehrere IP-Bereiche für jede Gruppe definieren. Wiederholen Sie Schritte 2 und 3 nach Bedarf. Um einen Bereich zu entfernen, klicken Sie auf **Löschen** in der Zeileny-Aktionsliste.
5. Wenn Sie mit dem Hinzufügen von IP-Bereichen fertig sind, klicken Sie auf **Hinzufügen und schließen**. Die IP-Gruppe ist hinzugefügt.

   Um die Gruppe zu bearbeiten, klicken Sie auf **Bearbeiten** in der Zeilen-Aktionsliste. Um die Datei zu löschen, klicken Sie auf **Löschen** in der Zeilen-Aktionsliste.

6. Öffnen Sie die Seite Login-Beschränkungs-Konfiguration (**Konfigurationsmenü >Allgemein > Sicherheit > Login-Beschränkungs-Konfiguration**). Beachten Sie, dass Login-Einschränkungen solange deaktiviert sind, bis Sie diese auf dieser Seite aktivieren.



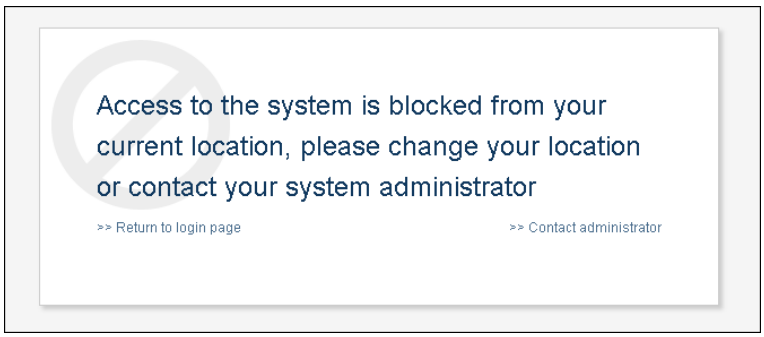
Konfiguration der Login-Beschränkung

7. Die Login-Einschränkungen können für einen bestimmten Benutzer überschrieben werden, indem beim Bearbeiten des Benutzers **Alle Login-Einschränkungen deaktivieren** ausgewählt wird (siehe Bearbeiten von Benutzern). (Neu für Mai) Das Aktivieren des Kontrollkästchens **Einschränkungen für alle Benutzer anwenden** hebt die Überschreibung auf Benutzerebene auf und wendet auch die Login-Einschränkungen für Benutzer mit der Rolle „Allgemeiner Systemadministrator“ an. Beachten Sie, dass die vorherige Konfiguration nicht entfernt wird und wiederhergestellt wird, sobald das Kontrollkästchen deaktiviert wird.
8. Wählen Sie die IP-Gruppen aus der Dropdown-Liste **IP-Gruppe** aus, deren IP-Adressen Sie einen Login-Zugriff erlauben möchten, und klicken Sie auf **Hinzufügen.** Sie können auf **Alle Gruppen hinzufügen** klicken, um alle IP-Gruppen hinzuzufügen.
Sobald eine IP-Gruppe ausgewählt ist, werden alle anderen IP-Adressen von der Anmeldung gesperrt.
9. Wählen Sie einen Manager aus dem Feld **IP-Einschränkungs-Manager** aus (Pflichtfeld). Dieser Manager erhält die durch Benutzer gesendete Meldungen, wenn ein Login-Versuch von einer eingeschränkten IP-Adresse unternommen wird.
10. Klicken Sie auf **Login-Einschränkungen aktivieren**. Um Ihre Änderungen zu speichern, ohne Login-Einschränkungen zu aktivieren oder zu deaktivieren, klicken Sie auf **Speichern**.

Note

- Sie müssen auf **LoginBeschränkungen aktivieren** klicken, damit die IP-Login-Beschränkungen in Kraft treten.
- Benutzer mit der Rolle des allgemeinen Systemadministrators sind nicht eingeschränkt.
- Um Login-Einschränkungen zu einem späteren Zeitpunkt zu deaktivieren, klicken Sie auf **Login-Einschränkungen deaktivieren**.

Wenn ein Benutzer mit einer eingeschränkten IP-Adresse versucht, sich bei Alma einzuloggen, wird die folgende Meldung angezeigt:

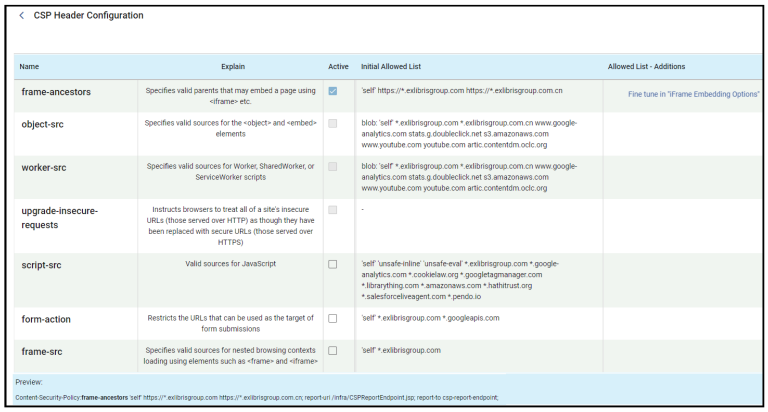


Zugriff gesperrt

Der Benutzer kann auf **Administrator kontaktieren** klicken, um den IP-Einschränkungs-Manager zu kontaktieren, den Sie oben konfiguriert haben.

Konfiguration der CSP-Überschrift (Content Security Policy)

Sie können CSP-Indexeintrag-Direktiven aktivieren und konfigurieren, um die Sicherheitsrichtlinie für Ihre Webanwendungen zu optimieren. Um auf diese Konfiguration zuzugreifen, gehen Sie zu **Konfiguration > Allgemein > Konfiguration der CSP-Überschrift**.



Konfiguration der CSP-Überschrift

Der Vorschaubereich unten zeigt die Indexeinträge an und wird automatisch aktualisiert, wenn die Einstellungen geändert werden.

Die ersten vier Anweisungen (Frame-Ancestors, Object-Src, Worker-Src, Upgrade-Insecure-Requests) sind standardmäßig aktiv und können nicht deaktiviert werden. Sie können der Zulassungsliste jedoch in der Spalte **Zulässige Liste – Ergänzungen** weitere Domains hinzufügen.

Die letzten fünf Anweisungen (unten beschrieben) sind standardmäßig deaktiviert, können aber im Gegensatz zu den ersten vier Anweisungen aktiviert werden. Sie können der Zulassungsliste in der Spalte **Zulässige Liste – Ergänzungen** weitere Domains hinzufügen.

1. **form-action**:
    - Diese Anweisung schränkt die URL ein, die als Ziel von Formular-Eingaben verwendet werden können (`<form action="..." />`). Dadurch wird verhindert, dass Formulare an bösartige Websites gesendet werden.
2. **base-uri**:
    - Diese Anweisung beschränkt die URLs, die in einem `<base>` -Element des Dokuments verwendet werden können Das `<base>` -Element gibt die Basis-URL an, die für alle relativen URLs in einem Dokument verwendet werden soll. Durch die Kontrolle kann daher verhindert werden, dass Angreifer die Basis-URL ändern und Links auf bösartige Websites umleiten.
3. **script-src**:
    - Diese Anweisung gibt gültige Quellen für JavaScript an. Dies trägt dazu bei, XSS-Angriffe abzuschwächen, indem es nur die Ausführung von Skripten aus vertrauenswürdigen Quellen auf der Seite zulässt. Sie können beispielsweise festlegen, dass Skripte nur von Ihrer eigenen Domain oder von einem vertrauenswürdigen CDN

geladen werden sollen.

4. **frame-src**:
   - Diese Direktive gibt gültige Quellen für das Einbetten von Inhalten mit `<frame>`, `<iframe>`, `<object>`, `<embed>` und `<applet>` an. Auf diese Weise lässt sich kontrollieren, welche Quellen in den Frame eingebettet werden können, und so Clickjacking und andere Arten von Frame-basierten Angriffen verhindern.
5. **connect-src**:
   - Diese Direktive beschränkt die URLs, die das Dokument mit Mechanismen wie `XMLHttpRequest`, `Fetch`, `WebSocket` und EventSource abrufen kann. Auf diese Weise lässt sich leichter kontrollieren, wohin Skripte Daten senden können, und das Risiko einer Datenexfiltration wird verringert.
6. **style-src**:
   - Die HTTP-Richtlinie `Content-Security-Policy` (CSP) `style-src` legt gültige Quellen für Formatvorlagen fest.
7. **img-src**:
   - Die HTTP-Richtlinie `Content-Security-Policy` `img-src` legt gültige Quellen für Bilder und Favicons fest.
8. **font-src**:
   - Die HTTP-Richtlinie `Content-Security-Policy` (CSP) `font-src` legt gültige Quellen für Schriften fest, die mittels `@font-face` geladen wurden.
9. **child-src**:
   - Die HTTP-Richtlinie `Content-Security-Policy` (CSP) `child-src` definiert die gültigen Quellen für Web-Angestellte und verschachtelte Browsing-Kontexte, die mit Elementen wie `<frame>` und `<iframe>` geladen werden. Für Angestellte werden nicht konforme Anfragen vom Benutzer-Agenten als schwerwiegende Netzwerkfehler behandelt.
10. **default-src**:
    - Die HTTP-Richtlinie `Content-Security-Policy` (CSP) `default-src` dient als Sicherheitsoption für die anderen CSP Abruf-Direktiven. Für jede fehlende Richtlinie sucht der Benutzer-Agent nach der Richtlinie `default-src` und verwendet diesen Wert.

Anmeldung - Weiterleitung - Erlaubte Liste

Um potenzielle Sicherheitsprobleme (offene Umleitungsschwachstelle) zu vermeiden, können Sie eine Liste vertrauenswürdiger Sites erstellen.

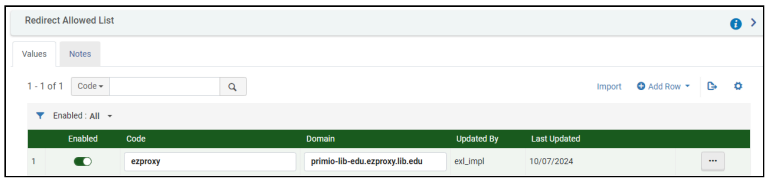
Um eine Liste vertrauenswürdiger Seiten zu erstellen:

1. Stellen Sie sicher, dass der Parameter **limit_login_redirects** (**Konfiguration > Allgemein > Andere Einstellungen**) auf Richtig gesetzt ist.
2. Navigieren Sie zu **Konfiguration > Allgemein > Weiterleitung - Erlaubte Liste**.
3. Fügen Sie für jede vertrauenswürdige Domain eine neue Zeile hinzu. Der Code ist nur beschreibend und wird von

Alma nicht verwendet.

Note

Domains, die zu Ex Libris gehören (*.exlibrisgroup.com), müssen nicht aufgeführt werden.



Vermeidung von Klickbetrug

Um die iFrame-Einbettungsoptionen zu steuern, müssen Sie die folgende Rolle innehaben:

- Allgemeiner Systemadministrator

Klickbetrug ist ein Angriff, bei dem Benutzer mit einer harmlosen Seite getäuscht werden, die echte Steuerelemente von sensiblen Seiten enthält. Diese Steuerelemente werden durch die Verwendung von Hintergrundrahmen getarnt, die alles mit Ausnahme der Steuerelemente maskieren, so dass der Benutzer nicht erkennen kann, dass er tatsächlich auf einer anderen Website eine sensible Funktion anklickt. Dies kann dazu führen, dass Benutzer unwissentlich Malware herunterladen, Zugangsdaten oder vertrauliche Informationen weitergeben, Geld überweisen oder Produkte online kaufen.

Um Klickbetrug über ExLibris-Produkte zu verhindern, hat ExLibris eine richtlinienbasierte Abwehrtechnik eingeführt. Nun können Institutionen den Browser anweisen, welche Maßnahmen zu ergreifen sind, wenn ihre Website in einem iFrame enthalten ist.

Note

Eine Änderung dieser Seite kann UI-Integrationen von anderen Produkten unterbrechen. Wenn Sie Zweifel haben, wie diese Seite zu nutzen ist, wenden Sie sich bitte an den Ex Libris Kundendienst.

Um die Aktionen festzulegen, die ausgeführt werden sollen, wenn Ihre Website in einem iFrame enthalten ist:

1. Öffnen Sie die Tabelle **iFrame-Einbettungsoptionen** (**Konfiguration > Allgemein > Sicherheit > iFrame-Einbettungsoptionen**).
2. Wählen Sie für das gewünschte Produkt und die gewünschte Komponente in den Zeilenaktionen**Anpassen** aus.

   Note

   - Die Alma-Verwaltung und Esploro-Verwaltung können nicht in einen Frame einbezogen werden. Diese Konfiguration kann nicht bearbeitet werden.
   - Das Einbetten von IFrames wird nicht unterstützt, wenn Sie einen Azure IDP verwenden.

   ---

3. Wählen Sie in der Spalte **Aktion** die geeignete Aktion, die ausgeführt werden soll, wenn Ihre Website in einem iFrame enthalten ist:
   - **Alle erlauben** (Standardoption) – Allen Seiten erlauben, diese Seite in einem iFrame zu laden.

- **Geschützte erlauben** – Nur vertrauenswürdige Seiten dürfen diese Seite in einen iFrame laden. Wenn Sie diese Option gewählt haben, geben Sie in der Spalte **Safe Domain** die vertrauenswürdigen URLs an (es gibt keine Einschränkung der Anzahl an URLs, die Sie angeben können, führen Sie mehrere URLs getrennt durch ein Leerzeichen an).

Note

Wir empfehlen das Hinzufügen von `https://*.WEBSITEHERE.com`, zum Beispiel `https://*.amazon.com`".

- **Alle sperren** – Alle Versuche zum Framing der Seite werden abgelehnt.

4. Klicken Sie auf **Speichern**.